DOI: https://doi.org/10.53486/sstc2026.v2.64
CZU: 343.63:004.8(478)

DIGITAL LAW AND DEEPFAKES: PROTECTION OF IMAGE AND IDENTITY

DREPTUL DIGITAL ȘI DEEPFAKE-URILE: PROTECȚIA IMAGINII ȘI IDENTITĂȚII

COZACENCO Domnica, studentă, specialitatea: Drept
Academia de Studii Economice din Moldova, Republica Moldova,
Chișinău, str. Bănulescu-Bodoni 61, www.ase.md
e-mail: domnica.cozacenco.ztvr@ase.md

Abstract: *The rapid development of digital technologies has led to the emergence of deepfakes, raising significant legal concerns regarding the protection of image and personal identity. This research addresses the growing risks posed by deepfake technologies, particularly in relation to privacy violations, reputational harm, and identity misuse in the digital environment. The purpose of the study is to analyze the existing legal framework governing digital rights and to evaluate its effectiveness in addressing challenges generated by deepfakes.The research is based on doctrinal legal analysis, comparative methods, and the examination of relevant case law and international regulations. Special attention is given to the balance between freedom of expression and the protection of individual rights. The study also considers the role of emerging regulations, such as data protection laws and digital services acts, in combating the misuse of synthetic media. The results highlight that current legal mechanisms are often insufficient to address the complexity and rapid evolution of deepfake technologies. There is a clear need for more specific regulations, improved detection tools, and enhanced cooperation between legal institutions and technology platforms. The paper concludes that strengthening legal safeguards and promoting digital literacy are essential for ensuring effective protection of image and identity in the digital age.*
Key words: *deepfakes, digital law, identity protection, privacy, image rights, artificial intelligence*
JEL CLASSIFICATION: K24, K38, O33.

INTRODUCERE

Dezvoltarea rapidă a tehnologiilor digitale și a inteligenței artificiale au condus la apariția deepfake-urilor, capabile să genereze conținut fals extrem de realist. Acestea ridică probleme juridice importante privind protecția imaginii, identității și a vieții private, mai ales în contextul utilizării abuzive în mediul online. Importanța cercetării constă în analiza impactului deepfake-urilor asupra drepturilor fundamentale și evidențierea limitelor cadrului juridic actual, care nu este pe deplin adaptat acestor tehnologii. În calitate de obiective ale studiului, autorul își propune să analizeze reglementările existente în dreptul digital, identificarea riscurilor generate de deepfake-uri și evaluarea eficienței mecanismelor de protecție a imaginii și identității, precum și formularea unor propuneri de îmbunătățire.

CONȚINUTUL DE BAZĂ

Analiza surselor bibliografice relevă un interes tot mai crescut al doctrinei juridice și al cercetării interdisciplinare pentru problema deepfake-urilor și impactul acestora asupra drepturilor fundamentale. Studiile recente evidențiază riscurile asociate utilizării acestor tehnologii, în special în ceea ce privește încălcarea dreptului la viață privată, a dreptului la imagine și a identității digitale. Literatura de specialitate subliniază, de asemenea, insuficiența cadrului juridic actual, care nu oferă întotdeauna mecanisme eficiente de prevenire și de sancționare a abuzurilor generate de conținutul manipulat digital. Totodată, lucrările analizate pun accent pe necesitatea adaptării legislației la evoluțiile tehnologice rapide și pe rolul cooperării internaționale în acest domeniu.

În ceea ce privește metodele de cercetare, studiul se bazează pe analiza doctrinară a literaturii de specialitate, metoda comparativă și examinarea reglementărilor juridice relevante la nivel național

și internațional. De asemenea, a fost utilizată analiza practicii judiciare și a unor exemple concrete privind utilizarea deepfake-urilor, pentru a evidenția modul în care aceste situații sunt tratate din punct de vedere juridic. Abordarea interdisciplinară permite o înțelegere mai amplă a fenomenului, prin corelarea aspectelor juridice cu cele tehnologice.

