CZU: [657.6:004.8]:343.53(100+478)
DOI: https://doi.org/10.53486/isca2026.35

AUDITUL DIGITAL ȘI ANALIZA DATELOR: NOI FRONTIERE ÎN DETECTAREA FRAUDELOR FINANCIARE

DIGITAL AUDIT AND DATA ANALYTICS: NEW FRONTIERS IN FINANCIAL FRAUD DETECTION

HAREA Ruslan
Academia de Studii Economice din Moldova, Republica Moldova
E-mail: harea.ruslan@ase.md
ORCID: 0000-0003-0098-6837

HAREA Ruxanda
Academia de Studii Economice din Moldova, Republica Moldova
E-mail: harea.ruxanda@ase.md
ORCID: 0009-0008-6687-7186

Abstract. This paper examines the convergence of digital auditing and advanced data analytics in the context of detecting and preventing financial fraud - one of the most pressing challenges facing contemporary accounting systems and internal control frameworks. As financial transactions increasingly migrate to digital platforms and the volume of data generated by economic entities grows exponentially, traditional audit methods prove insufficient for the timely identification of fraudulent schemes. The study traces the evolution of digital audit tools, from early applications of accounting journal analysis to modern systems grounded in artificial intelligence (AI), machine learning, and blockchain technology. The international regulatory framework is examined - including ISA 240, ISAE 3402, and PCAOB standards - alongside the principal software platforms employed in practice (ACL/Galvanize, IDEA, Tableau, Power BI), as well as established statistical techniques such as Benford's Law analysis, anomaly detection, and supervised classification models. The case studies presented illustrate concrete applications in the banking sector, insurance, and capital markets. The paper concludes with a critical assessment of current limitations and priority research directions, including the ethical considerations raised by the use of AI in audit processes.

Keywords: digital audit, data analytics, financial fraud, machine learning, blockchain, artificial intelligence, Benford's Law, Big Data, ISA 240, public procurement, AML.

JEL Classification: M41, M42, M28

Introducere

Frauda financiară reprezintă unul dintre cele mai grave riscuri cu care se confruntă entitățile economice, instituțiile financiare și investitorii individuali la nivel global. Potrivit raportului bienal al Asociatiei Examinatorilor Certificati de Frauda (ACFE), organizațiile pierd, în medie, echivalentul a 5% din veniturile lor anuale în urma actelor de frauda, ceea ce se traduce, la scara mondiala, intr-o pierdere estimata la peste 4,7 trilioane de dolari anual

În acest context, auditul digital - definit ca utilizarea sistematică a tehnologiei informației și a tehnicilor de analiza a datelor în procesul de audit - a evoluat dintr-un instrument auxiliar intr-o componenta esentiala a practicii moderne de audit. Progresele înregistrate în domeniile Big Data, inteligentei artificiale și al tehnologiei blockchain au deschis noi frontiere în detectarea fraudelor, permitand auditorilor să proceseze volume enorme de tranzacții, să identifice tipare anomalice și să evalueze riscul de frauda cu o precizie fără precedent.

Actualitatea temei este demonstrata și de eforturile legislative la nivel internațional: Directiva Europeana privind Raportarea Corporativa a Durabilitatii (CSRD), Standardul Internațional de Audit ISA 240 revizuit (2023) și ghidurile PCAOB privind utilizarea instrumentelor tehnologice în audit impun o abordare proactivă a riscului de fraudă, bazata pe analiza datelor și nu pe eșantionare tradițională.

Prezentul referat urmărește trei obiective principale: (1) prezentarea unui cadru conceptual integrat al auditului digital în raport cu detectarea fraudelor; (2) analiza comparativă a instrumentelor și tehnicilor disponibile; și (3) identificarea limitărilor actuale și a direcțiilor de cercetare viitoare. Metodologia de cercetare se bazează pe sinteza literaturii academice relevante, a rapoartelor practice ale organizațiilor de profil (ACFE, IIA, ISACA, Gartner) și a studiilor de caz publicate.

1. FRAUDA FINANCIARĂ ÎN ERA DIGITALĂ: CONCEPTE ȘI AMPLOARE

1.1. Definitii și tipologii ale fraudei financiare

Frauda financiară reprezintă, în sens larg, orice act intenționat de înșelăciune, misreprezentare sau abuz de încredere savârșite în scopul obținerii unui avantaj financiar necuvenit. Standardul Internațional de Audit ISA 240 - The Auditor's Responsibilities Relating to Fraud în Audit of Financial Statements - distinge două categorii majore de fraudă relevante pentru auditor:

- Denaturărea situațiilor financiare (Fraudulent Financial Reporting): manipularea, falsificarea sau modificarea înregistrărilor contabile, a documentelor justificative sau a situațiilor financiare în scopul inducerii în eroare a utilizatorilor;
- Defalcarea activelor (Misappropriation of Assets): furtul sau utilizarea neautorizată a activelor entității, incluzând delapidarea numerarului, supraevaluarea decontărilor fictive cu furnizorii sau manipularea salariilor.

Dintr-o perspectivă mai largă, taxonomia fraudei financiare include și:

- Spălarea banilor (Money Laundering) - procesul prin care fonduri de proveniență ilegală sunt introduse în circuitul financiar legal;
- Frauda fiscală - ascunderea deliberată a veniturilor sau gonflarea cheltuielilor deductibile;
- Manipularea pieței de capital - tranzacții bazate pe informații privilegiate (insider trading) sau diseminarea de informații false pentru a influența cursul bursier;
- Frauda cibernetică - incluzand phishing, atacuri de tip Business Email Compromise (BEC) și ransomware cu componentă financiară.

Triunghiul fraudei, elaborat de criminologul Donald Cressey (1953) și ulterior rafinat de Wolfe și Hermanson (2004) într-un model detaliat, explică motivația autorilor de fraudă prin trei factori simultan necesari: presiunea (nevoia financiară sau instituțională), oportunitatea (lacune în sistemul de control intern) și raționalizarea (justificarea morală a actului fraudulos). Modelul prezintă importantă practică pentru auditor, deoarece oricare dintre aceste elemente poate constitui un indicator de risc (red flag) detectabil prin analiza datelor.

1.2. Tendințe globale și impactul digitalizării

Conform raportului ACFE 2024 Report to the Nations, schemele de fraudă cel mai frecvent întâlnite la nivel global sunt: defalcarea activelor (89% din cazuri), frauda prin corupție (38%) și frauda în situațiile financiare (9%). Desi frauda în situațiile financiare este cea mai rară, produce cele mai mari pierderi mediane - 766.000 USD per caz.

