CZU: 343.98:004.738.5:004.93:61

DOI: https://doi.org/10.5281/zenodo.18680779

VIDEOCLIPURILE DEEPFAKE DIN DOMENIUL SĂNĂTĂȚII, SUBIECT DE ANALIZĂ CRIMINALISTICĂ

Constantin PISARENCO [1]

Dezvoltarea rapidă a rețelelor neuronale generative a dat naștere fenomenului deepfake-urilor – înregistrări audio și video sintetice care sunt practic imposibil de distins de cele reale. În domeniul medical, astfel de substituții pot dezorienta pacienții și medicii, pot masca erori medicale, pot falsifica consultațiile de telemedicină și pot crea dovezi false. Acest articol oferă o analiză criminalistică a videoclipurilor deepfake și explorează provocările juridice și tehnologice ale detectării acestora. Bazat pe o analiză comparată a legislației și a metodelor moderne de criminalistică digitală, articolul examinează indicatorii vizuali, audiovizuali și digitali ai falsificării, amenințările la adresa fiabilității probelor și nevoia sectorului medical de noi protocoale de autentificare. De asemenea, se susține necesitatea armonizării internaționale a cerințelor de etichetare, a dezvoltării de seturi de date specializate în scopuri medicale, a implementării tehnologiilor blockchain în lanțul de evidență a probelor și a formării interdisciplinare a experților.

Cuvinte-cheie: deepfake, dovezi digitale, telemedicină, criminalistică, drept medical, examinare digitală.

DEEPFAKE VIDEOS IN THE HEALTHCARE FIELD, SUBJECT OF CRIMINALISTIC ANALYSIS

Constantin PISARENCO [1]

The rapid development of generative neural networks has given rise to the phenomenon of deepfakes—synthetic audio and video recordings that are virtually indistinguishable from the real thing. In the medical field, such substitutions can confuse patients and doctors, mask medical errors, falsify telemedicine consultations, and create false evidence. This article provides a forensic analysis of deepfake videos and explores the legal and technological challenges of detecting them. Based on a comparative analysis of legislation and modern digital forensics methods, the article examines visual, audiovisual, and digital indicators of falsification, threats to the reliability of evidence, and the medical sector's need for new authentication protocols. It also argues for the need for international harmonization of labeling requirements, the development of specialized datasets for medical purposes, the implementation of blockchain technologies in the evidence chain, and interdisciplinary training of experts.

Keywords: deepfake, digital evidence, telemedicine, forensics, medical law, digital examination.

INTRODUCERE

Termenul „*deepfake*” a apărut la sfârșitul anilor 2010 pentru a descrie o nouă generație de media sintetică bazată pe învățarea automată profundă. Se referă la fotogtafii, conținuturi audio și video create sau modificate artificial, care imită persoane și evenimente reale. Legislația europeană consacră această definiție: conținutul deepfake este reprezentat de imagini fotografice, audio și video generate sau modifi-

INTRODUCTION

The term „*deepfake*” emerged in the late 2010s to describe a new generation of synthetic media based on deep machine learning. It refers to artificially created or modified audio, photo, and video content that mimics real people and events. European legislation enshrines this definition: deepfake content is represented by images, audio, and video generated or modified

[1] Conferențiar universitar, doctor în drept, Catedra „Drept public”, Universitatea Liberă Internațională din Moldova; e-mail: office@ulim.md, ulim@ulim.md; e-mail: constantin.pisarenco@gmail.com; ORCID ID: https://orcid.org/0000-0001-5548-4653

Associate Professor, Doctor of Law, Department of Public Law, Free International University of Moldova; e-mail: office@ulim.md, ulim@ulim.md; e-mail: constantin.pisarenco@gmail.com; ORCID ID: https://orcid.org/0000-0001-5548-4653

cate de inteligență artificială, care seamănă cu persoane, obiecte sau evenimente reale și sunt percepute ca fiind autentice [21]. Algoritmii moderni ai rețelelor neuronale permit modificarea aspectului și a expresiilor faciale ale unei persoane, sincronizarea vorbirii și a imaginilor sau clonarea unei voci folosind un set de date sursă foarte limitat. Inițial, un astfel de conținut deepfake conținea artefacte rudimentare, dar îmbunătățirea rapidă a generatoarelor, disponibilitatea bibliotecilor open source și a serviciilor comerciale a avut drept consecință distribuirea în masă a videoclipurilor deepfake de înaltă calitate. Ca urmare, chiar și observatorii experimentați au dificultăți în detectarea lor [28].

Industria medicală s-a dovedit a fi unul dintre cele mai vulnerabile sectoare. Jurnaliștii au raportat că escrocii folosesc videoclipuri false cu medici cunoscuți datorită TV pentru a face publicitate la medicamente dubioase, iar aproximativ jumătate dintre telespectatori nu detectează substituția [31]. Au apărut cazuri de „clonare" a specialiștilor în telemedicină: escrocii creează conturi false ale medicilor sau pacienților, efectuează consultații fictive și extorchează plăți [30]. În Moldova au fost raportate atacuri telefonice în care escrocii, folosind o voce sintetizată, i-au convins pe cetățeni să transfere fonduri, dându-se drept rude [20].

La nivel internațional, în 2024, Parlamentul European a aprobat Regulamentul privind inteligența artificială (Legea IA), care introduce etichetarea obligatorie a materialelor audio, fotografice și video sintetice, clasificând aplicațiile IA în funcție de nivelurile de risc [12]. Organizația pentru Cooperare și Dezvoltare Economică (OCDE) a propus principii valorice pentru o IA responsabilă, bazată pe transparență, securitate și respectarea drepturilor omului [23]. Convenția de la Budapesta privind criminalitatea cibernetică subliniază necesitatea cooperării internaționale pentru colectarea și schimbul de probe electronice [7].

Alegerea domeniului medical este determinată nu doar de creșterea telemedicinii și de digitalizarea serviciilor medicale,

by artificial intelligence that resemble real people, objects, or events and are perceived as authentic [21]. Modern neural network algorithms allow the modification of a person's appearance and facial expressions, the synchronization of speech and images, or the cloning of a voice using a very limited source data set. Initially, such deepfake content contained rudimentary artifacts, but rapid improvements in generators and the availability of open-source libraries and commercial services have led to the mass distribution of high-quality deepfake videos. As a result, even experienced observers have difficulty detecting them [28].

The medical industry has proven to be one of the most vulnerable sectors. Journalists have reported that scammers use fake videos of well-known doctors from television to advertise dubious drugs; about half of viewers do not detect the substitution [31]. There have been cases of "cloning" of telemedicine specialists: scammers create fake accounts of doctors or patients, conduct fictitious consultations, and extort payments [30]. In Moldova, there have been reports of telephone attacks in which fraudsters, using a synthesized voice, have convinced citizens to transfer funds by posing as relatives [20].