Înainte de toate, menționăm că dreptul digital a devenit din ce în ce mai important în ultimii ani, mai ales odată cu apariția tehnologiilor care pot crea conținut fals, dar extrem de realist. Printre acestea, deepfake-urile ocupă un loc special, deoarece pot reproduce chipul, vocea și gesturile unei persoane într-un mod care, la prima vedere, pare complet autentic (Deepfake. Ghid pentru organizații, 2025). Această evoluție tehnologică ridică probleme serioase legate de protecția imaginii și identității unei persoane. În context, amintim că deepfake-ul este un tip de conținut digital (video, audio sau imagine), creat cu ajutorul inteligenței artificiale, în care chipul, vocea sau expresiile unei persoane sunt înlocuite sau imitate astfel încât să pară reale.

„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 fotografii, conținuturi audio și video create sau modificate artificial, care imită persoane și evenimente reale" (Pisarenco, 2025). Deepfake poate fi definit ca "un produs sintetic, conceput și realizat cu ajutorul sistemelor inteligente ce conține valențe de deep *learning* (învățare profundă) și *conținut fake* (fals)" (Stati, Croitor, 2025).

Deepfake-urile sunt create cu ajutorul inteligenței artificiale, folosind algoritmi care analizează imagini, videoclipuri și înregistrări audio existente. Cu cât există mai multe materiale despre o persoană, cu atât rezultatul final va fi mai convingător (Deepfake. Ghid pentru organizații, 2025). Astfel, persoane publice, influenceri sau chiar oameni obișnuiți pot deveni victime ale unor videoclipuri sau înregistrări false, fără să aibă control asupra modului în care sunt reprezentați (Deepfake. Manipulat sau informat?, 2025). Iar una dintre cele mai mari probleme este faptul că imaginea unei persoane poate fi folosită fără consimțământ (Stati, Croitor, 2025).

În dreptul clasic, dreptul la imagine presupune că nimeni nu poate utiliza chipul sau identitatea altei persoane fără acordul acesteia. În mediul digital însă, acest principiu devine mai greu de aplicat, deoarece conținutul poate fi creat și distribuit foarte rapid, uneori anonim.

Deepfake-urile pot avea consecințe grave. De exemplu, ele pot fi folosite pentru a crea videoclipuri compromițătoare, pentru a răspândi informații false sau pentru a manipula opinia publică. În unele cazuri, acestea au fost utilizate în scopuri de hărțuire sau șantaj (Stati, Croitor, 2025).

Victimele pot suferi nu doar pierderi de imagine, ci și efecte emoționale puternice, cum ar fi anxietatea sau pierderea încrederii în sine (Pisarenco, 2025). Un alt aspect important ține de identitatea digitală. În prezent, identitatea unei persoane nu mai este doar una fizică, ci și una online, formată din conturi pe rețele de socializare, fotografii, videoclipuri și alte date personale.

Deepfake-urile pot afecta direct această identitate, creând o versiune falsă a unei persoane, care poate circula liber pe internet. Acest lucru poate duce la confuzie, dar și la pierderea controlului asupra propriei imagini. Din punct de vedere juridic, există mai multe instrumente care pot fi folosite pentru a proteja persoanele afectate. De exemplu, legea privind protecția datelor personale oferă anumite drepturi, cum ar fi dreptul la ștergerea datelor sau dreptul de a se opune prelucrării acestora. De asemenea, în unele cazuri, se poate apela la dreptul civil pentru a solicita despăgubiri pentru prejudiciul suferit.

Totuși, legislația nu este încă complet adaptată la viața cotidiană. În multe state, nu există reguli specifice pentru deepfake-uri, ci doar norme generale care sunt aplicate prin analogie (Deepfake. Manipulat sau informat?, 2025). Acest lucru creează uneori incertitudine, atât pentru victime, cât și pentru autorități.