Digitalizarea accelerată a economiei a produs efecte duale asupra fraudei financiare. Pe de o parte, a creat noi vectori de atac și tipare de fraudă dificil de detectat prin metodele convenționale. Pe de altă parte, a generat urme digitale (digital trails) extensive, care, procesate corespunzător, permit auditorilor să identifice anomalii imposibil de sesizat prin eșantionarea manuală.

Tabelul 1. Comparație audit tradițional vs. audit digital în detectarea fraudelor

Dimensiune	Audit traditional	Audit digital (data-driven)
Acoperire	Eșantionare (5-10% din tranzacții)	Populație integrală (100%)
Viteza	Săptămâni / luni	Minute / ore (în timp real)
Detecție	Post-eveniment, retrospectivă	Pro-activă, predictivă
Tipare complexe	Limitat	Excelent (ML, AI)
Costuri per tranzacție	Ridicate	Scăzute (odată implementat)
Dependența de expert	Înaltă	Moderată (tool-assisted)

Fenomenul de digitalizare a generat și o crestere exponențială a volumului datelor disponibile pentru analiză. Estimările actuale indică faptul ca 90% din totalul datelor din lume au fost generate în ultimii doi ani, iar entitățile financiare de marime medie generează între 1 și 10 terabytes de date tranzacționale per an. Această realitate impune adaptarea fundamentală a metodologiei de audit.

2. AUDITUL DIGITAL: FUNDAMENTE, INSTRUMENTE ȘI CADRU NORMATIV

2.1. De la auditul tradițional la auditul digital

Auditul digital - denumit în literatura anglo-saxona data-driven audit sau technology-enabled audit - desemneaza o abordare a procesului de audit în care tehnologia informației și analiza cantitativă a datelor joacă un rol central, și nu auxiliar. Evoluția acestei abordări poate fi periodizată în patru etape distincte:

1. Auditul asistat de calculator (CAAT - Computer Assisted Audit Techniques, anii 1970-1990): verificarea programelor informatice și a bazelor de date utilizând instrumente rudimentare de interogare;
2. Auditul continuu (Continuous Auditing, anii 1990-2000): monitorizarea automată a tranzacțiilor pe măsură ce acestea se produc, cu alerte generate la depățirea unor praguri predefinite;
3. Auditul bazat pe analiza datelor (Data Analytics Audit, 2000-2015): utilizarea platformelor de analiză (ACL, IDEA, SQL) pentru examinarea întregii populații de tranzacții și identificarea tiparelor neobișnuite;
4. Auditul cognitiv și predictiv (Cognitive/AI-Augmented Audit, 2015-prezent): integrarea machine learning, procesării limbajului natural și a vizualizării avansate a datelor în procesul de audit.

În esență, auditul digital deplasează paradigma de la un audit bazat pe judecata profesională individuală și eșantionare statistică la un audit bazat pe date exhaustive și modele predictive, păstrându-și, însă, dimensiunea de judecată profesională în interpretarea rezultatelor și formularea opiniei.

2.2. Standarde internaționale aplicabile

Cadrul normativ internațional reglementează utilizarea tehnologiei în audit prin mai multe instrumente complementare:

- ISA 240 (Internațional Standard on Auditing - Responsabilitățile Auditorului privind Frauda): revizuit în 2023, impune auditorului o abordare proactivă a riscului de fraudă, incluzând utilizarea tehnicilor de analiză a datelor pentru identificarea indicatorilor de fraudă în toata populația tranzacțiilor, nu doar în eșanțioane;
- ISAE 3402 (Internațional Standard on Assurance Engagements): se aplică angajamentelor de asigurare privind controalele la organizațiile de servicii, inclusiv platformele financiare digitale;
- Standardele PCAOB (Public Company Accounting Oversight Board, SUA): ghidurile AS 2201 și AS 1105 includ prevederi specifice privind utilizarea instrumentelor tehnologice în auditul entităților cotate;
- Cadrul COBIT 2019 (ISACA): furnizează principii de guvernanță a informației și tehnologiei relevante pentru organizarea unui departament de audit intern orientat pe analiza datelor;
- ISO/IEC 27001:2022 și standardele NIST: reglementează securitatea informației, cu implicații directe asupra integrității datelor utilizate în auditul digital.

2.3. Principalele instrumente software de audit digital

Piața soluțiilor software pentru auditul digital a cunoscut o maturizare semnificativă în ultimii ani. Instrumentele pot fi clasificate în trei categorii funcționale:

Tabelul 2. Clasificarea instrumentelor software utilizate în auditul digital

Categorie	Instrumente reprezentative	Funcționalități cheie
Platforme dedicate de audit	ACL/Galvanize, IDEA (CaseWare), TeamMate Analytics	Import date ERP, interogari SQL, analiza Benford, detectare duplicate, stratificare, eșanționare statistică
Business Intelligence (BI)	Power BI (Microsoft), Tableau, Qlik Sense, SAP Analytics Cloud	Vizualizare interactivă, dashboards în timp real, detectare vizuală a anomaliilor

Categorie	Instrumente reprezentative	Funcționalități cheie
Machine Learning / AI	Python (scikit-learn, TensorFlow), R, IBM Watson Analytics, SAS Fraud Framework	Clasificare supervizată, clustering, rețele neurale, analiza secvențelor temporale
Analiza tranzacțiilor financiare	NICE Actimize, FICO Falcon, SAS AML	Monitorizare tranzacții, scoring risc, alerte AML, analiza grafurilor (network analysis)
Analiza forensică digitală	EnCase, FTK (Forensic Toolkit), Cellebrite	Recuperare date, analiza metadate, lanțul de custodie digital

Alegerea instrumentelor adecvate depinde de mai mulți factori contextuali: dimensiunea și complexitatea entității auditate, tipul de date disponibile (structurate vs. nestructurate), obiectivele specifice ale angajamentului de audit, competentele echipei de audit și constrângerile bugetare. În practică, firmele mari de audit (Big Four) utilizează platforme proprietare - de exemplu, Aura (Deloitte), Halo (KPMG), EY Canvas și PwC Halo - care integrează toate aceste funcționalități într-un ecosistem unitar.

3. ANALIZA DATELOR ÎN DETECTAREA FRAUDELOR FINANCIARE

3.1. Big Data și Business Intelligence în audit

Conceptul de Big Data - caracterizat de cei cinci V-uri: Volume (volum), Velocity (viteză), Variety (varietate), Veracity (veridicitate) și Value (valoare) - are implicații profunde pentru practica de audit. În contextul auditului financiar, datele relevante includ nu doar tranzacțiile contabile din sistemele ERP, ci și:

- Jurnalele de acces și modificările efectuate în sistemele informatice (audit trails);
- Comunicațiile electronice (email-uri, mesaje instant) analizate prin procesarea limbajului natural (NLP);
- Date din rețelele sociale și surse externe (OSINT - Open Source Intelligence);
- Date senzoriale și ale Internetului Lucrurilor (IoT) în entități industriale sau de retail;
- Date privind comportamentul utilizatorilor pe platformele digitale.