At the international level, in 2024, the European Parliament approved the Artificial Intelligence Regulation (AI Law), which introduces mandatory labeling of synthetic audio, photo, and video s and classifies AI applications according to risk levels [12]. The Organization for Economic Cooperation and Development (OECD) has proposed value-based principles for responsible AI, based on transparency, security, and respect for human rights [23]. The Budapest Convention on Cybercrime emphasizes the need for international cooperation in the collection and exchange of electronic evidence [7].

The choice of the medical field is determined not only by the growth of telemedicine and the digitization of medical

ci și de importanța publică deosebită a datelor medicale. Înlocuirea înregistrărilor video ale operațiilor chirurgicale, autopsiilor medico-legale sau consultațiilor medicale poate duce la diagnostice false, ascunderea erorilor medicale, fraudă în asigurări și încălcarea confidențialității pacient-medic. Articolul examinează videoclipurile deepfake ca formă de probă digitală și examinează indicatorii medico-legali ai acestor falsificări și metodele de detectare a acestora într-un context medical.

Scopul studiului este de a identifica semnele, riscurile și abordările metodologice pentru identificarea falsificărilor video ale rețelelor neuronale (videoclipuri deepfake) în domeniul investigării infracțiunilor și încălcărilor din domeniul medical.

METODE ȘI MATERIALE APLICATE

A fost realizată o analiză comparativă a legislațiilor Republicii Moldova, Uniunii Europene și Statelor Unite privind admisibilitatea probelor digitale și reglementarea conținutului deepfake. Au fost utilizate metode criminalistice (fotografice și video, computerizate și fonografice) și metode de examinare digitală (analiza metadatelor, secvențelor GOP și coerenței semnalelor audio și video). Pentru a evalua eficacitatea detectoarelor, au fost studiate seturi de date moderne de la DFDC [11], MedForensics [15] și studii privind analiza fiziologică, inclusiv fotopletismografia la distanță (rPPG) [28]. Baza empirică a constat în exemple de abuz cu aplicarea tehnologiilor deepfake, înregistrate în mass-media și în actele de reglementare. De asemenea, au fost utilizate metode analitice descriptive și analiza de conținut.

DISCUȚII ȘI REZULTATE OBȚINUTE

Transformarea digitală a proceselor judiciare a făcut din datele electronice o sursă importantă de probe. Convenția de la Budapesta recunoaște datele electronice ca un subiect cheie al cooperării internaționale și impune statelor să dezvolte proceduri pentru colectarea, stocarea și schimbul acestora [7].

services, but also by the particular public importance of medical data. Replacing video recordings of surgical operations, forensic autopsies, or medical consultations can lead to false diagnoses, concealment of medical errors, insurance fraud, and violation of patient-doctor confidentiality. The article examines deepfake videos as a form of digital evidence and examines the forensic indicators of these fakes and methods for detecting them in a medical context.

The aim of the study is to identify the signs, risks, and methodological approaches for identifying neural network video forgeries (deepfake videos) in the investigation of crimes and violations in the medical field.

METHODS AND MATERIALS APPLIED

A comparative analysis of the legislation of the Republic of Moldova, the European Union, and the United States on the admissibility of digital evidence and the regulation of deepfake content was carried out. Forensic methods (photo and video, computerized and phonographic) and digital examination methods (analysis of metadata, GOP sequences, and audio and video signal coherence) were used. To evaluate the effectiveness of detectors, modern datasets from DFDC [11], MedForensics [15], and studies on physiological analysis, including remote photoplethysmography (rPPG) [28], were studied. The empirical basis consisted of examples of deepfake technology abuse recorded in the media and regulatory documents. Content analysis and descriptive analytical methods were used.

DISCUSSIONS AND RESULTS OBTAINED

The digital transformation of judicial processes has made electronic data an important source of evidence. The Budapest Convention recognizes electronic data as a key subject of international cooperation and requires states to develop procedures

Literatura juridică face distincție între „falsificări complexe" – acele materiale audio, fotografice și video atent elaborate, create folosind abilități profesionale (modelare 3D, efecte speciale, compoziție) fără utilizarea inteligenței artificiale. „Falsificările profunde" (deepfakes) sunt un subtip specific de falsificări complexe: acestea sunt create folosind rețele neuronale generative care înlocuiesc automat fețele sau vocile. The European Union's AI regulation (the „AI Act") definește un deepfake ca o imagine, un fișier audio sau un videoclip generat sau modificat de inteligența artificială care imită persoane sau evenimente reale și este perceput ca fiind autentic [27].

Normele internaționale iau din ce în ce mai mult în considerare specificul deepfake-urilor. The European Union's AI regulation (the „AI Act") stabilește o clasificare bazată pe risc a sistemelor de IA și impune dezvoltatorilor și distribuitorilor să eticheteze conținutul sintetic [12] [27]. Principiile OCDE privind IA solicită transparență, corectitudine și responsabilitate în dezvoltarea și implementarea algoritmilor, precum și crearea de mecanisme de combatere a dezinformării [23]. În Statele Unite, potrivit Conferinței Naționale a Adunărilor Legislative, peste patruzeci de state au adoptat legi care interzic diseminarea mass-media înșelătoare, în special în perioadele electorale [22].

Jurisdicțiile vorbitoare de limbă engleză discută modificări ale regulilor procedurale. Conferința Judecătorilor Federali din Statele Unite are în vedere adăugarea unei noi subsecțiuni la Regula 901 din Regulile Federale privind Probele, 901(c), care ar impune judecătorilor să verifice în prealabil autenticitatea materialelor generate de inteligența artificială înainte de a fi prezentate juraților [10]. Doctrina juridică propune înăsprirea criteriilor de autentificare, înlocuirea termenilor „exactitate" cu „valid" și „fiabil" și organizarea de audieri preliminare în timpul cărora judecătorii evaluează valoarea probatorie și potențialele daune ale probelor false [17] [19].

Moldova ia, de asemenea, măsuri pentru a-și consolida infrastructura juridică.

for its collection, storage, and exchange [7].

Legal literature distinguishes between „complex fakes" — carefully crafted audio, photo, and video materials created using professional skills (3D modeling, special effects, composition) without the use of artificial intelligence. „Deepfakes" are a specific subtype of complex fakes: they are created using generative neural networks that automatically replace faces or voices. The European Union's AI regulation (the „AI Act") defines a deepfake as an image, audio file, or video generated or modified by artificial intelligence that mimics real people or events and is perceived as authentic [27].

International standards are increasingly taking into account the specific nature of deepfakes. The European Union's AI regulation (the „AI Act") establishes a risk-based classification of AI systems and requires developers and distributors to label synthetic content [12] [27]. The OECD principles on AI call for transparency, fairness, and accountability in the development and implementation of algorithms, as well as the creation of mechanisms to combat misinformation [23]. In the United States, according to the National Conference of Legislative Assemblies, more than forty states have passed laws prohibiting the dissemination of misleading media, particularly during election periods [22].

English-speaking jurisdictions are discussing changes to procedural rules. The United States Conference of Federal Judges is considering adding a new subsection to Rule 901 of the Federal Rules of Evidence, 901(c), which would require judges to verify in advance the authenticity of materials generated by artificial intelligence before they are presented to jurors [10]. The legal doctrine proposes tightening the criteria for authentication, replacing the terms „accuracy" with „valid" and „reliable", and organizing preliminary hearings during which judges assess the probative value and potential harm of false evidence [17][19].