Pentru a înțelege mai bine amploarea fenomenului, putem analiza cazul Băncii Naționale a României (BNR) care a avertizat publicul cu privire la o schemă de înșelăciune ce implică utilizarea tehnologiei Deepfake pentru a crea videoclipuri false cu guvernatorul BNR. În aceste videoclipuri, guvernatorul pare să promoveze o platformă de investiții, însă BNR a declarat că acestea sunt false. Scamul folosește AI pentru a modifica vocea și imaginea guvernatorului, cu scopul de a induce în

eroare publicul pentru a participa la investiții frauduloase, promițând câștiguri financiare rapide și ușoare (Financiarul, 2026, Libertatea, 2024).

Un alt exemplu relevant, la nivel internațional, conform informațiilor publicate de BBC News, este cel din Statele Unite ale Americii, în contextul alegerilor primare din New Hampshire. Un apel automat fals, care imita vocea președintelui Joe Biden, le-a cerut alegătorilor să nu participe la votul din cadrul primarelor și să „păstreze" votul pentru alegerile generale din noiembrie. Autoritățile au deschis o anchetă, suspectând utilizarea inteligenței artificiale pentru generarea vocii, iar procurorul general din New Hampshire a confirmat că mesajul pare a fi unul fals și creat artificial. Cazul a fost considerat o tentativă de influențare și perturbare a procesului electoral, afectând între 5.000 și 25.000 de alegători și evidențiind riscurile majore ale deepfake-urilor în context democratic. În urma investigațiilor, s-a stabilit că apelurile automate false din New Hampshire au fost organizate de consultantul politic Steven Kramer. Acesta a fost acuzat penal, iar cazul a ajuns în instanță, însă a fost achitat. Deși, din punct de vedere juridic, responsabilitatea sa nu a fost stabilită definitiv, implicarea lui în organizarea acestor apeluri este documentată public și rămâne asociată cu acest caz (Matza, BBC News, 2024).

Așadar, protecția imaginii și identității în acest context necesită atât măsuri juridice, cât și tehnice. Platformele online au început să implementeze sisteme de detectare a conținutului fals, însă acestea nu sunt perfecte. Unele deepfake-uri sunt atât de bine realizate încât pot trece neobservate.

Conform „Deepfake Statistics 2025: AI Fraud Data & Trends", realizat de Mohammed Khalil, fenomenul deepfake-urilor a cunoscut o creștere extrem de rapidă și îngrijorătoare în ultimii ani. Numărul fișierelor deepfake a crescut de la aproximativ 500.000 în 2023 la peste 8 milioane în 2025, ceea ce reflectă accesibilitatea tot mai mare a acestor tehnologii. În paralel, tentativele de fraudă bazate pe inteligență artificială au crescut cu aproximativ 3.000% în 2023, iar în America de Nord cu 1.740%. Clonarea vocii a devenit principalul vector de atac, fiind preferată datorită costurilor reduse, vitezei și nivelului ridicat de realism. În același timp, oamenii reușesc să detecteze doar aproximativ 24,5% dintre videoclipurile deepfake de înaltă calitate, ceea ce arată cât de ușor poate fi manipulat publicul. Toate aceste date confirmă o creștere anuală de aproximativ 900% a volumului de videoclipuri deepfake, ceea ce face ca protecția imaginii și a identității să devină o provocare tot mai dificilă (Khalil, 2025).

De asemenea, educația digitală joacă un rol important. Utilizatorii trebuie să învețe să fie mai atenți la conținutul pe care îl consumă și să verifice sursele informațiilor. De multe ori, răspândirea deepfake-urilor este posibilă tocmai pentru că oamenii nu pun la îndoială autenticitatea materialelor.

Așadar, suntem de aceeași opinie ca și cea a cercetătorilor din domeniu, care accentuează conceptul de necesitate de "îmbunătățire a alfabetizării digitale, ce rămâne un domeniu important: programele educaționale ar trebui să explice cum se verifică autenticitatea videoclipurilor, ce semne indică falsificarea și ce trebuie făcut dacă se suspectează comiterea unei fraude" (Pisarenco, 2025).