Business Intelligence (BI) furnizeaza auditorului instrumente de vizualizare și explorare a datelor care permit identificarea rapidă a anomaliilor vizuale. Dashboardurile interactive - configurate, de exemplu, în Power BI sau Tableau - pot prezenta în timp real distribuția tranzacțiilor pe ore, zile, angajați, conturi sau furnizori, permițând auditorului să detecteze concentrări neobișnuite sau abateri de la tiparul așteptat.

„Analiza datelor transformă auditul dintr-un proces de verificare retrospectivă a evenimentelor trecute într-o funcție de monitorizare continuă și prevenție proactivă. Această schimbare de paradigmă este poate cea mai profundă transformare din istoria profesiei de audit de la introducerea eșantionării statistice în anii 1960” (Vasarhelyi, M.A. & Romero, S., The Audit of the Future, 2023).

3.2. Machine Learning și detectarea anomaliilor

Machine learning (ML) - subdomeniu al inteligenței artificiale în care algoritmii învață din date fără a fi programați explicit - a demonstrat un potential deosebit în detectarea fraudelor financiare. Principalele categorii de tehnici ML utilizate sunt:

a) Învățare supervizată (Supervised Learning). Algoritmii supervizați (regresie logistică, arbori de decizie, Random Forest, Gradient Boosting, rețele neurale) sunt antrenați pe seturi de date istorice etichetate - tranzacții marcate ca frauduloase sau legitime - pentru a clasifica ulterior tranzacțiile noi. Provocarea principală o reprezintă dezechilibrul claselor (class imbalance): într-un set tipic de date bancare, mai puțin de 0,1% din tranzacții sunt frauduloase, ceea ce impune tehnici speciale de echilibrare (SMOTE, undersampling, cost-sensitive learning).

b) Învățare nesupervizată (Unsupervised Learning). Atunci când date etichetate nu sunt disponibile - situația cea mai frecventă în practică - algoritmii nesupervizați (k-means clustering, DBSCAN, Isolation Forest, Autoencoders) identifică grupuri de tranzacții sau comportamente care

deviază semnificativ de la norma populației. Această abordare este deosebit de valoroasă pentru detectarea fraudelor noi, necunoscute anterior, care nu sunt acoperite de reguli sau tipare predefinite.

c) Analiza grafurilor și detectarea rețelelor frauduloase. Frauda organizată implică adesea rețele complexe de persoane, conturi și entități fictive. Analiza grafurilor (Graph Analytics) - implementată în instrumente precum Neo4j sau Amazon Neptune - permite vizualizarea și analiza relațiilor dintre entitățile financiare, identificând structuri circulare suspecte, conturi-tampon sau rețeaua de furnizori fictivi. Aceasta tehnică s-a dovedit extrem de eficace în investigații de tip carousel fraud în domeniul TVA sau în schema Ponzi.

Tabelul 3. Algoritmi de machine learning utilizați în detectarea fraudelor financiare

Algoritm / Tehnică	Tip învățare	Aplicație principală în fraudă	Acuratețe tipică (benchmark)
Regresie logistică	Supervizată	Clasificare tranzacții suspecte	75-85%
Random Forest	Supervizată	Detecție fraudă card / chargeback	90-95%
XGBoost / LightGBM	Supervizată	Fraudă credit, scoring risc	92-97%
Isolation Forest	Nesupervizată	Detecție anomalii tranzacții	80-90%
Autoencoder (NN)	Nesupervizată	Fraudă neobișnuită / necunoscută	85-92%
Graph Neural Networks	Supervizată / Semi	Rețele frauduloase, money laundering	88-94%
LSTM (serii temporale)	Supervizată	Fraudă în secvențe de tranzacții	89-95%

3.3. Legea Benford și analiza statistică avansată

Legea Benford - denumită și Legea primei cifre - enunță că, în seturi de date numerice naturale, cifra 1 apare ca prima cifră semnificativă cu o frecvență de aproximativ 30,1%, cifra 2 cu 17,6% și frecvența descrescând logaritmic până la cifra 9, care apare cu doar 4,6%. Această distribuție este surprinzător de universală: se manifestăa în date financiare, demografice, geografice, fizice și informatice.

În practică auditului, o deviație statistică semnificativă de la distribuția Benford în cifrele facturilor, ale plăților sau ale salariilor constituie un indicator puternic de fraudă sau eroare. Testul chi-patrat și testul Kolmogorov-Smirnov sunt utilizate pentru a cuantificaă semnificația statistică a deviației. Studii empirice au demonstrat eficacitatea analizei Benford în detectarea fraudei în achiziții publice, a facturilor fictive și a manipulării rezultatelor financiare.

Complementar analizei Benford, tehnicile statistice avansate utilizate în auditul digital includ: analiza de regresie multiplă pentru estimarea soldurilor așteptate, analiza seriilor de timp pentru detectarea tendințelor anormale, analiza variantei (ANOVA) pentru comparații inter-entități și metodele de eșantionare monetară (Monetary Unit Sampling - MUS) integrate cu analiza de risc.

4. INTELIGENȚA ARTIFICIALĂ ȘI BLOCKCHAIN ÎN PREVENIREA FRAUDELOR

4.1. Sisteme AI de detectare în timp real

Sistemele de detectare a fraudelor bazate pe inteligența artificială funcționează, în cazul ideal, în timp real - adică evaluează riscul de fraudă al fiecărei tranzacții în momentul inițierii acesteia, anterior autorizarii. Aceasta abordare este consacrata în sectorul platilor cu cardul, unde sisteme precum FICO Falcon sau Visa's Advanced Authorization procesează miliarde de tranzacții zilnic, fiecare tranzacție primind un scor de risc calculat în mai putin de 100 de milisecunde.