În 2025, la Chișinău a avut loc o sesiune de instruire în cadrul proiectului CyberEast +, unde reprezentanți ai organelor de drept și ai centrelor de răspuns la incidente informatice au discutat despre standarde unificate pentru colectarea, prelucrarea și analiza probelor electronice, propunând standardizarea interacțiunilor dintre CSIRT-uri și autoritățile judiciare [8]. Aceste inițiative reflectă angajamentul Republicii Moldova de a integra probele digitale, inclusiv videoclipurile deepfake, în normele procedurale bazate pe experiența europeană.

Tehnologiile deepfake moderne au apărut în urma cercetărilor în domeniul modelelor generative: de la autoencodere și rețele generative adverse (GAN) la modele de difuzie. Aceste sisteme sunt antrenate pe seturi masive de date și învață tipare subtile de expresii faciale, iluminare și vorbire, permițându-le să creeze falsuri convingătoare care imită nu numai trăsăturile feței, ci și limbajul corpului și intonația caracteristice. Democratizarea acestor instrumente prin intermediul bibliotecilor open source și al aplicațiilor comerciale a făcut tehnicile deepfake accesibile răufăcătorilor. Prin urmare, știința criminalistică este forțată să se adapteze la un nou tip de obiect: fișierele deepfake sunt simultan documente digitale care necesită lanț de custodie și înregistrări audiovizuale care au nevoie de analiză video și fonografică [13].

Principalii markeri utilizați pentru identificarea deepfake-urilor sunt împărțiți în mod convențional în vizuali, audiovizuali, digitali și biometrici. Analiza vizuală include o evaluare a modelelor de lumină și umbră și a microexpresiilor; chiar și cele mai avansate modele fac uneori greșeli de reproducere a luminii, ceea ce duce la străluciri neobișnuite, umbre nenaturale și tranziții neuniforme ale nuanței pielii. Experții observă un număr insuficient de clipiri și rigiditate facială, în timp ce metodele de fotopletismografie la distanță (rPPG) arată că variațiile locale ale fluxului sanguin în deepfake-uri sunt incorecte [28]. Inconsecvențele audiovizuale apar din cauza sincronizării imperfecte a vorbirii și a expresiilor faciale: algoritmii

Moldova is also taking steps to strengthen its legal infrastructure. In 2025, a training session was held in Chișinău as part of the CyberEast+ project, where representatives of law enforcement agencies and computer incident response centers discussed unified standards for the collection, processing, and analysis of electronic evidence, proposing the standardization of interactions between CSIRTs and judicial authorities [8]. These initiatives reflect the Republic of Moldova's commitment to integrating digital evidence, including deepfake videos, into procedural rules based on European experience.

Modern deepfake technologies have emerged from research in generative modeling: from autoencoders and generative adversarial networks (GANs) to diffusion models. These systems are trained on massive datasets and learn subtle patterns of facial expressions, lighting, and speech, allowing them to create convincing fakes that mimic not only facial features but also characteristic body language and intonation. The democratization of these tools through open-source libraries and commercial applications has made deepfake techniques accessible to criminals. As a result, forensic science is forced to adapt to a new type of object: deepfake files are simultaneously digital documents requiring chain of custody and audiovisual recordings requiring video and phonographic analysis [13].

The main markers used to identify deepfakes are conventionally divided into visual, audiovisual, digital, and biometric. Visual analysis includes an assessment of light and shadow patterns and microexpressions; even the most advanced models sometimes make mistakes in reproducing light, resulting in unusual glare, unnatural shadows, and uneven skin tone transitions. Experts observe insufficient blinking and facial rigidity, while remote photoplethysmography (rPPG) methods show that local blood flow variations in deepfakes are in-

omit adesea detalii despre dicție, melodie și pauzele respiratorii, astfel încât analiza intervalelor de articulare și de sincronizare ajută la identificarea discrepanțelor; cadrele audiovizuale dedicate demonstrează o precizie ridicată în potrivirea mișcărilor buzelor cu vorbirea [26].

Caracteristicile digitale sunt legate de structura internă a fișierului: recodificarea lasă urme în secvențele GOP, codecuri și timestamp-uri. Standardele internaționale ISO/IEC 27037 și 27050 impun înregistrarea acestor parametri și a fiecărei operațiuni pe fișier pentru a permite verificarea ulterioară [13]. Indicatorii biometrici constituie un grup special: pe lângă rPPG, sunt studiate frecvența și amplitudinea clipirilor, microvibrațiile musculare, modificările diametrului pupilei și reacțiile fiziologice asociate cu emoțiile [28].

Astfel, tehnologiile deepfake extind posibilitățile de creare a unor medii sintetice, dar în același timp le transformă într-un subiect complex de analiză criminalistică. Natura hibridă a unor astfel de fișiere necesită o sinteză a metodelor criminalistice informatice, video , audio și lingvistice; nicio disciplină singulară nu poate oferi o imagine completă a originii și autenticității.

Videoclipurile deepfake ocupă un loc unic în sistemul obiectelor criminalistice. Acestea moștenesc proprietățile echipamentelor video, deoarece necesită analiza imaginilor, luminii, umbrelor și dinamicii faciale, în același timp fiind fișiere cărora li se aplică metode criminalistice informatice: studiul codecurilor, metadatelor și structurii GOP. Componentele audio și text necesită analiza lingvistică a timbrului, dicției și sincronizării vorbirii. În cele din urmă, trasologia digitală studiază „urmele" – valori hash, timestamp-uri și jurnalele de rețea care înregistrează istoricul manipulării fișierelor. Complexitatea obiectului implică faptul că fiabilitatea unui videoclip deepfake poate fi confirmată doar printr-o sinteză a constatărilor specialiștilor în echipamente video, sunet, infrastructură IT și drept.

Medicina se bazează pe cantități vaste de informații audiovizuale: înregistrări ale

correct [28]. Audiovisual inconsistencies arise due to imperfect synchronization of speech and facial expressions: algorithms often omit details about diction, melody, and breathing pauses, so analysis of articulation and synchronization intervals helps identify discrepancies; Dedicated audiovisual frames demonstrate high accuracy in matching lip movements to speech [26].

Digital characteristics are related to the internal structure of the file: recoding leaves traces in GOP sequences, codecs, and timestamps. International standards ISO/IEC 27037 and 27050 require the recording of these parameters and the logging of each operation on the file to allow for subsequent verification [13]. Biometric indicators constitute a special group: in addition to rPPG, the frequency and amplitude of blinks, muscle microvibrations, changes in pupil diameter, and physiological reactions associated with emotions are studied [28].

Thus, deepfake technologies expand the possibilities for creating synthetic environments, but at the same time turn them into a complex subject of forensic analysis. The hybrid nature of such files requires a synthesis of computer, video, audio, and linguistic forensic methods; no single discipline can provide a complete picture of origin and authenticity.