Un alt aspect care merită menționat este responsabilitatea platformelor. Rețelele sociale și site-urile de distribuire a conținutului au un rol esențial în limitarea răspândirii deepfake-urilor (Circa, 2013). Ele pot elimina conținutul raportat, pot bloca conturile care încalcă regulile și pot colabora cu autoritățile. Totuși, există și critici legate de faptul că aceste măsuri sunt uneori lente sau insuficiente.

În același timp, apar și soluții tehnologice pentru protecția identității, cum ar fi semnăturile digitale pentru conținut video sau sisteme care pot verifica autenticitatea unui material. Acestea pot ajuta la diferențierea dintre conținutul real și cel fals, însă implementarea lor la scară largă este încă în curs (Deepfake. Manipulat sau informat?, 2025).

CONCLUZII

În concluzie, dezvoltarea deepfake-urilor arată cât de rapid evoluează tehnologia și cât de greu este să ținem pasul cu aceste schimbări. Protecția imaginii și a identității nu mai este doar o problemă clasică de drept, ci devine o provocare complexă, aflată la intersecția dintre tehnologie, etică și

legislație. Chiar dacă există deja instrumente juridice care pot fi folosite pentru apărarea persoanelor afectate, ele nu sunt întotdeauna suficiente sau ușor de aplicat în mediul online.

Pentru viitor, este nevoie de reguli mai clare și adaptate realităților digitale, dar și de o implicare mai activă a platformelor și a utilizatorilor. Fără o reacție comună, riscul ca deepfake-urile să fie folosite în mod abuziv va rămâne ridicat. În același timp, fiecare persoană trebuie să fie mai atentă la modul în care consumă și distribuie informația, deoarece protecția identității nu depinde doar de lege, ci și de responsabilitatea fiecăruia în mediul digital.

REFERINȚE:

1. Circa, A. (2013). *Protecția drepturilor intelectuale. Actualități și Perspective.* București: Universul Juridic.
2. Pisarenco, C. (2025). *Videoclipurile deepfake din domeniul sănătății, subiect de analiză criminalistică.* [Online]. Disponibil la: p_85-100.pdf.
3. Deepfake. *Ghid pentru organizații.* (2025). Directoratul Național de Securitate Cibernetică. [Online]. Disponibil la: DNSC Ghid Deepfake Organizații v2024.09.13 FINAL.
4. Deepfake. *Manipulat sau informat?* (2025). Directoratul Național de Securitate Cibernetică. [Online]. Disponibil la: DNSC Ghid Deepfake.
5. Imaginea site-ului Financiarul. [Online]. Disponibil la: Avertisment BNR. Imaginea lui Mugur Isărescu, folosită într-o fraudă deepfake - Financiarul.
6. Inteligența artificială și deepfake-uri: UE pregătește legea „AI Act". (2025). Chișinău. [Online]. Disponibil la: Inteligență artificială și deepfake-uri: UE pregătește legea „AI Act" | Bizlaw.
7. Khalil, M. (2025). Deepfake statistics 2025: AI fraud data & trends. [Online]. Disponibil la: Deepfake Statistics 2025: AI Fraud Data & Trends.
8. Matza M.(2024). Apelul automat fals al lui Biden le spune alegătorilor să sară peste alegerile primare din New Hampshire. [Online]. Disponibil la: Fake Biden robocall tells voters to skip New Hampshire primary election.
9. Stati, V., & Croitor, C. (2025). *Deepfake-ul cu conținut sexual în Republica Moldova: Provocări sociale și soluții juridice.* Universitatea de Stat din Moldova. [Online]. Disponibil la: 18_Stati_Croitor.pdf.

Coordonator științific: CODREANU Alina, asistent universitar, drd.,
Academia de Studii Economice din Moldova,
Republica Moldova, Chișinău, str. Bănulescu-Bodoni 61, www.ase.md
Telefon: +37369479874
e-mail: codreanu.alina@ase.md