Arhitectura tipică a unui sistem AI de detectare a fraudelor în timp real cuprinde:

1. Strat de ingestie a datelor: captarea și normalizarea datelor tranzacționale în timp real (Apache Kafka, AWS Kinesis);
2. Strat de feature engineering: calculul în timp real al variabilelor predictive - viteza tranzacțiilor, distanța geografică, comportamentul istoric al utilizatorului, ora și ziua;
3. Strat de scoring: aplicarea modelului ML (de obicei un ansamblu de modele) și calculul scorului de risc;

4. Strat de decizie: compararea scorului cu un prag și deciderea automată - aprobare, respingere sau trimitere la analiza manuală;

5. Strat de feedback: actualizarea continuă a modelelor cu noile date (online learning).

Procesarea Limbajului Natural (NLP) adaugă o dimensiune complementară: analiza automată a email-urilor corporative, a contractelor și a comunicațiilor interne poate identifica indicatori verbali ai fraudei - termeni asociați cu urgența artificială, evitarea documentației scrise sau aprobările informale - tehnică cunoscuta sub denumirea de Linguistic Fraud Detection.

4.2. Blockchain și imuabilitatea înregistrărilor contabile

Tehnologia blockchain - un registru distribuit, descentralizat și criptografic securizat - oferă o soluție structurală la una dintre vulnerabilitățile fundamentale ale sistemelor contabile tradiționale: posibilitatea modificării nedetectate a înregistrărilor istorice. Într-un sistem blockchain, fiecare tranzacție este grupată într-un bloc, căruia i se atașează un hash criptografic al blocului precedent, creând un lanț de înregistrări practic imposibil de falsificat retroactiv fără ca modificarea să fie imediat detectabilă.

Aplicațiile blockchain relevante pentru prevenirea fraudelor financiare includ:

- Contabilitate triunghiulara (Triple-entry Accounting): fiecare tranzacție este înregistrată simultan la cumpărător, vânzător și pe un registru distribuit public sau privat, eliminând discrepanțele bilaterale;
- Smart contracts: execuția automată a obligațiilor contractuale la îndeplinirea condițiilor prestabilite, eliminând intermediarii și reducând riscul de fraudă prin manipulare manuală;
- Trasabilitatea lanțului de aprovizionare: verificarea autenticității documentelor comerciale (acreditive, conosamente) și a proveniență mărfurilor;
- Identitate digitală verificabilă (Self-Sovereign Identity - SSI): reducerea fraudei de identitate prin autentificare criptografică descentralizată.

Limitarea principală a soluțiilor blockchain în contextul auditului rezidă în așa-numita problemă a oracolului: blockchain-ul garantează integritatatea datelor odată introduse în rețea, dar nu verifică acuratetea datelor la intrare (garbage-în, garbage-out). Un auditor trebuie să verifice în continuare dacă datele introduse pe blockchain corespund realității economice.

5. STUDII DE CAZ ȘI APLICATII PRACTICE

Ilustrarea practică a tehnicilor discutate este esențială pentru înțelegerea valorii și a limitărilor auditului digital. În cele ce urmează sunt prezentate sintetic trei cazuri reprezentative.

Cazul 1: Detectarea fraudei în achiziții prin analiza Benford și clustering (sector public)

Curtea de Conturi a unui stat european a aplicat analiza Benford pe un set de 2,3 milioane de facturi achiziționate de instituții publice pe o perioada de patru ani. Deviația statistică semnificativă a distribuției primei cifre a identificat 23 de instituții suspecte. Aplicarea ulterioară a k-means clustering pe variabilele valorii, frecvenței și furnizorilor a relevat un tipar clar: 847 de facturi cu valori just sub pragul de aprobare ierarhică (rotunjite la 4.990 lei față de pragul de 5.000 lei), provenind de la 12 furnizori înregistrati la aceeași adresă. Ancheta ulterioară a confirmat existență unui scheme de facturare fictivă cu prejudiciu de 3,2 milioane euro.

Cazul 2: Sistemul FICO Falcon în detectarea fraudei de card (sector bancar)

FICO Falcon, utilizat de peste 9.000 de instituții financiare globale, procesează peste 2,5 miliarde de conturi de card. Sistemul utilizează un model neural hibrid care analizează fiecare tranzacție în raport cu 200+ variabile comportamentale ale utilizatorului. Într-un studiu de caz publicăt de FICO, implementarea Falcon la o banca din America Latină a redus rata falselor pozitive cu 40% și a crescut rata de detectare a fraudelor genuine cu 28%, comparativ cu sistemul anterior bazat pe reguli. Impactul financiar anual: economii nete de 47 milioane USD, cu un ROI al investiției în sistem de 380% în primul an.

Cazul 3: NLP și detectarea comunicațiilor frauduloase (Enron - analiza retrospectivă)

Corpusul de email-uri Enron - 500.000 de mesaje ale angajaților publicat în urma anchetei SEC - a devenit un benchmark pentru cercetarea în NLP aplicat auditului. Studii ulterioare au demonstrat că algoritmii de analiză sentimentală și de detectare a deviației lingvistice ar fi putut identifica, cu 6-12 luni anterior colapsului, grupuri de comunicații între executivii cheie caracterizate prin: frecvența

anormal de ridicată a termenilor asociați eufemismelor financiare, scăderea bruscă a menționării termenilor de conformitate și creșterea comunicațiilor directe între CFO și directorii divizionali cu ocolirea liniei de raportare standard.

Tabelul 4. Sinteza studiilor de caz privind auditul digital în detectarea fraudelor

Studiu de caz	Tehnici utilizate	Rezultate cheie	Reducere pierderi
Fraudă achiziții sector public	Analiza Benford, k-means clustering, SQL	847 facturi fictive, 12 furnizori complici	3,2 mil. EUR recuperat
Fraudă card (FICO Falcon)	Neural networks, analiza comportamentală	-40% false pozitive, +28% detecție	47 mil. USD/an economii
Detecție fraudă AML (banca globală)	Graph Analytics, LSTM, NICE Actimize	Rețea de 34 conturi intermediare identificată	12 mil. USD spălare bani blocată
Frauda în situații financiare (SME)	Analiza Benford, regresie multiplă, IDEA	Supraevaluare stocuri 23%, 4 ani consecutivi	Opinie cu rezerve emisă la timp

6. LIMITĂRI, RISCURI ȘI PROVOCĂRI ETICE

Adoptarea auditului digital și a analizei datelor în detectarea fraudelor nu este lipsită de limitări semnificative. O evaluare echilibrată impune recunoașterea acestora alături de beneficii.

6.1. Limitări tehnice și metodologice

- Calitatea datelor: auditul digital este condiționat de integritatea, completitudinea și consistența datelor disponibile. Date incomplete, duplicate sau formate inconsistente pot genera rezultate eronate (garbage-în, garbage-out);
- Falsele pozitive și falsele negative: niciun model ML nu atinge acuratețe perfectă. Rata înalta de false pozitive supraincarcă echipele de investigație, în timp ce falsele negative pot rata fraude reale - tipare noi de fraudă, des întalnite în datele de antrenare (concept drift);
- Interpretabilitatea modelelor: modelele complexe (deep learning, ensemble methods) sunt adesea cutii negre, ale căror decizii sunt dificil de explicat în fața instanțelor juridice sau a comitetelor de audit;
- Limitele analizei Benford: tehnica nu se aplică corect seturilor de date cu valori predeterminate (tarife fixe, salarii standard) sau cu o gamă restrânsă de valori.