Deepfake videos occupy a unique place in the system of forensic objects. They inherit the properties of video equipment, as they require analysis of images, light, shadows, and facial dynamics, and at the same time, they are files to which computer forensic methods are applied: the study of codecs, metadata, and GOP structure. Audio and text components require linguistic analysis of timbre, diction, and speech synchronization. Finally, digital trasology studies „traces" — hash values, timestamps, and network logs that record the history of file manipulation. The complexity of the subject implies that the reliability of a deepfake video can only be

intervențiilor chirurgicale, consultațiilor, diagnosticelor și examinărilor medico-legale. Proliferarea modelelor generative prezintă o gamă largă de amenințări. Revista BMJ a remarcat că escrocii au creat reclame cu „doctori" pentru a promova medicamente dubioase și că o parte semnificativă a telespectatorilor nu a reușit să distingă falsurile de consultațiile reale [31]. În telemedicină, infractorii creează conturi false de medici sau pacienți, programează consultații online și extorchează plăți; experții recomandă ca profesioniștii din domeniul sănătății să verifice datele biometrice ale persoanei cu care vorbesc, să compare informațiile pe mai multe canale și să utilizeze platforme securizate [30]. Avertismentele publice din partea autorităților moldovene evidențiază desincronizarea buzelor și a vocii, expresiile faciale dure și pauzele ciudate ca semne de deepfake [20].

O problemă separată este ascunderea erorilor medicale și a fraudei în asigurări: videoclipurile chirurgicale modificate pot ascunde acțiuni reale sau, dimpotrivă, pot înscena leziuni pentru a obține despăgubiri. În sfera publică, falsificările extinse care implică uzurparea identității medicilor sau politicienilor pot submina încrederea în instituțiile medicale și în sistemul de sănătate. Falsificarea înregistrărilor chirurgicale pentru a ascunde neglijența, uzurparea identității unui medic sau pacient în timpul consultațiilor online, crearea de videoclipuri false despre rezultatele studiilor clinice de succes, simularea procedurilor sau falsificarea rapoartelor video ale autopsiei.

Accesibilitatea instrumentelor generative este sporită de faptul că cetățenii adesea nu au abilitățile tehnice necesare pentru a verifica sursa unui videoclip și pentru a avea încredere în orice dovadă vizuală. Prin urmare, consolidarea încrederii în dovezile digitale în medicină și creșterea alfabetizării digitale în rândul populației sunt deosebit de importante.

Abordările moderne de detectare a deepfake-urilor sunt împărțite în tradiționale (pasive) și tehnice (active). Dezvoltarea lor este determinată de fap-

confirmed by a synthesis of the findings of specialists in video equipment, sound, IT infrastructure, and law.

Medicine relies on vast amounts of audiovisual information: recordings of surgeries, consultations, diagnoses, and forensic examinations. The proliferation of generative models poses a wide range of threats. The BMJ magazine noted that scammers have created advertisements featuring „doctors" to promote dubious drugs and that a significant proportion of viewers were unable to distinguish the fakes from real consultations [31]. In telemedicine, criminals create fake accounts for doctors or patients, schedule online consultations, and extort payments; experts recommend that healthcare professionals verify the biometric data of the person they are talking to, compare information across multiple channels, and use secure platforms [30]. Public warnings from Moldovan authorities highlight lip and voice desynchronization, stiff facial expressions, and awkward pauses as signs of deepfakes [20].

A separate issue is the concealment of medical errors and insurance fraud: edited surgical videos can hide real actions or, conversely, stage injuries to obtain compensation. In the public sphere, widespread fakes involving the impersonation of doctors or politicians can undermine trust in medical institutions and the healthcare system. Falsifying surgical records to conceal negligence, impersonating a doctor or patient during online consultations, creating fake videos about successful clinical trial results, simulating procedures, or falsifying autopsy video reports.

The accessibility of generative tools is compounded by the fact that citizens often lack the technical skills to verify the source of a video and trust any visual evidence. Therefore, building trust in digital evidence in medicine and increasing digital literacy among the population are particularly important.

Modern approaches to detecting

tul că deepfake-urile devin din ce în ce mai realiste, iar simpla inspecție vizuală nu mai este suficientă.

Etapa de bază a analizei criminalistice rămâne indispensabilă: un specialist examinează înregistrarea video, comparând cadrele disputate cu sursele de referință, verificând continuitatea temporală, lipsa de uniformitate de editare, modificările de rezoluție, codecurile și marcajele temporale. Abordările timpurii s-au concentrat pe artefacte spațiale evidente – modele neregulate de pixeli, nepotriviri de iluminare și umbre. Verificarea metadatelor (marcaje temporale, structuri GOP, codecuri) dezvăluie cazuri de recodificare, adesea folosite pentru a ascunde urme de generare. Expertul acordă atenție, de asemenea, desincronizării buzelor și vocii, imaginilor statice de fundal și estompării imaginii. Cu toate acestea, metodele tradiționale se confruntă cu limitări: ochiul uman nu poate detecta inconsecvențe microscopice, iar falsificările care au suferit mai multe cicluri de compresie maschează semnele primare. Prin urmare, analiza vizuală este completată de analiza frecvenței și spectrală, care dezvăluie anomalii în distribuția frecvenței și ajută la detectarea manipulării chiar și în fișiere puternic comprimate [26].

Metodele tehnice de detectare evoluează la fel de rapid ca sistemele generative în sine. Detectoarele de uz general utilizează rețele neuronale profunde care învață reprezentările ascunse ale imaginilor și înregistrărilor video fără a se concentra pe artefacte specifice. Eficacitatea lor depinde de diversitatea datelor de antrenament: modelele antrenate pe un singur set de date nu se generalizează bine la noi tipuri de generații, așa că cercetătorii utilizează transfer learning [29]. O altă clasă de metode analizează artefactele vizuale și caracteristicile spectrale: algoritmii caută anomalii ale pixelilor, neregularități ale texturii pielii, estompare artificială și nuanțe inconsistente. Astfel de metode sunt utile pentru filtrarea inițială, dar pe măsură ce modelele generative se îmbunătățesc, defectele vizuale sunt netezite, necesitând analize

deepfakes are divided into traditional (passive) and technical (active). Their development is driven by the fact that deepfakes are becoming increasingly realistic, and simple visual inspection is no longer sufficient.

The basic stage of forensic analysis remains indispensable: a specialist examines the video recording, comparing the disputed frames with reference sources, checking for temporal continuity, editing inconsistencies, resolution changes, codecs, and timestamps. Early approaches focused on obvious spatial artifacts—irregular pixel patterns, lighting mismatches, and shadows. Verifying metadata (timestamps, GOP structures, codecs) reveals cases of recoding, often used to hide traces of generation. The expert also pays attention to lip and voice desynchronization, static background images, and image blurring. However, traditional methods face limitations: the human eye cannot detect microscopic inconsistencies, and fakes that have undergone multiple compression cycles mask the primary signs. Therefore, visual analysis is complemented by frequency and spectral analysis, which reveals anomalies in frequency distribution and helps detect manipulation even in heavily compressed files [26].

