DINCOLO DE ECRAN. CRIMINALITATEA DIGITALĂ ÎN ROMÂNIA

(BEYOND THE SCREEN. DIGITAL CRIME IN ROMANIA)

Ioana PICU[*]

Abstract

Fenomenul infracțional, în accepțiunea sa tradițională, a fost întotdeauna ancorat în spațiul material, având ca obiect bunuri corporale, valori patrimoniale ori integritatea persoanei, pe când astăzi atenția trebuie plasată asupra unui univers infracțional invizibil, dar extrem de eficient, în care datele personale, infrastructurile informatice și chiar percepțiile publice devin obiect și instrument al infracțiunilor. Articolul de față analizează problematica criminalității digitale în România, care prezintă trăsături particulare, determinate de un paradox structural: pe de o parte, un potențial ridicat de competențe IT în rândul tinerilor, recunoscut la nivel european și internațional, pe de altă parte, o infrastructură juridică și instituțională care se adaptează cu dificultate la noile exigențe ale spațiului digital.

Cuvinte cheie: *criminalitate digitală, cybercrime, cryptomonede, phishing, malware, ransomware, ingineria socială, deepfake-urile, clonarea biometrică a vocii, entitățile virtuale autonome, realitatea simulată*

Abstract

The criminal phenomenon, in its traditional meaning, has always been anchored in the material space, having as its object tangible goods, patrimonial values or the integrity of the person, while today the attention must be placed on an invisible but extremely efficient criminal universe, in which personal data, IT infrastructures and even public perceptions become the object and instrument of crimes. This article analyzes the issue of digital crime in Romania, which presents particular features, determined by a structural paradox: on the one hand, a high potential for IT skills among young people, recognized at European and international level, on the other hand, a legal and institutional infrastructure that adapts with difficulty to the new demands of the digital space.

Keywords: *digital crime, cybercrime, cryptocurrencies, phishing, malware, ransomware, social engineering, deepfakes, biometric voice cloning, autonomous virtual entities, simulated reality.*

Introducere

Transformările accelerate ale societății contemporane, determinate de expansiunea tehnologiilor digitale, au remodelat nu doar viața economică și socială, ci și dimensiunile

[*]PhD. student – ”Nicolae Titulescu” University of Bucharest (Romania). Attorney at Law, Constanța Bar.

fenomenului infracțional. În ultimele două decenii, asistăm la o mutație semnificativă: criminalitatea tradițională, ancorată în spațiul fizic, este tot mai des înlocuită sau suplimentată de forme complexe de criminalitate digitală, desfășurate în mediul virtual, transnațional și greu de circumscris unor granițe juridice clasice. Dacă în trecut analiza criminologică se concentra pe delictele *„de stradă”*, astăzi atenția trebuie plasată asupra unui univers infracțional invizibil, dar extrem de eficient, în care datele personale, infrastructurile informatice și chiar percepțiile publice devin obiect și instrument al infracțiunilor.

În România, problematica criminalității digitale prezintă trăsături particulare, determinate de un paradox structural: pe de o parte, un potențial ridicat de competențe IT în rândul tinerilor, recunoscut la nivel european și internațional, pe de altă parte, o infrastructură juridică și instituțională care se adaptează cu dificultate la noile exigențe ale spațiului digital. Astfel, fenomenul a cunoscut în ultimii ani o dezvoltare rapidă, de la fraudele informatice de tip *„phishing”* sau *„carding”*, până la atacuri cibernetice sofisticate, campanii de dezinformare și utilizarea tehnologiilor emergente precum *„deepfake”* sau criptomonedele pentru activități ilicite.

Această realitate reclamă o abordare științifică și interdisciplinară. Din perspectivă criminologică, se impune o reevaluare a teoriilor clasice și o adaptare a metodologiilor de cercetare la dinamica mediului online. Din perspectivă juridico-penală, se resimte necesitatea perfecționării cadrului normativ și a mecanismelor execuțional-penale, capabile să răspundă unor forme de criminalitate ce se desfășoară în afara spațiului material tradițional și care pun în discuție atât eficiența sancțiunilor, cât și posibilitățile reale de reintegrare socială.

Prin urmare, studiul de față își propune să analizeze fenomenul criminalității digitale în România, surprinzând specificul național al acestei problematici, tendințele actuale și provocările pe care le generează pentru sistemul juridic și pentru științele criminologice. Articolul are în vedere atât dimensiunea descriptivă, prin identificarea principalelor tipologii infracționale, cât și dimensiunea explicativă, prin raportarea la teoriile criminologice și la mecanismele execuțional-penale menite să gestioneze acest nou val de infracționalitate.

Scurt istoric

Fenomenul infracțional, în accepțiunea sa tradițională, a fost întotdeauna ancorat în spațiul material, având ca obiect bunuri corporale, valori patrimoniale ori integritatea persoanei. Criminalitatea clasică se manifesta prin forme recognoscibile, precum furt, tâlhărie, omor, înșelăciune, toate fiind circumscrise unui context spațio-temporal definit și reglementate de norme juridice clare. Aceasta presupunea, de principiu, contact direct sau mediat între infractor și victimă și putea fi observată, investigată și sancționată în cadrul structurilor instituționale clasice ale dreptului penal.

Odată cu pătrunderea și generalizarea tehnologiilor digitale, aceste paradigme au început însă să fie subminate. Criminalitatea digitală, apărută ca răspuns adaptativ al comportamentului infracțional la noile condiții tehnologice, se desfășoară într-un mediu virtual, intangibil și transnațional, în care granițele juridice și teritoriale își pierd relevanța. În acest cadru, obiectul

infracțiunii nu mai este exclusiv un bun material, ci poate consta în date personale, informații confidențiale, infrastructuri informatice sau chiar în manipularea opiniei publice. Instrumentele utilizate sunt, la rândul lor, de natură specifică: programe informatice malițioase, rețele de servere anonimizate, criptomonede ori platforme de comunicare socială.

Apariția criminalității digitale este indisolubil legată de procesul de globalizare și de migrarea progresivă a activităților umane în spațiul virtual. Extinderea comerțului electronic, digitalizarea serviciilor publice, circulația instantanee a informației și interconectarea generalizată prin internet au creat nu doar oportunități economice și sociale, ci și noi vulnerabilități. Infractorii, adaptați la aceste realități, au valorificat rapid mediul digital pentru a-și extinde aria de acțiune, beneficiind de anonimitate, rapiditate și dificultatea identificării autorilor în spații transfrontaliere.