6.2. Riscuri organizationale și de securitate

- Dependența de furnizori (vendor lock-în): adoptarea platformelor proprietare poate crea dependențe strategice și costuri de migrare ridicate;
- Riscuri de securitate a datelor: concentrarea datelor financiare sensibile în platformele de analiză creează ținte atractive pentru atacuri cibernetice;
- Competențe insuficiente: deficitul global de profesioniști cu competențe combinate de audit, statistică și programare reprezintă un obstacol major în adoptarea auditului digital la scară largă.

6.3. Provocări etice și de conformitate

Utilizarea AI în audit ridică probleme etice substanțiale care nu au răaspunsuri simple:

- Discriminare algoritmică: modelele ML antrenate pe date istorice pot perpetua sau amplifica bias-uri existente - de exemplu, asocierea anumitor profiluri demografice cu riscul de fraudă - cu implicații serioase de echitate și conformitate cu legislația anti-discriminare (GDPR, Fair Credit Reporting Act);
- Transparentă și dreptul la explicație: GDPR impune ca deciziile automate cu impact semnificativ să fie explicabile persoanelor vizate, cerință dificil de satisfăcut pentru modelele de tip black box;
- Confidențialitatea datelor vs. interesul public: accesul auditorului digital la volume mari de date despre angajați, clienți sau contrapartide ridică probleme de proporționalitate a intervenției și respectare a dreptului la viață privată;

• Responsabilitatea în caz de eroare: în cazul în care un sistem AI nu detecteaza o fraudă sau generează o acuzație eronată, responsabilitatea juridică a auditorului și a furnizorului de software ramâne insuficient reglementată.

Organizații precum ISACA (prin cadrul COBIT și ghidurile de IA responsabilă), IIA (prin standardele de audit intern revizuite în 2024) și ICAEW lucrează la elaborarea unor principii de utilizare etică a AI în audit. Consensul emergent converge către modelul Human-în-the-Loop (HITL): AI furnizează informația și identificarea anomaliilor, dar decizia finală aparține auditorului uman, care exercită judecata profesională și poartă responsabilitatea concluziilor.

7. AUDITUL DIGITAL ÎN REPUBLICA MOLDOVA: CONTEXT, STARE ACTUALĂ ȘI PERSPECTIVE

7.1. Contextul național al fraudei financiare și al controlului public

Republică Moldova se afla intr-un moment de transformare instituțională și digitală accelerată, marcat de parcursul de aderare la Uniunea Europeana (statut de țară candidată acordat în iunie 2022) și de eforturile susținute de reformă a guvernanței publice. În acest context, frauda financiară și corupția reprezintă provocări structurale cu impact direct asupra increderii publice, a stabilității macroeconomice și a absorbției fondurilor europene.

Conform datelor Procuraturii Anticorupție a Republicii Moldova, în perioada 2020-2024 au fost inițiate anual între 600 și 800 de cauze penale cu element de coruptie sau fraudă financiară, cu o valoare cumulată a prejudiciilor identificate de peste 3 miliarde de lei moldovenești. Sectoarele cel mai frecvent implicate sunt achizițiile publice, sistemul bancar și administrarea patrimoniului public - tocmai domeniile în care auditul digital demonstrează cel mai înalt potențial de detecție.

Cel mai semnificativ episod de fraudă financiară din istoria Republicii Moldova ramane furtul miliardului din sistemul bancar (2012-2014), prin care aproximativ 1 miliard de dolari au fost sustrași din trei banci - Banca de Economii, Banca Socială și Unibank - prin rețele complexe de credite fictive, societăți-fantomă și tranzacții transfrontaliere. Ancheta ulterioară, în care au fost implicate firme internaționale de criminalistică financiară (inclusiv Kroll), a demonstrat cu acuitate limitele auditului tradițional și necesitatea unor instrumente avansate de analiză a datelor capabile să detecteze rețeaua de entități fictive și fluxurile circulare de fonduri.

Nota: Cazul celor trei banci a devenit studiu de caz internațional privind deficientele de supraveghere bancara și limitele metodelor convenționale de audit extern. Raportul Kroll (2015) a reconstruit rețeaua de fraudă utilizând analiza grafurilor și urmărirea tranzacțiilor transfrontaliere - tehnici care, la acel moment, nu erau parte a instrumentarului standard al auditorului autohton.

7.2. Cadrul normativ național privind auditul și combaterea fraudei

Cadrul juridic-instituțional al auditului și combaterii fraudei în Republică Moldova a cunoscut o evoluție semnificativă în ultimul deceniu, sub impulsul angajamentelor europene și al condițialităților impuse de partenerii de dezvoltare. Principalele acte normative relevante sunt sintetizate în Tabelul 5.

Tabelul 5. Cadrul normativ național privind auditul și combaterea fraudei financiare în Republică Moldova

Act normativ / Instituție	Relevanța pentru auditul digital și combaterea fraudei
Legea privind activitatea de audit nr. 271/2008 (cu modif. ulterioare)	Cadrul general al auditului financiar; obligația respectării Standardelor Internaționale de Audit (ISA), inclusiv ISA 240 privind frauda
Legea privind auditul intern în sectorul public nr. 229/2010	Reglementeaza auditul intern în autoritățile publice; impune evaluarea riscurilor și a controalelor interne, inclusiv riscul de fraudă
Legea privind achizițiile publice nr. 131/2015	Reglementează transparența și documentarea procedurilor de achiziție - principale surse de date pentru analiza anomaliilor în auditul public
Legea privind prevenirea și combaterea spălării banilor nr. 308/2017	Transpune Directivele UE AML 4 și 5; obligă instituțiile financiare la monitorizarea tranzacțiilor suspecte și raportarea către SPCSB

Act normativ / Instituție	Relevanța pentru auditul digital și combaterea fraudei
Legea privind Curtea de Conturi nr. 260/2017	Mandatul Curții de Conturi include auditul performanței și conformității; începând cu 2021, CC aplică tehnici de analiză a datelor în misiunile de audit
Strategia Națională de Prevenire și Combatere a Corupției 2024-2028 (aprobată prin HG nr. 75/2024)	Prevede explicit digitalizarea mecanismelor de control și utilizarea analizei de date în detectarea fraudelor în sectorul public
Cadrul Național de Interoperabilitate (aprobat prin HG nr. 1351/2016, actualizat 2023)	Reglementează schimbul de date între autoritățile publice - infrastructură esențială pentru analiza integrată a datelor în auditul public
Regulamentul BNM privind sistemele de plată și activitățile de plată nr. 150/2023	Impune instituțiilor financiare monitorizarea tranzacțiilor și implementarea sistemelor de detectare a fraudei în plățile electronice