Technical detection methods are evolving as rapidly as generative systems themselves. General-purpose detectors use deep neural networks that learn the hidden representations of images and videos without focusing on specific artifacts. Their effectiveness depends on the diversity of the training data: models trained on a single dataset do not generalize well to new types of generations, so researchers use transfer learning [29]. Another class of methods analyzes visual artifacts and spectral characteristics: algorithms look for pixel anomalies, skin texture irregularities, artificial blurring, and inconsistent shades. Such methods are useful for initial filtering, but as generative models improve, visual

spectrale suplimentare și îmbunătățirea componentelor de înaltă frecvență [26].

Indicii biologici și comportamentali permit detectarea inconsecvențelor dificil de sintetizat. Metodele rPPG analizează variațiile nuanței pielii asociate cu ritmul cardiac și identifică inconsecvențele locale [28]. Analiza microvibrațiilor musculare, a frecvenței și amplitudinii clipitului, a direcției privirii și a sincronizării vorbirii cu mișcările buzelor îmbunătățește precizia detectării. Detectoarele multimodale recente combină imagini, audio și text folosind arhitecturi care combină CNN-uri, Vision Transformers și rețele temporale, obținând performanțe ridicate pe seturi de testare. Cu toate acestea, testele arată că modelele antrenate pe seturi de date academice pierd din precizie atunci când sunt expuse la dosare medicale reale; acest lucru evidențiază necesitatea actualizărilor regulate ale setului de date și a adaptării algoritmilor la noile condiții de imagistică [15].

Pe lângă detectare, integritatea lanțului de date este importantă în practica criminalistică. Utilizarea jurnalelor securizate și a registrelor blockchain înregistrează fiecare operațiune cu fișierele, prevenind modificarea nedetectată a datelor și confirmând autenticitatea înregistrării. Utilizarea blockchain-urilor private pentru înregistrările video ale intervențiilor chirurgicale și ale consultațiilor de telemedicină permite verificarea independentă și respectă standardele internaționale [13].

Implementarea metodelor descrise în domeniul sănătății necesită luarea în considerare a specificului proceselor medicale. Verificarea fiabilă a înregistrărilor video ale intervențiilor chirurgicale și autopsiilor medico-legale necesită păstrarea fluxurilor originale fără compresie, protejarea acestora cu sume hash unice și filmarea paralelă din unghiuri multiple. Astfel de înregistrări ar trebui stocate în sisteme informatice spitalicești criptate, unde fiecare acces este înregistrat într-un jurnal de evenimente. În telemedicină, persoanele rău intenționate utilizează tehnologii deepfake pentru a se da drept medici, a efectua consultații fictidefects are smoothed out, requiring additional spectral analysis and improvement of high-frequency components [26].

Biological and behavioral cues allow for the detection of inconsistencies that are difficult to synthesize. rPPG methods analyze skin tone variations associated with heart rate and identify local inconsistencies [28]. Analysis of muscle microvibrations, blink frequency and amplitude, gaze direction, and speech synchronization with lip movements improves detection accuracy. Recent multimodal detectors combine images, audio, and text using architectures that combine CNNs, Vision Transformers, and temporal networks, achieving high performance on test sets. However, tests show that models trained on academic datasets lose accuracy when exposed to real medical records; this highlights the need for regular dataset updates and adaptation of algorithms to new imaging conditions [15].

In addition to detection, data chain integrity is important in forensic practice. The use of secure logs and blockchain registries records every operation with the files, preventing undetected data modification and confirming the authenticity of the record. The use of private blockchains for video recordings of surgical procedures and telemedicine consultations allows for independent verification and complies with international standards [13].

Implementing the methods described in healthcare requires consideration of the specifics of medical processes. Reliable verification of video recordings of surgical procedures and forensic autopsies requires storing the original streams without compression, protecting them with unique hash sums, and parallel filming from multiple angles. Such recordings should be stored in encrypted hospital information systems, where each access is recorded in an event log. In telemedicine, malicious individuals use deepfake technologies to impersonate doctors, conduct fictitious consultations,

ve, a emite rețete și a obține acces la date personale; infractorii cibernetici pot adapta stilul de comunicare și jargonul medical la un anumit specialist [25] [32] [33]. Pacienții care utilizează date biometrice false ocolesc procedurile de înregistrare și primesc servicii sau fonduri în mod ilegal [33].

Pentru a contracara aceste amenințări, platformele de telemedicină trebuie să implementeze mecanisme de verificare multistratificate: identificare video în timp real, autentificare de doi factori, comparare biometrică cu bazele de date și înregistrările sesiunilor anterioare, precum și criptare obligatorie a canalelor de comunicare. În practica criminalistică, detectoarele multimodale care analizează imaginea, sunetul și textul ar trebui combinate cu metode fiziologice, cum ar fi rPPG, pentru a determina dacă circulația sângelui și micromișcările observate sunt naturale. Compararea fișierelor contestate cu înregistrările oficiale stocate în sistemele spitalicești ajută la identificarea inconsecvențelor. Companiile oferă soluții adaptate instituțiilor medicale: detectoarele locale de conținut deepfake verifică fiecare flux în timp real și nu trimit date în afara instituției, asigurând conformitatea cu cerințele HIPAA și GDPR [33]. Eficacitatea unor astfel de sisteme depinde de calitatea datelor sursă și de actualizările regulate ale algoritmilor ca răspuns la noile tipuri de falsificări.

În pofida progreselor înregistrate în recunoașterea conținutului deepfake, experții continuă să se confrunte cu provocări serioase. În primul rând, există o lipsă a unei legislații unificate și a unor standarde metodologice pentru evaluarea criminalistică a videoclipurilor digitale: standardele internaționale (ISO/IEC 27037, The European Union's AI regulation - the „AI Act") nu au fost încă integrate în sistemele juridice naționale, astfel încât experții sunt obligați să se bazeze pe documente departamentale disparate [12] [13]. În al doilea rând, mulți detectori demonstrează o precizie ridicată pe seturi de date deschise, dar își pierd eficacitatea atunci când se confruntă cu noi modele generative și scene medicale slab

issue prescriptions, and gain access to personal data; cybercriminals can adapt their communication style and medical jargon to a particular specialist [25][32][33]. Patients using false biometric data bypass registration procedures and receive services or funds illegally [33].

To counter these threats, telemedicine platforms must implement multi-layered verification mechanisms: real-time video identification, two-factor authentication, biometric comparison with databases and previous session recordings, and mandatory encryption of communication channels. In forensic practice, multimodal detectors that analyze image, sound, and text should be combined with physiological methods, such as rPPG, to determine whether the blood flow and micro-movements observed are natural. Comparing disputed files with official records stored in hospital systems helps identify inconsistencies. Companies offer solutions tailored to medical institutions: local deepfake content detectors check each stream in real time and do not send data outside the institution, ensuring compliance with HIPAA and GDPR requirements [33]. The effectiveness of such systems depends on the quality of the source data and regular updates to the algorithms in response to new types of fakes.