Criminalitatea digitală, apărută ca răspuns adaptativ al comportamentului infracțional la noile condiții tehnologice, se desfășoară într-un mediu virtual, intangibil și transnațional, în care granițele juridice și teritoriale își pierd relevanța. În acest cadru, obiectul infracțiunii nu mai este exclusiv un bun material, ci poate consta în date personale, informații confidențiale, infrastructuri informatice sau chiar în manipularea opiniei publice. Instrumentele utilizate sunt, la rândul lor, de natură specifică: programe informatice malițioase, rețele de servere anonimizate, criptomonede ori platforme de comunicare socială.

Termenul de *cybercrime* desemnează multitudinea de acte ilicite îndreptate împotriva sau realizate prin intermediul calculatoarelor, rețelelor ori dispozitivelor digitale. În realitate, *„hacking-ul”* sau încălcările de securitate informatică nu reprezintă singura dimensiune a criminalității informatice. În această categorie se includ orice fapte comise prin internet ori prin alte mijloace electronice. Definiția largă a faptelor sancționabile acoperă o paletă variată de conduite, de la furtul de identitate, hărțuirea online și fraudele informatice, până la breșele de securitate a datelor ori răspândirea de programe malițioase. Motivațiile care stau la baza criminalității informatice sunt, la rândul lor, diverse: obținerea de câștiguri financiare, activismul politic, răfuieli personale sau activitatea grupărilor de crimă organizată, care exploatează vulnerabilitățile sistemelor informatice pentru a-și atinge scopurile.[1]

Primele evenimente istorice asociate cu criminalitatea informatică își au originea în perioada în care au fost constituite primele rețele de calculatoare, în paralel cu dezvoltarea rapidă a computerelor personale. Aceste evenimente au marcat începutul expansiunii fenomenului infracțional în mediul digital. Primele manifestări ale ceea ce avea să fie cunoscut ulterior drept *„hacking”* au apărut în cadrul Massachusetts Institute of Technology (MIT), încă din anii 1960, fiind menționate, la 20 noiembrie 1963, într-o publicație redactată de studenți ai universității (The Tech: MIT Student Journal). Deși, inițial, termenul de *„hacker”* era utilizat pentru a desemna o utilizare ingenioasă și creativă a calculatorului, de-a lungul timpului acesta a dobândit o semnificație negativă, fiind asociat cu producerea de daune asupra sistemelor informatice și a datelor electronice.[2]

[1] Hussein Jassim Akeiber, “A comprehensive study of Cybercrime and Digital Forensics through Machine Learning and AI”, *Rafidain J. Eng. Sci.*, vol. 3, no. 1, pp. 369–395, Feb. 2025

[2] Regner Sabillon, Jeimy Cano, Victor Cavaller, jordi Serra - Cybercrime and Cybercriminals: A Comprehensive Study, International Journal of Computer Networks and Communications Security, vol. 4, no. 6, June 2016, p. 166;

Un alt moment semnificativ este raportat de Einar Stefferud, care consemnează că, în anul 1978, a fost transmis primul mesaj electronic nesolicitat, cunoscut ulterior sub denumirea de *„spam”*. Abuzul a fost comis de compania Digital Equipment Corporation (DEC), care a utilizat lista de distribuție a rețelei ARPANET (Advanced Research Projects Agency Network) pentru a promova un nou calculator, modelul „DEC-20”.[3]

Odată cu începutul noului mileniu, s-a constatat o creștere semnificativă atât a frecvenței, cât și a gradului de sofisticare al atacurilor cibernetice. Programele malițioase au dobândit capacitatea de a se răspândi extrem de rapid prin intermediul rețelelor informatice, așa cum s-a întâmplat în cazurile notorii ale virusului Melissa din 1999 sau ale *viermelui* ILOVEYOU din 2000, incidente care au generat pierderi financiare substanțiale și au atras atenția opiniei publice și a specialiștilor asupra vulnerabilităților din domeniul securității informatice. Aceste evenimente au declanșat dezbateri intense privind colectarea și protecția datelor personale, determinând mediul de afaceri să aloce investiții considerabile pentru consolidarea propriilor sisteme de securitate IT.[4]

O privire retrospectivă asupra unor dintre cele mai reprezentative atacuri cibernetice din istorie:

- 1962 – baza de date a Massachusetts Institute of Technology (MIT) a fost compromisă printr-un acces neautorizat;
- 1971 – a fost creat primul virus informatic;
- 1981 – Ian Murphy a devenit prima persoană condamnată pentru o infracțiune informatică;
- 1988 – Robert Morris a desfășurat primul atac cibernetic de amploare;
- 1989 – a apărut prima formă de ransomware;
- 1994 – a fost utilizat pentru prima dată un program de tip *„password sniffer”*;
- 1995 – un hacker a încercat pentru prima dată să jefuiască o bancă prin mijloace informatice;
- 1998 – guvernul Statelor Unite a fost victima unui atac cibernetic pentru prima dată;
- 1999 – virusul Melissa a produs efecte semnificative la nivel global;
- 2000 – atacuri de tip Distributed Denial of Service (DDoS) au paralizat activitatea mai multor mari companii de retail;
- 2000 – virusul ILOVEYOU a infectat milioane de calculatoare la nivel mondial;
- 2005 – banca HSBC a suferit o breșă de securitate, ce a afectat aproximativ 180.000 de clienți;
- 2008 – compromiterea sistemelor companiei Heartland Payment Systems a dus la sustragerea datelor a 134 de milioane de utilizatori;
- 2010 – viermele Stuxnet, considerat prima *„armă digitală”*, a vizat instalațiile nucleare din Iran;
- 2010 – virusul Zeus a produs pagube majore prin furturi informatice;

[3] Regner Sabillon, Jeimy Cano, Victor Cavaller, jordi Serra - Cybercrime and Cybercriminals: A Comprehensive Study, International Journal of Computer Networks and Communications Security, vol. 4, no. 6, June 2016, p. 166;
[4] Waqas. "The Evolution of Cybercrime Investigation". Jul 2024.