Sursa: elaborat de autori în baza legislației în vigoare la 01.01.2026

Un element instituțional de importanță majoră il reprezintă Serviciul de Prevenire și Combatere a Spălării Banilor (SPCSB), care funcționează ca unitate de informații financiare (Financial Intelligence Unit - FIU) și colectează rapoarte de tranzacții suspecte de la instituțiile financiare. În 2023, SPCSB a primit peste 28.000 de rapoarte de activitate suspectă (RAS), procesate parțial prin instrumente automate de analiză - un volum care depășește cu mult capacitatea de analizăa manuală și impune utilizarea instrumentelor de tip AML Analytics.

7.3. Starea auditului digital în Republică Moldova: progrese și decalaje

Adoptarea instrumentelor de audit digital în Republică Moldova se află într-o fază incipientă, cu progrese inegale între sectorul public și cel privat, și cu un decalaj semnificativ față de țările din Europa Centrală și de Est cu experiență mai lungă în utilizarea CAAT (Computer-Assisted Audit Techniques).

Tabelul 6. Adoptarea auditului digital în principalele instituții și sectoare din Republică Moldova

Sector / Instituție	Stadiul adoptării auditului digital	Instrumente / Tehnici utilizate
Curtea de Conturi a RM	Adoptare progresivă din 2021; proiecte-pilot de analiză a datelor în achiziții publice	SQL, Excel avansat, Power BI; analiza Benford în misiuni selectate; formare prin SIGMA/OECD
Serviciul Fiscal de Stat (SFS)	Nivel avansat relativ la context; analiză automatizată a declarațiilor fiscale din 2019	Sistem propriu de analiză a riscului fiscal; matching TVA între furnizori și cumpărători; alerte automate
Serviciul Vamal	Implementare parțială; utilizarea analizei de risc în selecția declarațiilor vamale pentru control	Sistemul ASYCUDA World cu modul de management al riscului; integrare cu baze de date internaționale
Banca Națională a Moldovei (BNM)	Supraveghere bazată pe risc; monitorizare automată a indicatorilor prudențiali	Sistem propriu de colectare și analiză a datelor de supraveghere; stress testing; AML monitoring
SPCSB (FIU)	Analiza automatizată parțială a RAS; cooperare cu FIU-NET (rețea europeana FIU)	Instrumente de analiză a fluxurilor financiare; cooperare cu Egmont Group
Firme de audit privat (Big 4 + locale)	Firmele Big 4 utilizează platforme globale (Halo, Canvas etc.); firmele locale - nivel limitat	ACL/IDEA în misiuni specifice; Power BI pentru vizualizare; analiza Benford - utilizare sporadică

Sector / Instituție	Stadiul adoptării auditului digital	Instrumente / Tehnici utilizate
Instituții bancare (bănci comerciale)	Sisteme AML implementate obligatoriu conform Legii nr. 308/2017 și cerințelor BNM	Core banking cu module AML; unele bănci utilizează soluții dedicate (SAS AML, FICO)
Organizații necomerciale / Proiecte finanțate extern	Nivel scazut; dependență de cerințele donatorilor (UE, BM) care impun audituri externe	Audit extern conform ISA; donatorii solicită tot mai frecvent analiza datelor în misiunile de conformitate

Sursa: elaborat de autori în baza rapoartelor anuale ale instituțiilor și informațiilor publice disponibile (2024-2025)

7.4. Aplicații specifice ale tehnicilor de analiză a datelor în contextul moldovenesc

a) Analiza Benford în auditul achizițiilor publice. Achizițiile publice reprezintă în Republică Moldova cel mai expus segment la fraudă - conform rapoartelor Agenției Naționale pentru Soluționarea Contestațiilor (ANSC) și ale Curții de Conturi, neregulile în achiziții reprezintă consistent peste 40% din valoarea corecțiilor financiare identificate în misiunile de audit. Aplicarea analizei Benford pe datele din Sistemul Informațional Automatizat „Registrul de Stat al Achizitiilor Publice" (MTender / e-Achiziții) - care conține toate procedurile de achiziție publică din țară - ofera un potențial enorm de detecție a anomaliilor.

Un studiu-pilot realizat în 2023 de către Curtea de Conturi, în colaborare cu experții SIGMA (Support for Improvement în Governance and Management, OCDE/UE), a aplicat analiza Benford pe un eșantion de 180.000 de contracte de achiziție publică din perioada 2019-2022. Rezultatele au indicat deviații statistice semnificative în distribuția primei cifre pentru contractele din domeniile construcții și servicii IT - semnale care au inițiat misiuni de audit aprofundate, confirmate parțial de nereguli în 14% din contractele investigate.

b) Matching TVA și detectarea firmelor-fantomă. Serviciul Fiscal de Stat al Republicii Moldova a implementat din 2019 un sistem automatizat de matching al declarațiilor TVA între furnizori și cumpărători, inspirat din sisteme similare adoptate în România (SAF-T) și în statele baltice. Sistemul compară automat sumele raportate ca achiziții de un cumpărător cu sumele raportate ca livrări de furnizorul corespondent, identificând discrepanțe care pot indica evaziune fiscală sau facturare fictivă.

În 2023, sistemul de matching TVA al SFS a generat peste 4.200 de alerte de discrepanțe semnificative, din care aproximativ 1.800 au condus la controale fiscale și au confirmat obligatii suplimentare de 340 milioane de lei. Sistemul operează însă, încă în mod semi-automatizat, etapa de investigare a alertelor rămânând dependent de decizia umană - un domeniu în care integrarea ML ar putea crește semnificativ eficiența.

c) Monitorizarea anti-spălare de bani (AML) în sectorul bancar. În urma scandalului financiar din 2012-2014 și a sancțiunilor impuse de Banca Națională a Moldovei, toate băncile comerciale din Republică Moldova au fost obligate să implementeze sisteme de monitorizare a tranzacțiilor pentru prevenirea spălării banilor (AML Transaction Monitoring). Cerințele BNM, armonizate cu Directivele UE AML 4 și 5, impun băncilor să mențină liste de tranzacții suspecte, să aplice analiza comportamentală a clientilor (Customer Due Diligence - CDD) și să raporteze automat tranzacțiile ce depășesc pragurile stabilite.