Despite advances in deepfake content recognition, experts continue to face serious challenges. First, there is a lack of unified legislation and methodological standards for the forensic evaluation of digital videos: international standards (ISO/IEC 27037, The European Union's AI regulation (the „AI Act")) have not yet been integrated into national legal systems, so experts are forced to rely on disparate departmental documents [12][13]. Second, many detectors demonstrate high accuracy on open datasets but lose their effectiveness when confronted with new generative models and poorly lit medical scenes. The emergence of deepfake videos with realistic

iluminate. Apariția videoclipurilor deepfake cu ritmuri realiste ale bătăilor inimii a complicat aplicarea metodelor rPPG [28]. Chiar și rețelele multimodale care combină analiza imaginilor, audio și textului se dovedesc instabile atunci când se confruntă cu secvențe chirurgicale zgomotoase sau înregistrări video de calitate scăzută. Setul limitat de date specializate rămâne o problemă serioasă: majoritatea seturilor de date cunoscute conțin actori în condiții controlate, în timp ce materialele medicale reale sunt practic indisponibile, ceea ce reduce capacitatea algoritmilor de a generaliza [15].

Problemele organizatorice și de personal prezintă nu mai puține dificultăți. O analiză cuprinzătoare a conținutului deepfake necesită o echipă care să reunească specialiști în criminalistică, medicină, învățare automată, criptografi și experți în securitate digitală. În Moldova, o astfel de sinteză a competențelor este încă rară; mulți experți criminaliști nu sunt familiarizați cu principiile de funcționare ale rețelelor generative și ale metodelor biometrice, în timp ce specialiști IT nu înțeleg întotdeauna cerințele procedurale pentru probe. Lipsa de încredere în instrumentele open source reprezintă, de asemenea, un obstacol: deși studiile arată rezultate comparabile pentru soluțiile open source atunci când se respectă procedurile de validare [13], autoritățile judiciare nu sunt întotdeauna dispuse să accepte astfel de constatări. Schimbul internațional este, de asemenea, subdezvoltat: doar o parte din evaluările experților sunt recunoscute de instanțele din alte țări în cadrul asistenței reciproce, ceea ce complică investigarea infracțiunilor transfrontaliere. Toate acestea fac relevante inițiativele de armonizare a metodologiilor și recunoaștere a standardelor internaționale în cadrul Convenției de la Budapesta și al proiectelor precum CyberEast + [7] [8].

Este necesară o abordare cuprinzătoare pentru a crește încrederea în dovezile digitale. La nivel legislativ ar trebui elaborat un standard unificat pentru criminalistica digitală, care să definească procedura de etichetare, eliminare și verificare a conținutului sintetic, precum și responsabilitatea participanților pentru ascunderea originii acestuia. Acest standard ar trebui să se bazeze pe cele internaționale.

heartbeat rhythms has complicated the application of rPPG methods [28]. Even multimodal networks that combine image, audio, and text analysis prove unstable when confronted with noisy surgical images or low-quality video recordings. The limited set of specialized data remains a serious problem: most known datasets contain actors in controlled conditions, whil ly real medical materials are virtually unavailable, which reduces the ability of algorithms to generalize [15].

Organizational and staffing issues present no fewer difficulties. A comprehensive analysis of deepfake content requires a team that brings together specialists in forensics, medicine, machine learning, cryptography, and digital security. In Moldova, such a synthesis of skills is still rare; many forensic experts are unfamiliar with the operating principles of generative networks and biometric methods, while IT specialists do not always understand the procedural requirements for evidence. Lack of trust in open-source tools is also an obstacle: although studies show comparable results for open-source solutions when validation procedures are followed [13], judicial authorities are not always willing to accept such findings. International exchange is also underdeveloped: only some expert assessments are recognised by courts in other countries in the context of mutual assistance, which complicates the investigation of cross-border crimes. All this makes initiatives to harmonize methodologies and recognize international standards under the Budapest Convention and projects such as CyberEast + [7][8] relevant.

A comprehensive approach is needed to increase confidence in digital evidence. At the legislative level, a unified standard for digital media forensics should be developed, defining the procedure for labeling synthetic content, its removal and verification, as well as the liability of participants for concealing its origin. This standard should be based on the international rec-

nalistica media digitală, care să definească procedura de etichetare a conținutului sintetic, eliminarea și verificarea acestuia, precum și răspunderea participanților pentru ascunderea originii sale. Acest standard ar trebui să se bazeze pe recomandările internaționale ISO/IEC 27037 și The European Union's AI regulation (the „AI Act") [12] [13], să fie adaptat la legislația moldovenească și să prevadă păstrarea metadatelor și a valorilor hash. De asemenea, este important să se stimuleze dezvoltarea de seturi de date medicale specializate: experiența din proiectele MedForensics arată că crearea de seturi de date care reflectă mediul clinic real îmbunătățește semnificativ calitatea clasificatorilor [15]. Astfel de baze de date ar trebui dezvoltate cu participarea instituțiilor medicale, respectând în același timp confidențialitatea și regulile etice.

Pe lângă măsurile de reglementare, este necesară implementarea unor soluții tehnice pentru controlul lanțului de custodie: registrele blockchain și contractele inteligente vor asigura transparența tranzacțiilor cu fișierele și vor verifica imutabilitatea datelor [13]. Următorul pas este crearea unor centre interdisciplinare în cadrul instituțiilor criminalistice, care să reunească avocați, criminologi, medici și specialiști IT. Îmbunătățirea alfabetizării digitale rămâne un domeniu important: programele educaționale pentru medici, pacienți și personalul tehnic ar trebui să explice cum se verifică autenticitatea videoclipurilor, ce semne indică falsificarea și ce trebuie făcut dacă se suspectează comiterea unei fraude. Odată cu dezvoltarea rapidă a modelelor generative, comunitatea științifică trebuie să fie cu un pas înaintea răufăcătorilor, propunând metode inovatoare de detectare și protecție. Un domeniu promițător este studiul caracteristicilor fiziologice locale: în timp ce generatoarele moderne de deepfake reproduc deja cu acuratețe pulsul general, analiza distribuției fluxului sanguin facial, a ritmurilor de microvibrații și a modelelor de clipit poate dezvălui anomalii ascunse [28].

În domeniul stocării și autentifică-

ommendations ISO/IEC 27037 and the European Union's AI regulation (the „AI Act") [12] [13], be adapted to Moldovan legislation, and provide for the preservation of metadata and hash values. It is also important to stimulate the development of specialized medical datasets: experience from MedForensics projects shows that creating datasets that reflect the real clinical environment significantly improves the quality of classifiers [15]. Such databases should be developed with the participation of medical institutions, while respecting confidentiality and ethical rules.

In addition to regulatory measures, technical solutions for chain of custody control need to be implemented: blockchain registries and smart contracts will ensure the transparency of file transactions and verify the immutability of data [13]. The next step is to create interdisciplinary centers within forensic institutions, bringing together lawyers, criminologists, doctors, and IT specialists. Improving digital literacy remains an important area: educational programs for doctors, patients, and technical staff should explain how to verify the authenticity of videos, what signs indicate falsification, and what to do if fraud is suspected. With the rapid development of generative models, the scientific community needs to stay one step ahead of the bad guys by coming up with innovative ways to detect and protect against them. One promising area is the study of local physiological characteristics: while modern deepfake generators already accurately reproduce the general pulse, analysis of facial blood flow distribution, microvibration rhythms, and blinking patterns can reveal hidden anomalies [28].