- 2010 – a fost declanșată „Operațiunea Aurora” de către entități atribuite Chinei;
- 2011 – corporația Sony a fost victima unui atac cibernetic de amploare;
- 2013 – Edward Snowden a făcut publice informații guvernamentale clasificate din mai multe state;
- 2013 – compania Target a căzut victimă unui atac de tip phishing, cu efecte majore asupra securității datelor clienților;
- 2013 – datele bancare ale utilizatorilor Adobe au fost publicate online în urma unui atac cibernetic;
- 2014 – a avut loc incidentul cunoscut sub numele de Celebgate, constând în compromiterea și difuzarea fotografiilor private ale unor persoane publice;
- 2015 – a apărut varianta de ransomware denumită SamSam;
- 2015 – baza de date a platformei Ashley Madison a fost piratată și publicată;
- 2017 – atacul WannaCry a afectat peste 200.000 de dispozitive care utilizau sistemul de operare Windows;
- 2017 – angajați ai companiilor Facebook și Google au fost induși în eroare și au transferat sute de milioane de dolari către hackeri;
- 2018 – platforma GitHub a înregistrat un atac DDoS de 1,3 terabiți pe secundă, considerat unul dintre cele mai ample din istorie;
- 2018 – atac de tip crypto-jacking prin utilizarea platformei Coinhive;
- 2018 – lanțul hotelier Marriott a suferit o breșă de securitate care a compromis datele personale a circa 500 de milioane de clienți;
- 2019 – banca Capital One a fost victima celei mai mari breșe de securitate a datelor de până atunci;
- 2020 – mai multe conturi de utilizatori cu vizibilitate ridicată de pe platforma X (Twitter) au fost implicate într-un atac de tip phishing;
- 2022 – Guvernul statului Costa Rica a declarat stare de urgență națională după un atac al grupării Conti Ransomware;
- 2023 – atacul informatic de tip MOVEit a afectat peste 2000 de organizații și a expus datele a peste 60 de milioane de persoane;
- 2024 – platforma Ticketmaster a suferit o breșă de securitate exploatând o vulnerabilitate Snowflake;
- 2024 – hackeri au sustras jurnalele de apel și mesajele text ale tuturor clienților AT&T.[5]

De la primele manifestări ale criminalității informatice, consemnate punctual în mediile universitare și tehnologice, s-a ajuns treptat la un fenomen care, prin natura sa virtuală, scapă încadrării în limitele jurisdicționale clasice.

Criminalitatea informatică nu cunoaște granițe fizice sau geografice și poate fi comisă cu ușurință. Absența limitelor teritoriale permite infractorilor să acționeze dincolo de frontierele

[5] Waqas- The evolution of cybercrime investigation, 14 July 2024, https://hackread.com/the-evolution-of-cybercrime-investigations/;

naționale, ceea ce complică semnificativ activitățile de investigare și urmărire penală. În aceste condiții, autoritățile de aplicare a legii depind tot mai mult de cooperarea internațională pentru a contracara acest tip de criminalitate transnațională.[6]

Formele criminalității informatice

Analiza criminalității informatice impune o delimitare atentă a formelor prin care aceasta se manifestă, având în vedere diversitatea metodelor utilizate și complexitatea obiectivelor vizate. Spre deosebire de criminalitatea clasică, ale cărei tipologii pot fi circumscrise unor categorii tradiționale, criminalitatea informatică prezintă o structură fluidă, în continuă transformare, dependentă de inovația tehnologică și de adaptabilitatea autorilor. De la atacuri aparent simple, precum transmiterea de e-mailuri frauduloase, până la operațiuni sofisticate, coordonate transnațional și orientate împotriva infrastructurilor critice, spectrul fenomenului este extrem de variat. Prin urmare, prezentarea principalelor forme de criminalitate informatică nu are doar un rol descriptiv, ci constituie o premisă necesară pentru înțelegerea riscurilor actuale, pentru evaluarea impactului social și economic al acestor fapte și, în egală măsură, pentru fundamentarea unor mecanisme juridice și criminologice de răspuns adecvat.

Deși inventarierea exhaustivă a tuturor tipologiilor și subcategoriilor de fapte ar fi anevoioasă, se impune totuși reliefarea unor dintre cele mai frecvente manifestări:

- ***phishing*** – acest tip de infracțiune constă în transmiterea de atașamente sau linkuri capcană prin e-mail către utilizatori, pentru a obține acces la conturile sau dispozitivele acestora. Victimele tind să reacționeze la mesaje care pretind a proveni de la companii sau instituții legitime, fiind încurajate să își schimbe parola ori să își actualizeze datele de facturare. În realitate, această manevră oferă infractorilor acces la conturile și fondurile persoanei vizate;
- ***malware*** – termenul desemnează programe software capcană care *„infectează”* sistemele ori dispozitivele individuale, având ca scop deteriorarea sau accesarea ilegală a acestora. Printre formele uzuale se numără virușii, viermii, programele de tip spyware și ransomware. De regulă, malware-ul este distribuit prin e-mailuri, site-uri nesigure sau fișiere disimulate sub forma unor documente ori imagini. Utilizatorii introduc adesea involuntar malware-ul în sistem, accesând linkuri sau descărcând conținut de pe pagini neverificate. Obiectivul autorilor este, de cele mai multe ori, preluarea controlului asupra dispozitivelor și sustragerea de date ori informații.
- ***ransomware*** – reprezintă o formă particulară de malware, bine mediatizată, prin care un sistem sau o rețea este blocată, împiedicând accesul utilizatorilor la propriile date. Autorii solicită plata unei răscumpărări, de regulă în criptomonede, pentru deblocarea fișierelor sau evitarea publicării unor date sensibile. În multe cazuri, infractorii amenință cu divulgarea informațiilor confidențiale dacă suma nu este achitată. Agenția Uniunii

[6] European Parliament policies – Insight - Understanding cybercrime, European Union, 2024, p. 2;

Europene pentru Securitate Cibernetică (ENISA) a semnalat o creștere semnificativă a atacurilor de tip ransomware asupra statelor membre;