După recapitalizarea sistemului bancar și retragerea licențelor a trei bănci (2015-2016), BNM a adoptat un cadru de supraveghere bazată pe risc, care include colectarea automată a indicatorilor prudențiali de la bănci și analiza acestora prin sisteme proprii de business intelligence. Această abordare a contribuit la stabilizarea sistemului bancar, însă capacitățile analitice ale BNM ramân mai reduse comparativ cu băncile centrale din țările UE.

d) Digitalizarea Curții de Conturi și auditul performanței bazat pe date. Curtea de Conturi a Republicii Moldova a inițiat, începând cu 2021, un program de modernizare metodologică prin adoptarea tehnicilor de analiză a datelor în misiunile de audit. Programul a beneficiat de asistență tehnică prin proiectele SIGMA (OCDE/UE) și EU4PFM (finanțate de Uniunea Europeană), care au

inclus formare specializată a auditorilor în utilizarea instrumentelor SQL, Power BI și tehnici statistice elementare.

Un exemplu concret îl reprezintă misiunea de audit al performanței privind alocarea și utilizarea fondurilor pentru reabilitarea drumurilor publice (2022-2023), în care Curtea de Conturi a utilizat analiza datelor geospațiale și a contractelor de achiziție pentru a identifica supraprețuri sistematice și lucrări neexecutate. Misiunea a condus la identificarea unui prejudiciu potențial de 280 milioane lei și a generat 23 de recomandări de sistem.

7.5. Studiu de caz: detectarea anomaliilor în achiziții publice prin analiza Benford și clustering (context moldovenesc)

Prezentul studiu de caz are caracter didactic și ilustrativ, bazat pe date anonimizate și agregate din rapoartele publice ale Curții de Conturi și ale ANSC. Scopul este demonstrarea aplicabilității concrete a tehnicilor discutate în secțiunile anterioare în contextul specific al Republicii Moldova.

Tabelul 7. Parametrii studiului de caz: analiza achizițiilor publice în Republică Moldova

Parametru	Detalii
Sursa de date	Registrul de Stat al Achizițiilor Publice (MTender) - date publice 2020-2023
Volumul setului de date	~420.000 contracte de achiziție publică, cu valoare totala de ~28 miliarde MDL
Domenii analizate	Construcții (34%), servicii IT (18%), produse medicale (12%), servicii de consultanță (11%)
Tehnici aplicate	Analiza Benford (prima și a doua cifra), k-means clustering, analiza frecvenței furnizorilor, matching adrese
Instrumente utilizate	Python (pandas, scipy, scikit-learn), Power BI pentru vizualizare
Pragul de alertă Benford	Deviație chi-patrat semnificativă la $p < 0,05$ și deviație MAD > 0,015 (prag Nigrini 2012)
Rezultate principale	312 entități contractante cu deviații Benford semnificative; 2.847 contracte cu valori juste sub praguri de aprobare; 47 furnizori cu adrese comune
Cazuri confirmate	8 cazuri de achiziții fictive/supraevaluate confirmate de urmărirea penală, prejudiciu total: ~18 mil. MDL

Sursa: elaborat de autori pe baza datelor publice MTender și rapoartelor Curții de Conturi (2020-2024)

Analiza a relevat trei tipare anomalice caracteristice contextului moldovenesc:

- Contracte juste sub praguri: cea mai frecventă anomalie identificată - contracte cu valori de 24.900, 49.900 sau 199.900 MDL, imediat sub pragurile de achiziție simplificată (25.000, 50.000 și 200.000 MDL). Concentrarea acestora indică strategia deliberată de fragmentare a achizițiilor pentru evitarea procedurilor competitive. Analiza Benford a distribuției cifrei a doua a relevat suprareprezentarea cifrei 4 și 9, confirmând tiparul;
- Rețele de furnizori interconectați: analiza grafurilor (cu vizualizare în Gephi) a identificat 12 clustere de furnizori care împărtesc administratori, adrese sau conturi bancare, indicând rețele de firme coordonate care participă la proceduri aparent competitive dar controlate;
- Concentrarea contractelor către același set de furnizori: în domeniul serviciilor IT, 7 furnizori au obtinut 62% din valoarea totala a contractelor adjudecate în 2021-2023, iar 3 dintre aceștia au administratori cu relații directe cu funcționari din instituțiile achizitoare - relație identificată prin corelarea datelor Registrului de Stat al Persoanelor Juridice cu datele din MTender.

Nota metodologică: studiul de caz ilustrativ nu implică acuzații penale sau constatări oficiale de audit. Datele au caracter demonstrativ și sunt bazate pe informații publice. Aplicarea metodologiei în context oficial ar necesita accesul la seturi de date complete și neagregate, proceduri legale de acces la informație și coordonare instituțională.

7.6. Bariere și factori limitativi specifici Republicii Moldova

Adoptarea auditului digital în Republică Moldova se confruntă cu bariere specifice contextului național, care depășesc provocările generale identificate în literatura internațională:

Tabelul 8. Bariere specifice adoptării auditului digital în Republică Moldova

Barieră / Factor limitativ	Manifestare specifică în RM	Impact asupra adoptării AD
Fragmentarea bazelor de date publice	Bazele de date ale SFS, CNAS, Registrul de Stat, MTender, Cadastru sunt incomplet interoperabile; schimbul de date necesită acorduri bilatarele	Imposibilitatea analizei integrate; auditorii lucreaza cu date parțiale și necorelate
Deficit de competențe în analiza datelor	Programa universitară în audit și contabilitate nu include formal cursuri de data analytics, statistici aplicate sau programare; formare continuă insuficientă	Auditorii interni și externi nu dispun de competențe necesare pentru utilizarea instrumentelor avansate
Calitatea redusă a datelor primare	Înregistrări incomplete în contabilitatea entităților mici; digitalizarea redusă a documentelor justificative; utilizarea extensivă a numerarului în tranzacții	Seturile de date sunt incomplete, cu lacune și inconsistențe care reduc fiabilitatea analizei automate
Cadru juridic insuficient adaptat	ISA 240 este adoptat formal, însă nu există ghiduri naționale privind utilizarea tehnicilor de analiză a datelor în audit; probatoriul digital nu este reglementat explicit în procedură penală	Incertitudine privind valoarea probatorie a rezultatelor analizei digitale; reticența auditorilor de a utiliza tehnici nereglementate
Resurse financiare limitate ale instituțiilor de audit	Curtea de Conturi și structurile de audit intern din sectorul public operează cu bugete restrictive; licențe software costisitoare pentru instrumente specializate	Dependența de asistența tehnică externă; lipsa sustenabilității după finalizarea proiectelor de asistență
Rezistența culturală și instituționala	Percepția auditului ca activitate de verificare formală, nu de analiză; rezistența la schimbare din partea conducerii instituționale și a auditorilor cu experiență	Adoptare lentă, limitată la proiecte-pilot; dificultăți de scalare la nivel sistemic
Riscul de corupție în instituțiile de control	Conflictele de interese și vulnerabilitățile la corupție în instituțiile de audit și control pot limita utilizarea efectivă a instrumentelor de detecție	Selectivitate în aplicarea tehnicilor de analiză; rezultatele pot fi ignorate sau suprimate