In the field of media file storage and authentication, combinations of blockchain and post-quantum cryptography offer promising results, ensuring long-term data protection. The concept of "Forensic of Things" involves equipping medical devices with sensors and digital trace record-

rii fișierelor media, combinațiile dintre blockchain și criptografia post-cuantică oferă rezultate promițătoare, asigurând protecția datelor pe termen lung. Conceptul de „Forensic of Things" implică dotarea echipamentelor medicale cu senzori și înregistratoare digitale de urme, ceea ce va permite colectarea automată a dovezilor și va crește transparența operațiunilor [13]. De asemenea, ar trebui dezvoltată cercetarea juridică: este necesar să se analizeze experiența țărilor care implementează reglementări speciale împotriva deepfake-urilor (de exemplu, cerința Chinei privind etichetarea obligatorie a conținutului sintetic [14]) și, pe baza acesteia, să se elaboreze propuneri pentru modernizarea legislației naționale. Inițiativele internaționale, cum ar fi Convenția de la Budapesta și proiectele CyberEast +, oferă o platformă pentru schimbul de experiență, dezvoltarea de standarde comune și îmbunătățirea calificărilor experților, ceea ce este important pentru combaterea eficientă a criminalității deepfake [7] [8].

CONCLUZII

Falsificările video bazate pe rețele neuronale au schimbat radical domeniul probelor digitale, punând sub semnul întrebării nu doar credibilitatea videoclipurilor individuale, ci și încrederea publicului în sistemul judiciar. În contextul digitalizării asistenței medicale, astfel de falsificări pot induce în eroare pacienți și medici, masca erori medicale, discredita instituțiile medicale și submina garanțiile procedurale. O analiză a cadrului de reglementare relevă faptul că în Republica Moldova nu există o definiție unificată a deepfake-ului, în pofida cerințelor documentelor internaționale – The European Union's AI regulation (the „AI Act"), Principiile OCDE privind IA și Convenția de la Budapesta – cu privire la transparența, etichetarea și responsabilitatea în vederea utilizării conținutului sintetic. În consecință, conceptul de deepfake trebuie încorporat în legislația națională ca subiect independent al examinării criminalistice.

ers, which will enable automatic evidence collection and increase the transparency of operations [13]. Legal research should also be developed: it is necessary to analyze the experience of countries that implement special regulations against deepfakes (for example, China's requirement for mandatory labeling of synthetic content [14]) and, based on this, develop proposals for modernizing national legislation. International initiatives such as the Budapest Convention and CyberEast+ projects provide a platform for sharing experience, developing common standards, and improving expert qualifications, which is important for effectively combating deepfake crime [7][8].

4. CONCLUSIONS

Neural network-based video forgeries have radically changed the field of digital evidence, calling into question not only the credibility of individual videos, but also public trust in the justice system. In the context of the digitization of healthcare, such fakes can mislead patients and doctors, mask medical errors, discredit medical institutions, and undermine procedural safeguards. An analysis of the regulatory framework reveals that there is no unified definition of deepfakes in the Republic of Moldova, despite the requirements of international documents – The European Union's AI regulation (the „AI Act"), the OECD Principles on AI, and the Budapest Convention - on transparency, labeling, and responsibility in the use of synthetic content. Consequently, the concept of deepfakes must be incorporated into national legislation as an independent subject of forensic examination.

The technological race between deepfake creators and detectors continues. Traditional methods based on visual analysis and metadata verification are giving way to combined approaches involving deep neural networks, audiovisual synchronization analysis, biometric signals, and spectral artifacts. New research shows

Cursa tehnologică dintre creatorii și detectorii de deepfake-uri continuă. Metodele tradiționale bazate pe analiza vizuală și verificarea metadatelor cedează locul unor abordări combinate care implică rețele neuronale profunde, analiza sincronizării audiovizuale, semnale biometrice și artefacte spectrale. Noi cercetări arată că falsurile de înaltă calitate pot conține un puls general realist, astfel încât atenția se îndreaptă către variațiile locale ale fluxului sanguin, micromișcări și integrarea informațiilor prin diferite modalități. Contramăsurile eficiente necesită standarde internaționale, certificarea detectoarelor, dezvoltarea de seturi de date medicale specializate și implementarea tehnologiilor blockchain pentru înregistrarea lanțului de custodie. Doar colaborarea interdisciplinară între avocați, profesioniști din domeniul medical, specialiști în științe criminalistice și în inteligență artificială poate asigura fiabilitatea dovezilor video și protejarea drepturilor pacienților în era mediilor sintetice.

that even high-quality fakes can contain a generally realistic pulse, so attention is turning to local variations in blood flow, micro-movements, and the integration of information from different modalities. Effective countermeasures require international standards, detector certification, the development of specialized medical datasets, and the implementation of blockchain technologies for chain of custody recording. Only interdisciplinary collaboration between lawyers, medical professionals, forensic scientists, and artificial intelligence specialists can ensure the reliability of video evidence and protect patients' rights in the era of synthetic media.

REFERINȚE BIBLIOGRAFICE

BIBLIOGRAPHICAL REFERENCES

1. Advisory Committee on Evidence Rules. Agenda for committee meeting, April 19, 2024. Washington: Judicial Conference of the USA, 2024. În: https://www.uscourts.gov/sites/default/files/2024-04_agenda_book_for_evidence_rules_meeting_final.pdf (accesat la 15.12.2025).
2. Advisory Committee on Evidence Rules. Agenda for committee meeting, May 2, 2025. Washington: Judicial Conference of the USA, 2025. În: https://www.uscourts.gov/sites/default/files/document/2025-05_evidence_rules_committee_agenda_book_final.pdf (accesat la 15.12.2025).
3. Amped Software. Deepfake forensics is much more than deepfake detection! În: Amped Blog, 2025. În: https://blog.ampedsoftware.com/2025/04/deepfake-forensics-is-much-more-than-deepfake-detection/ (accesat la 15.12.2025).
4. Babic B. et al. A general framework for governing marketed AI/ML medical devices. În: npj Digital Medicine, 2025, art. 328. În: https://www.nature.com/articles/s41746-025-01717-9 (accesat la 15.12.2025).
5. Bodrov N.F., Lebedeva A.K. Analysis of judicial practice in establishing circumstances in cases of unlawful distribution of generative content created using artificial intelligence technologies. În: Legal Research, 2024. În: https://cyberleninka.ru/article/n/analiz-sudebnoy-praktiki-ustanovleniya-obstoyatelstv-v-sluchayah-protivopravnogo-rasprostraneniya-generativnogo-kontenta-sozdannogo (accesat la 15.12.2025).