- ***ingineria socială*** *(„social engineering")* – presupune manipularea psihologică a persoanelor, astfel încât acestea să divulge informații personale sau confidențiale, ulterior folosite în activități frauduloase. Infractorii exploatează mecanisme comportamentale naturale – curiozitatea, sentimentul de urgență sau încrederea, pentru a câștiga accesul la date ori pentru a determina victimele să efectueze acțiuni pe care, în mod normal, nu le-ar fi realizat. Odată cu apariția și perfecționarea instrumentelor bazate pe inteligență artificială, infractorii pot genera mesaje personalizate, în mai multe limbi, cu un grad de verosimilitate mult mai ridicat decât în trecut;
- ***denial of Service*** *(DoS/DDoS)* – sunt atacuri ce constau în bombardarea unei rețele sau a unui site cu un volum excesiv de solicitări, care supraîncarcă sistemele și le face indisponibile utilizatorilor obișnuiți. Aceste atacuri pot trece o perioadă neobservate, iar efectele sunt adesea costisitoare, implicând atât pierderi financiare, cât și deteriorarea reputației organizației vizate. Variantele sofisticate, cunoscute drept atacuri *„persistente și avansate"*, sunt asociate cu actori mai bine pregătiți și resurse superioare;
- ***dezinformarea și dezinformarea intenționată*** (*„disinformation/misinformation"*) - răspândirea de informații false sau înșelătoare nu este o practică nouă, însă amploarea și viteza sa au fost amplificate exponențial de internet și de omniprezența rețelelor sociale. În lipsa filtrului media tradițional și în contextul proliferării platformelor partizane, publicul consumă informația într-un mod complet diferit. Impactul asupra societății civile este considerabil: de la răspândirea de mituri privind bolile infecțioase și vaccinarea, până la negarea schimbărilor climatice și propagarea unor idei extremiste. Potrivit OCDE, combinația dintre modelele lingvistice de inteligență artificială și campaniile de dezinformare poate conduce la manipulări de anvergură și la deteriorarea încrederii publice.[7]

Tot în această vastă sferă a criminalității digitale se integrează și noile metamorfoze ale falsificării tehnologice, născute din simbioza dintre inteligența artificială generativă și capacitățile nelimitate ale rețelelor neuronale: deepfake-urile, clonarea biometrică a vocii și a chipului, producerea de entități virtuale autonome și fabricarea de realități simulate, capabile să submineze însăși noțiunea de autenticitate.

- ***deepfake-urile*** - reprezintă conținuturi media sintetice manipulate digital, precum videoclipuri, imagini sau înregistrări audio, în care persoanele sunt prezentate făcând sau spunând lucruri care, în realitate, nu au existat și nu s-au petrecut niciodată[8];
- ***clonarea biometrică a vocii*** - reprezintă procesul prin care tehnologia utilizează mostre vocale ale unei persoane, elemente precum timbrul vocal, intonația sau respirația, pentru a

[7] European Parliament policies – Insight - Understanding cybercrime, European Union, 2024, p. 4,5;
[8]Mekhail Mustak et al. - Deepfakes: Deceptions, mitigations, and opportunities, Journal of Business Research, Volume 154, January 2023, 113368, https://www.sciencedirect.com/science/article/abs/pii/S0148296322008335 , pagină web consultată în data de 12.10.2025;

genera artificial replici aproape identice ale vocii respective, capabile să rostească texte care nu au fost niciodată pronunțate[9];

- ***entitățile virtuale autonome*** - sunt definite ca agenți digitali creați prin inteligență artificială, care acționează și interacționează autonom, manifestând o formă de intenționalitate algoritmică și persistență comportamentală.[10]
- ***realitatea simulată*** - descrie un proces complex de reconstrucție digitală a lumii percepute, în care tehnologiile de inteligență artificială generează medii și evenimente inexistente, dar suficient de coerente încât să substituie percepția realului.[11]

Aceste instrumente de manipulare digitală, a căror sofisticare depășește adesea puterea de detecție a mijloacelor clasice de investigare, marchează o nouă etapă în evoluția criminalității contemporane, una în care frontiera dintre adevăr și iluzie devine permeabilă, iar agresiunea informațională capătă forme subtile, invizibile, dar profund destabilizatoare pentru ordinea socială și juridică.

Autorii criminalității informatice

Autorii criminalității informatice sunt eterogeni sub aspectul motivațiilor și al modului de operare, putând fi grupați în câteva categorii principale:

- *actorii susținuți de state* – finanțați și instruiți de guverne, motivați în principal politic, vizează ținte cu valoare strategică ridicată, precum infrastructurile critice. Războiul din Ucraina a demonstrat persistența acestora, atacurile vizând nu doar Ucraina, ci și state membre ale UE;
- *infractorii orientați spre câștig financiar* – flexibili și inventivi, creează site-uri comerciale false, compromit sisteme de e-mail și baze de date pentru a frauda clienți, sau folosesc adrese clonate pentru a redirecționa plăți. Acționează adesea în momente favorabile, precum sfârșitul de săptămână;
- *insiderii* – angajați actuali sau foști, contractori ori parteneri de afaceri. Amenințările pot fi intenționate sau rezultatul neglijenței. Conform IBM Cost of a Data Breach Report 2023, breșele cauzate de insideri malițioși sunt cele mai costisitoare, media pierderilor fiind estimată la 4,9 milioane USD per incident;
- *hacktiviștii* – animați de idealuri politice sau sociale, urmăresc perturbarea activităților instituțiilor sau companiilor, prin atacuri de tip denial of service, modificarea site-urilor sau divulgarea de date. Deși în scădere, fenomenul a cunoscut o revigorare recentă în context geopolitic;

[9]Mohamed Lazzouni - Voice Cloning: What It Is and Why It's Scary, 14.06.2023, https://builtin.com/artificial-intelligence/what-is-voice-cloning, pagină web consultată la data de 12.10.2025;
[10] Tim Cotten - Autonomous Virtual Beings, Jan 5, 2024, https://blog.cotten.io/autonomous-virtual-beings-aaef7cbbe5de, pagină web consultată la data de 12.10.2025;
[11] João Phillipe Cardenuto et al., The Age of Synthetic Realities: Challenges and Opportunities, Fri, 9 Jun 2023, arXiv:2306.11503, pagină web consultată la data de 12.10.2025.