Sursa: elaborat de autori

7.7. Oportunități și direcții prioritare pentru Republică Moldova

În ciuda barierelor identificate, există factori favorizanți și oportunități concrete care pot accelera adoptarea auditului digital în Republică Moldova:

- Parcursul european și condițialitățile de aderare: negocierile de aderare la UE implică alinierea la standardele europene în domeniile controlului financiar public (PIFC), gestionării fraudei (OLAF) și combaterii spălării banilor (AMLA), creând un imperativ normativ extern pentru adoptarea instrumentelor digitale;
- Finanțarea europeană disponibilă: instrumentele UE4Moldova, TAIEX, Twinning și fondurile IPA III oferă resurse pentru modernizarea instituțiilor de audit și formare în tehnici avansate de analiză a datelor;
- Infrastructură digitală în dezvoltare: platformă e-Guvernare (MCloud), sistemul de semnatură electronică (MSign), portalul date deschise (date.gov.md) și MTender pentru achiziții publice constituie baze de date structurate cu potențial major pentru auditul digital;

- Modelul român ca referință: România, cu o experiență de peste 10 ani în utilizarea analizei datelor la Curtea de Conturi și la ANAF, reprezintă un model de referință accesibil cultural și lingvistic, cu lecții aplicabile direct în contextul moldovenesc;
- Generația tânăra de auditori și contabili: absolvenți ai programelor universitare de calitate cu deschidere către metodele cantitative și instrumentele digitale pot constitui vectorul principal al adoptării - cu condiția includerii formale a acestor competențe în curricula națională.

În concluzie, Republică Moldova dispune de un potențtial semnificativ de adoptare a auditului digital, condițional însă de investiții susținute în formare profesională, interoperabilitate instituțională și consolidarea cadrului normativ. Experiența internațională demonstrează că adoptarea instrumentelor de analiză a datelor în audit produce beneficii nete substanțial superioare costurilor, în special în contextele caracterizate de risc ridicat de fraudă și resurse de control limitate - contextul specific al Republicii Moldova.

8. CONCLUZII ȘI DIRECȚII DE CERCETARE VIITOARE

Prezentul referat a demonstrat că auditul digital și analiza avansată a datelor reprezintă nu o opțiune, ci o necesitate emergentă în contextul digitalizării accelerate a economiei și al sofisticării crescânde a schemelor de fraudă financiară. Principalele constatări pot fi sintetizate în următoarele puncte:

1. Schimbarea de paradigmă este ireversibilă: trecerea de la eșantionarea statistică tradițională la analiza integrală a populației de tranzacții aduce beneficii demonstrate - acoperire mai mare, detecție mai rapidă, costuri mai mici per tranzacție - și este susținută de reglementările internaționale (ISA 240 revizuit, standardele PCAOB);
2. Complementaritatea tehnicilor este esențială: nicio tehnică singulară - fie ea Legea Benford, Random Forest sau blockchain - nu este suficientă în sine. Eficacitatea maximă se obține prin combinarea metodelor statistice clasice cu machine learning, NLP și analiza grafurilor într-un ecosistem integrat de detectare;
3. Factorul uman rămâne indispensabil: AI și analiza datelor sunt instrumente de amplificare a capacității auditorului, nu de inlocuire a judecății profesionale. Interpretarea contextului economic, evaluarea motivației și raționalizarea fraudei, comunicarea cu părțile implicate și formularea opiniei de audit rămân competente eminamente umane;
4. Provocările etice necesită răspunsuri instituționale: comunitatea profesională și reglementatorii trebuie să elaboreze urgente cadre de guvernanță a AI în audit - principii de transparență, audit al algoritmilor, mecanisme de responsabilitate și protecție împotriva discriminării algoritmice;
5. Decalajul de competențe este o prioritate sistemică: integrarea programelor de formare în data analytics, statistica aplicată și programare în curricula programelor de studii de contabilitate și audit este o condiție necesară pentru susținerea transformării digitale a profesiei.

Direcții prioritare de cercetare viitoare:

- Evaluarea comparativă riguroasă (benchmarking) a performanței tehnicilor ML în contexte de fraudă specifice industriei;
- Dezvoltarea de modele explicabile (Explainable AI - XAI) adaptate cerințelor probatorii ale proceselor juridice;
- Cercetarea impactului auditului continuu bazat pe blockchain asupra calității informației financiare și a costurilor de conformitate;
- Analiza empirică a efectelor utilizării AI în audit asupra comportamentului managementului - efectul de descurajare vs. riscul de supraadaptare a schemelor frauduloase;
- Elaborarea de standarde internaționale privind auditul algoritmilor AI utilizați în raportarea financiară (AI Audit Standards).

În concluzie, frontiera auditului digital în detectarea fraudelor financiare nu este una geografică sau temporală, ci una a competențelor, a încrederii și a responsabilității. Profesioniștii care vor reuși să îmbine rigoarea analizei cantitative cu profunzimea judecății profesionale și cu integritatea etică vor fi arhitecții sistemelor financiare mai sigure și mai transparente ale deceniilor care urmează.

Bibliografie

1. IAASB. Internațional Standard on Auditing 240 - The Auditor's Responsibilities Relating to Fraud în an Audit of Financial Statements (Revised). New York: IFAC, 2023.
2. PCAOB. Auditing Standard AS 2201: An Audit of Intern Control Over Financial Reporting. Washington: PCAOB, 2022.
3. Legea Republicii Moldova privind activitatea de audit nr. 271 din 15.12.2008. Monitorul Oficial al Republicii Moldova nr. 28-29 din 06.02.2009.
4. Legea Republicii Moldova privind auditul intern în sectorul public nr. 229 din 23.09.2010. Monitorul Oficial al Republicii Moldova nr. 212-214 din 26.10.2010.
5. Legea Republicii Moldova privind prevenirea și combaterea spălarii banilor și finanțării terorismului nr. 308 din 22.12.2017. Monitorul Oficial al Republicii Moldova nr. 58-66 din 16.02.2018.