6. Ciftci U., Demir I., Yin L. FakeCatcher: Detecting synthetic portrait videos using biological signals. În: arXiv, 2020. În: https://arxiv.org/abs/1901.02212 (accesat la 15.12.2025).
7. Council of Europe. Convention on Cybercrime (Budapest Convention), 2001. În: https://www.coe.int/en/web/cybercrime/the-budapest-convention (accesat la 15.12.2025).
8. Council of Europe. CyberEast+: Stakeholders from the Republic of Moldova analyze the benefits of common tools for incident/evidence handling and digital forensics, 2025. În: https://www.coe.int/en/web/cybercrime/-/cybereast-stakeholders-from-the-republic-of-moldova-analyse-the-benefits-of-common-tools-for-incident/evidence-handling-and-digital-forensics (accesat la 15.12.2025).
9. Council of Europe. European Convention on Human Rights, Article 8 — Right to respect for private and family life. Strasbourg, 1950. În: https://www.coe.int/en/web/human-rights-convention/private-life (accesat la 15.12.2025).
10. Delfino R. Deepfakes on trial 2.0: a revised proposal for a new federal rule of evidence to mitigate deepfake deceptions in court. Advisory Committee on Evidence Rules (USA), 2025. În: https://www.uscourts.gov/sites/default/files/2025-04/25-ev-a_suggestion_from_prof._rebecca_delfino_-_rule_901.pdf (accesat la 15.12.2025).
11. Dolhansky B. et al. The DeepFake Detection Challenge (DFDC) dataset. În: arXiv, 2020. În: https://arxiv.org/abs/2006.07397 (accesat la 15.12.2025).
12. European Parliament. EU AI Act: first regulation on artificial intelligence. În: Parliament News, 2023. În: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (accesat la 15.12.2025).
13. Ismail I., Ariffin K.A.Z., Houck M.M. The admissibility of digital evidence from open-source forensic tools: development of a framework for legal acceptance. În: PLOS ONE, 2025. În: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0331683 (accesat la 15.12.2025).
14. Kochetova A. Deepfakes and responsibility for their distribution: what you need to know. În: LegalAcademy, 2024. În: https://legalacademy.ru/sphere/post/dipfeiki-i-otvetstvennost-za-ih-rasprostranenie-chto-vazhno-znat (accesat la 15.12.2025).
15. Li S. et al. Toward Medical Deepfake Detection: a comprehensive dataset and novel method. În: arXiv, 2025. În: https://arxiv.org/abs/2509.15711 (accesat la 15.12.2025).
16. Linna Jr. D. Deepfakes in Court: How Judges Can Proactively Manage AIGenerated Evidence. În: University of Chicago Legal Forum, 2025. În: https://legal-forum.uchicago.edu/print-archive/deepfakes-court-how-judges-can-proactively-manage-alleged-ai-generated-material (accesat la 15.12.2025).
17. Losey R. The problem of deepfakes and AIgenerated evidence. În: EDRM Blog, 2024. În: https://edrm.net/2024/04/the-problem-of-deepfakes-and-ai-generated-evidence (accesat la 15.12.2025).
18. Milmo D. Smudgy chins, weird hands, dodgy numbers: seven signs you're watching a deepfake. În: The Guardian, 01.07.2024. În: https://www.theguardian.com/technology/article/2024/jul/01/seven-signs-deepfake-artificial-intelligence-videos-photographs (accesat la 15.12.2025).
19. Mitchell A. Deepfaked evidence: what case law tells us about how the rules of authenticity need to change. În: Berkeley Technology Law Journal Blog, 2025. În: https://btlj.org/2025/06/deepfaked-evidence-what-case-law-tells-us-about-how-the-rules-of-authenticity-needs-to-change/ (accesat la 15.12.2025).
20. Moldova1. Authorities warn of fake video featuring Prime Minister Dorin Recean. 09.09.2025. În: https://www.moldpres.md/rus/politika/vlasti-preduprezhdayut-o-fejkovom-video-s-

premer-ministrom-dorinom-rechanom (accesat la 15.12.2025).
21. National Center for State Courts. Artificial Intelligence Evidence in Jury Trials: a discussion of current law and emerging issues. NCSC webinar, 2025. În: https://www.ncsc.org/events (accesat la 15.12.2025).
22. National Conference of State Legislatures. Deceptive audio or visual media ("Deepfakes") 2024 legislation, 2024. În: https://www.ncsl.org/technology-and-communication/deceptive-audio-or-visual-media-deepfakes-2024-legislation (accesat la 15.12.2025).
23. OECD. OECD AI Principles – values-based principles and policy recommendations, 2019 (actualizat 2024). În: https://oecd.ai/en/dashboards/ai-principles/P11 (accesat la 15.12.2025).
24. Paravision. Paravision Deepfake Detection: HighTrust AI for Face Recognition and Liveness, 2025. În: https://www.paravision.ai/products/paravision-deepfake-detection (accesat la 15.12.2025).
25. Ricci K. Exploitation of AI in the Healthcare Industry: Threats and Risk Management. În: Citrin Cooperman News & Insights, 03.09.2025. În: https://citrincooperman.com/In-Focus-Resource-Center/Exploitation-of-AI-in-the-Healthcare-Industry-Threats-and-Risk-Management (accesat la 15.12.2025).
26. Sandoval M.-P. et al. Threat of deepfakes to the criminal justice system: a systematic review. În: Crime Science, 2024. În: https://link.springer.com/article/10.1186/s40163-024-00239-1 (accesat la 15.12.2025).
27. Schjødt Law Firm. AI Act definition of deepfake and disclosure obligation, 2024. În: https://schjodt.com/news/deep-fakes-in-the-ai-act (accesat la 15.12.2025).
28. Seibold C. et al. Highquality deepfakes have a heart! În: Frontiers in Imaging, 2025. În: https://www.frontiersin.org/articles/10.3389/fimag.2025.1504551/full (accesat la 15.12.2025).
29. Singh S., Dhumane A. Unmasking digital deceptions: an integrative review of deepfake detection, multimedia forensics and cybersecurity challenges. În: MethodsX, 2025. În: https://www.sciencedirect.com/science/article/pii/S2215016125004765 (accesat la 15.12.2025).
30. Taylor Duma J. The evolving threat of deepfake telemedicine scams. În: Taylor Duma Insights, 2024. În: https://insights.taylorduma.com/the-evolving-threat-of-deepfake-telemedicine-scams (accesat la 15.12.2025).
31. The BMJ. Trusted TV doctors "deepfaked" to promote health scams on social media. BMJ, 2024. În: https://bmjgroup.com/trusted-tv-doctors-deepfaked-to-promote-health-scams-on-social-media/ (accesat la 15.12.2025).
32. VIDA. Deepfake Threatens Healthcare Services. În: VIDA Blog, 08.05.2024. În: https://vida.id/en/blog/beware-deepfake-threatens-healthcare-services (accesat la 15.12.2025).
33. XPHY. Secure healthcare & telemedicine with realtime deepfake detection: Deepfake Detector use cases. XPHY, 2025. În: https://x-phy.com/deepfake-detection/ (accesat la 15.12.2025).