- *teroriștii cibernetici* – motivați de ideologii extreme, recurg la atacuri asupra rețelelor și sistemelor informatice pentru a genera panică și incertitudine. Deși delimitarea lor de actorii statali sau de criminalitatea clasică este uneori neclară, amenințarea este reală, determinând statele și organizațiile să adopte măsuri de contracarare.[12]

Reglementare la nivel internațional

Deși a reprezentat, la momentul adoptării sale, un reper esențial pentru construcția juridică internațională în materie, Convenția Consiliului Europei privind criminalitatea informatică[13] se dovedește astăzi, în parte, inadecvată pentru a răspunde noilor manifestări ale criminalității informatice, mult mai complexe și diversificate. Această limitare se explică, în bună măsură, prin faptul că instrumentul normativ menționat își are originile conceptuale în Recomandarea Consiliului Europei din anul 1989, care a inspirat structura și filosofia sa juridică. Cu toate acestea, Convenția rămâne unul dintre cele mai importante și influente instrumente juridice internaționale în domeniul criminalității informatice, constituind, până în prezent, un punct de referință pentru legislațiile naționale și pentru cooperarea judiciară internațională în materie.

Dincolo de rolul fundamental pe care l-a avut Convenția Consiliului Europei privind criminalitatea informatică, trebuie remarcat că, în ultimele aproape două decenii, legislatorul european s-a dovedit remarcabil de activ în consolidarea cadrului normativ aplicabil fenomenului criminalității informatice. În această perioadă, a fost adoptată o serie de instrumente juridice de substanță, menită să asigure o armonizare la nivelul dreptului penal material al statelor membre. Dintre acestea, se cuvine a fi menționate:

- Decizia-cadru 2001/413/JAI a Consiliului Uniunii Europene privind combaterea fraudei și falsificării mijloacelor de plată, altele decât numerarul[14];
- Decizia-cadru 2004/68/JAI privind combaterea exploatării sexuale a copiilor și a pornografiei infantile[15];
- Decizia-cadru 2005/222/JAI privind atacurile împotriva sistemelor informatice[16];
- Directiva 2011/93/UE privind combaterea abuzului sexual asupra copiilor, exploatării sexuale și pornografiei infantile[17];

[12] European Parliament policies – Insight - Understanding cybercrime, European Union, 2024, p. 3,4.
[13] Ratificată prin Legea nr. 64/2004, publicată în M. Of. nr. 343 din 20 aprilie 2004.
[14] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32001F0413, pagină web consultată la data de 12.10.2025;
[15] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32004F0068, pagină web consultată la data de 12.10.2025;
[16] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32005F0222, pagină web consultată la data de 12.10.2025;
[17] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32011L0093, pagină web consultată la data de 12.10.2025;

- Directiva 2013/40/UE (*fostă 2013/222/JAI*, numerotare incorectă în unele surse) privind atacurile împotriva sistemelor informatice[18];
- Directiva (UE) 2019/713 a Parlamentului European și a Consiliului privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar[19];
- Directiva (UE) 2022/2555 – NIS2 privind măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice[20];
- Regulamentul (UE) 2022/2554 – DORA (Digital Operational Resilience Act)[21];
- Regulamentul (UE) 2024/2847 – Cyber Resilience Act (CRA)[22];
- Regulamentul (UE) 2024/903 – Cyber Solidarity Act (CSA)[23];
- Directiva „CER" – Critical Entities Resilience Directive (EU) 2022/2557)[24].

În timp ce actele normative europene menționate anterior, precum directivele privind atacurile informatice, frauda electronică ori securitatea rețelelor, au vizat, în principal, incriminarea faptelor și consolidarea infrastructurii de apărare cibernetică, **Regulamentul (UE) 2024/1689 privind inteligența artificială (AI Act) marchează o nouă etapă normativă, orientată nu asupra efectelor infracționale, ci asupra tehnologiei însăși care le poate genera**. Acesta reglementează dezvoltarea și utilizarea sistemelor de inteligență artificială, introducând pentru prima dată norme de transparență și responsabilitate aplicabile conținutului sintetic, *deepfake*-urilor și celorlalte forme emergente de manipulare digitală.[25]

Reglementare în România

Confruntată cu expansiunea rapidă a noilor forme de criminalitate generate de utilizarea tehnologiilor digitale, societatea românească a resimțit, încă de la începutul anilor 2000, necesitatea de a-și consolida instrumentele de protecție juridică. În acest context, legiuitorul național a urmărit edificarea unui cadru normativ coerent, capabil să prevină, să sancționeze și să descurajeze manifestările infracționale din sfera mediului informatic. Fundamentul acestor

[18] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32013L0040, pagină web consultată la data de 12.10.2025;
[19] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32019L0713, pagină web consultată la data de 12.10.2025;
[20] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555, pagină web consultată la data de 12.10.2025;
[21] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022R2554, pagină web consultată la data de 12.10.2025;
[22] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R2847, pagină web consultată la data de 12.10.2025;
[23] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R0903, pagină web consultată la data de 12.10.2025;
[24] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2557, pagină web consultată la data de 12.10.2025;
[25] https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng?utm_source=chatgpt.com pagină web consultată la data de 12.10.2025;

reglementări s-a sprijinit, în mod firesc, pe documentele juridice internaționale deja consacrate (în special Convenția Consiliului Europei privind criminalitatea informatic și Decizia-cadru a Consiliului Uniunii Europene din 28 mai 2001, la care am făcut referire anterior), adaptate însă realităților și nevoilor interne. În acest sens, pot fi identificate mai multe repere legislative majore care marchează etapele esențiale ale dezvoltării normative în domeniu:

- Legea nr. 365/2002 privind comerțul electronic[26] - a incriminat falsificarea instrumentelor de plată electronice, deținerea de echipamente pentru falsificare, efectuarea operațiunilor financiare frauduloase, acceptarea operațiunilor frauduloase. După adoptarea Codului penal nou (2014), articolele 24 – 28 din Legea 365/2002 au fost abrogate, dar prevederile au fost transferate / integrate în Codul penal;
- Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei[27] - a introdus în legislația română infracțiunile informatice în capitolul *„Prevenirea și combaterea criminalității informatice”* - acces ilegal, fals informatic, fraudă informatică etc., incriminări ce au constituit baza pentru reglementările ulterioare în Codul penal;
- Legea nr. 286/2009 privind Codul penal[28] - a codificat infracțiunile informatice, creând un cadru unitar pentru aceste fapte: art. 249 - Frauda informatică (preia și extinde noțiunile din legile precedente), art. 250 - Efectuarea de operaţiuni financiare în mod fraudulos, art. 251 - Acceptarea operaţiunilor financiare efectuate în mod fraudulos;
- Directiva (UE) 2013/40 privind atacurile asupra sistemelor informatice[29] - a înlocuit Decizia-cadru 2005/222/JAI și a impus statelor membre să incrimineze conduita privind accesul ilegal, afectarea integrității sistemului, afectarea integrității datelor, interceptarea ilegală și utilizarea instrumentelor de comitere a acestui gen de infracțiuni. În legislația română, aceste conduite au fost incluse în articolele 360-365 din Codul penal;

[26] În vigoare de la 05 iulie 2002, republicarea (r1) din Monitorul Oficial, Partea I nr. 959 din 29 noiembrie 2006, modificată prin următoarele acte: L 187/2012; L 50/2024; L 214/2024;

[27] În vigoare de la 21 aprilie 2003, publicarea din Monitorul Oficial, Partea I nr. 279 din 21 aprilie 2003, modificată prin OUG 40/2003 aprobat(ă) prin L 114/2004; L 171/2004; OUG 77/2003 aprobat(ă) prin L 280/2004; L 359/2004; OUG 92/2004; OUG 14/2005; L 348/2004; OG 2/2006; OUG 31/2006; L 96/2006; L 251/2006; OUG 119/2006 aprobat(ă) prin L 191/2007; L 144/2007; L 330/2009; L 284/2010; OUG 37/2011; L 134/2011; L 76/2012; L 255/2013; L 187/2012; Codul de Procedură Fiscală 2015; L 87/2017; L 128/2017; L 59/2019; L 265/2022; L 140/2023;

[28] În vigoare de la 01 februarie 2014, publicarea din Monitorul Oficial, Partea I nr. 510 din 24 iulie 2009, modificată prin L 187/2012; L 63/2012; L 27/2012; L 159/2014; OUG 18/2016; L 151/2016; L 193/2017; L 49/2018; OUG 28/2020; L 217/2020; L 228/2020; L 233/2020; L 274/2020; L 146/2021; L 186/2021; L 207/2021; L 219/2021; L 8/2022; OUG 71/2022; L 170/2022; L 171/2023; L 200/2023; L 213/2023; L 214/2023; L 248/2023; L 258/2023; L 291/2023; L 314/2023; L 323/2023; L 401/2023; L 217/2023; L 430/2023; L 58/2024; L 122/2024; L 172/2024; L 202/2024; L 269/2024; L 19/2025; L 116/2025; L 142/2025.

[29] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32013L0040, pagină web consultată la data de 12.10.2025;

- Directiva (UE) 2019/713 privind frauda și contrafacerea legate de instrumentele de plată fără numerar[30];
- Legea nr. 207/2021 pentru modificarea şi completarea Legii nr. 286/2009 privind Codul penal, precum şi pentru dispunerea unor măsuri de transpunere a Directivei (UE) 2019/713 a Parlamentului European şi a Consiliului din 17 aprilie 2019 privind combaterea fraudelor şi a contrafacerii în legătură cu mijloacele de plată fără numerar şi de înlocuire a Deciziei-cadru 2001/413/JAI a Consiliului[31] - a înlocuit Decizia-cadru 2001/413/JAI, a extins noțiunea de *„instrument de plată fără numerar"* pentru a include moneda virtuală și a impus adaptări la legislația națională. Prin urmare, la nivel național s-a adoptat Legea nr. 207/2021, care a adus următoarele modificări majore:
  - **art. 180** a fost modificat pentru a defini urmâtoarele noțiuni: *„instrument de plată fără numerar", „instrument de plată electronică", „monedă electronică"* și *„monedă virtuală";*
  - **art. 249** (frauda informatică) a fost redefinit, prin includerea expresă a transmisiei, modificării sau ștergerii datelor informatice;
  - **art. 250 alin. (1)** a fost modificat pentru a include operațiunile care implică monedă electronică sau virtuală și utilizarea instrumentelor de plată fără numerar neautorizate;
  - a fost introdus un nou articol: **250[1]** — *operațiuni ilegale cu instrumente de plată fără numerar*;
  - **art. 251** a suferit modificări, în cuprinsul alin. (1) fiind inclusă acceptarea unor operațiuni frauduloase legate de instrumente de plată fără numerar;
  - s-au realizat modificări și asupra articolelor **311 alin. (2)**, **313**, **314** și **316,** pentru a adapta sancțiunile și regimul legal la contextul instrumentelor de plată moderne.

- Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României[32] - a instituit cadrul juridic și instituțional pentru securitate și apărare cibernetică. A reglementat cooperarea interinstituțională, responsabilitățile autorităților, definirea conceptelor (amenințe cibernetică etc.). În mod specific, a înființat Directoratul Național de Securitate Cibernetică (DNSC) - autoritate competentă civilă în domeniul securității cibernetice și a stabilit că SRI este autoritate competentă în domeniul cyberintelligence pentru analizarea, prevenirea și contracararea incidentelor ce afectează securitatea națională. Legea a stabilit termeni și expresii (apărare cibernetică, amenințare cibernetică) și mecanisme de coordonare și cooperare instituțională;
- Ordonanța de urgență nr. 155/2024 privind securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil[33] - a transpus, parțial, directivele europene pentru domeniul civil. A stabilit obligații de gestionare a riscurilor, raportare a incidentelor,

[30] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32019L0713, pagină web consultată la data de 12.10.2025;
[31] În vigoare de la 25 iulie 2021, Publicat în Monitorul Oficial, Partea I nr. 720 din 22 iulie 2021;
[32] În vigoare de la 18 martie 2023, Publicat în Monitorul Oficial, Partea I nr. 214 din 15 martie 2023;
[33] În vigoare de la 31 decembrie 2024;

audit de securitate cibernetică, desemnare a DNSC ca autoritate competentă etc. Cu alte cuvinte, de la abordarea reactivă la una proactivă: entitățile esențiale și importante sunt obligate să identifice, evalueze și gestioneze riscuri, să adopte măsuri proporționale și să reducă efectele incidentelor;

- Legea nr. 14/2025 pentru aprobarea Ordonanței de urgență a Guvernului 155/2024 privind securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil – a completat și rafinat dispozițiile Ordonanței de urgență nr. 155/2024, extinzând sfera entităților reglementate, clarificând criteriile de raportare a incidentelor și întărind competențele DNSC ca autoritate centrală în domeniu.

Vid normativ și provocări juridice în fața noilor tehnologii digitale

Astfel cum am menționat, dincolo de formele *clasice* ale criminalității informatice, asistăm astăzi la emergența unor manifestări mult mai sofisticate, născute din interacțiunea dintre inteligența artificială generativă și tehnologiile de sinteză digitală, precum *deepfake*-urile, clonarea biometrică a vocii și a chipului, crearea de entități virtuale autonome sau fabricarea de realități simulate.

În fața acestei evoluții tehnologice amețitoare, rămâne o întrebare de importanță capitală: **în ce măsură legislația românească este pregătită să gestioneze aceste forme de infracționalitate?**

Dacă la nivel european s-a adoptat AI Act - Regulamentul (UE) 2024/1689, care prevede obligații clare de transparență și etichetare pentru conținutul generat artificial (inclusiv *deepfake*-uri), România se află, în schimb, într-o poziție mai puțin privilegiată, regăsindu-se în situația de a încadra aceste situații în mod analogic și interpretativ în reglementările existente, întrucât nimic nu precizează în mod explicit noțiunea de *conținut creat de inteligența artificială*.

Astfel, România nu are, până la acest moment (octombrie 2025), o lege care să reglementeze explicit *deepfake*-urile, conținutul sintetic sau inteligența artificială generativă.

Nu există nicio lege națională care să definească juridic *conținutul generat de inteligența artificială*, nu există nicio incriminare penală specifică pentru producerea, difuzarea sau utilizarea frauduloasă a *deepfake*-urilor, clonării vocale ori falsurilor sintetice și nu a fost încă adoptat un act normativ de transpunere a AI Act (Regulamentul UE 2024/1689).

Chiar dacă acest din urmă act este direct aplicabil în România, necesită o lege internă de implementare (pentru sancțiuni și desemnarea autorităților naționale competente în a urmări acest tip de infracționalitate).

În timp ce la nivel european AI Act (Regulamentul 2024/1689) prezintă o reglementare completă, prevăzând obligații de transparență și de etichetare clară pentru conținuturile generate de AI[34], impunând interdicții privind utilizarea AI pentru manipulare, dezinformare sau influență politică ascunsă, în România, în octombrie 2025, există doar reglementări indirecte (securitate cibernetică, protecția datelor, fals informatic).

[34] Art. 52 din Regulamentul (UE) 2024/1689 privind inteligența artificială (AI Act);

Codul penal poate acoperi doar parțial asemenea tip de criminalitate, prin raportare la următoarele dispoziții legale în vigoare: art. 249 - frauda informatică, art. 324 din Codul penal – falsificarea unei înregistrări tehnice, art. 325 – falsul informatic, art. 226 – violarea vieții private, art. 404 - răspândirea de informații false, texte de lege care însă nu includ explicit noțiunea de inteligență artificială și se aplică numai prin analogie.

În egală măsură, Legea nr. 363/2018 reglementează *publicitatea înșelătoare digitală* fără a menționa conținutul generat artificial, iar DNSC are competențe limitate la monitorizarea și avertizarea în materie de dezinformare online, fără prerogative de sancționare a utilizării abuzive a sistemelor de inteligență artificială.

În aceste condiții, se impune elaborarea unei incriminări autonome a falsificării digitale prin inteligență artificială, pentru a asigura protecția integrității informaționale, a dreptului la imagine și a ordinii publice digitale.

Necesitatea unei intervenții legislative derivă din următoarele rațiuni:

- **caracterul specific al prejudiciului cauzat de conținuturile sintetice** (falsificarea identității digitale și a realității perceptive), acesta distingându-se fundamental de cel generat de infracțiunile informatice tradiționale, întrucât nu vizează distrugerea sau alterarea datelor, ci substituirea realității însăși, a identității, a imaginii și a adevărului perceput social. [35] Astfel, acest gen de infracționalitate nu produce doar pierderi economice, ci alterează structura ontologică a adevărului digital și a identității personale. Falsul digital nu mai operează asupra unui suport material sau asupra unui sistem informatic, ci asupra realității percepute, substituind adevărul cu o copie algoritmică, convingătoare, dar iluzorie.[36]
- **lipsa unui element material clasic**, întrucât fapta nu vizează un *„sistem informatic”* înțeles în sensul art. 181 din Codul penal ca o acțiune fizică, tangibilă, exercitată asupra unei entități concrete. În cazul faptelor de tip *„deepfake”*, al manipulării algoritmice, al falsificării datelor prin intermediul inteligenței artificiale sau al distorsionării automate a fluxului informațional, nu se poate discuta despre o atingere directă adusă unui *„sistem informatic”* în accepțiunea art. 181 C. pen., ci despre o intervenție asupra realității informaționale însăși, o noțiune fluidă, dar care produce efecte juridice și sociale concrete. Prin urmare, elementul material nu mai constă în alterarea, distrugerea sau blocarea sistemului informatic, așa cum o prevede, de exemplu, art. 363 din Codul penal *(alterarea integrității datelor informatice),* ci în manipularea conținutului semantic al datelor, o *„re-scriere a realității digitale”*, care poate influența percepția, decizia sau voința persoanelor. Acest tip de acțiune nu presupune neapărat o *„atingere”* în sens tehnic, ci o *reconfigurare a sensului* informației.

  Astfel, dacă în paradigma clasică a infracțiunilor informatice elementul material era localizat în sfera tehnică, în actul de *acces, modificare, distrugere ori împiedicare a*

[35] Floridi, L., *The Logic of Information: A Theory of Philosophy as Conceptual Design*, Oxford University Press, 2019;
[36] ENISA, *AI-driven Disinformation and Deepfake Threat Landscape Report*, European Union Agency for Cybersecurity, 2024.

funcționării unui sistem informatic, în noua paradigmă post-digitală accentul se plasează pe dimensiunea simbolică și cognitivă a acțiunii. Subiectul activ nu mai *„distruge date”*, ci distorsionează adevărul informațional, generând efecte similare, uneori chiar mai grave decât o simplă compromitere tehnică a sistemului.

- **insuficiența aplicării prin analogie a dispozițiilor privind falsul informatic sau răspândirea de informații false.** În fața noilor forme de manifestare a criminalității digitale apare tentația de a recurge la aplicarea prin analogie a unor texte legale existente, precum art. 249 din Codul penal - frauda informatică, art. 324 din Codul penal – falsificarea unei înregistrări tehnice, art. 325 din Codul penal – falsul informatic, art. 226 din Codul penal – violarea vieții private, art. 404 din Codul penal - răspândirea de informații false.
  Cea mai apropiată reglementare incidentă este infracțiunea de falsificare a unei înregistrări tehnice, prevăzută de art. 324 din Codul penal, întrucât aceasta sancționează alterarea autenticității unui material audio, video sau fotografic destinat să servească drept mijloc de probă. Totuși, această incriminare nu corespunde în mod deplin realităților juridice generate de manipularea informațională prin mijloace algoritmice, întrucât falsificarea unei înregistrări tehnice presupune existența unui suport concret, o probă preexistentă supusă modificării, în timp ce falsul realizat prin sisteme de inteligență artificială operează într-un registru imaterial și generativ, în care conținutul falsificat este creat de la zero, fără un original de referință.
  Prin urmare, deși art. 324 din Codul penal exprimă un pas important spre adaptarea dreptului penal la mediul digital, el nu reușește să surprindă specificul noilor forme de fals, în care valoarea socială protejată nu mai este autenticitatea unui document probator, ci autenticitatea percepției realității însăși în spațiul informațional.
  O asemenea abordare, de analogie a situațiilor noi cu dispoziție existente se dovedește insuficientă și riscantă din perspectiva principiilor fundamentale ale dreptului penal, în special *nullum crimen, nulla poena sine lege certa et stricta,* reprezentând o extindere a sferei penale în afara limitelor legale, ceea ce ar contraveni nu doar principiului *legalității incriminării*, ci și exigenței de *previzibilitate a normei penale* impuse de jurisprudența CEDO;
- **tendința europeană de instituționalizare a responsabilității pentru utilizarea AI, în special în ceea ce privește deepfake-urile, conform AI Act (2024) și Recomandării OCDE privind guvernanța inteligenței artificiale (2023).** Pe măsură ce tehnologiile AI, în special cele generative (deep learning, modele generative, generarea de imagini video) devin tot mai sofisticate și accesibile, riscul de abuz, manipulare informațională, dezinformare, încălcare a demnității umane sau prejudicii morale și materiale crește.
  Pentru a răspunde acestui nou peisaj, Uniunea Europeană și organisme internaționale precum OCDE au început să contureze reguli și principii care să asigure responsabilitatea

actanților în lanțul AI (dezvoltatori, distribuitori, utilizatori), nu doar din perspectiva eticii și autorizării, ci și din perspectiva răspunderii legale.[37]

Această tendință de instituționalizare a responsabilității urmărește să evite situațiile în care victimele prejudiciilor cauzate de AI rămân lipsite de mijloace efective de remediere, datorită dificultății de a identifica vinovăția, legătura de cauzalitate sau contribuția tehnologică.

Propunere de lege ferenda

Se propune completarea Titlului VI – Infracțiuni de fals, din Codul penal, cu un nou capitol, Capitolul IV, denumit *„Falsificarea conținuturilor generate automat”,* care să cuprindă următoarele articole:

Articolul 328¹ Falsificarea digitală prin inteligență artificială

(1) **Crearea** ori **modificarea**, prin mijloace de inteligență artificială, a unor imagini, înregistrări audio, video ori a oricărui alt tip de conținut digital care prezintă, în mod realist, o persoană reală implicată în acțiuni, fapte sau declarații neautentice, cu sau fără consimțământul său, **dacă făptuitorul folosește conținutul** digital astfel creat ori modificat **ori îl încredințează altei personae spre folosire**, precum și **folosirea de către altă persoană a unui conținut** digital falsificat prin inteligența artificială, cunoscând caracterul său neautentic, cu scopul de a induce în eroare publicul ori de a produce o consecință juridică, se pedepsește cu închisoare de la 1 la 5 ani.

(2) Dacă fapta prevăzută la alin. (1) a fost săvârșită în una dintre următoarele împrejurări:

a) fără consimțământul persoanei reprezentate și a avut ca urmare lezarea demnității, reputației ori vieții private;

b) prin diseminarea publică a conținutului digital falsificat;

c) în scopul obținerii unui folos patrimonial;

d) în scopul influențării procesului electoral;

limitele speciale ale pedepsei se majorează cu jumătate.

(3) Dacă fapta prevăzută la alin. (1) a fost săvârșită în scopul afectării securității naționale, pedeapsa este închisoarea de la 10 la 20 de ani.

(4) Tentativa se pedepsește.

Articolul 328² Clonarea biometrică neautorizată

Reproducerea, stocarea sau utilizarea, prin mijloace automatizate, a datelor biometrice vocale ori faciale ale unei persoane în scopul generării unui model digital apt să reproducă vocea, chipul ori gesturile acesteia, fără consimțământul său expres, constituie infracțiune și se pedepsește cu închisoare de la **6 luni la 3 ani**.

[37] Advancing accountability in AI, Governing and managing risks throughout the lifecycle for trustworthy AI, https://www.oecd.org/en/publications/advancing-accountability-in-ai_2448f04b-en.html?utm_source=chatgpt.com

Articolul 328³ – Fabricarea și utilizarea de realități simulate

(1) **Crearea** sau **modificarea** de medii digitale, conținuturi ori evenimente simulate, generate prin mijloace de inteligență artificială, apte să substituie realitatea obiectivă și să determine comportamente sociale, economice sau politice bazate pe eroare, **dacă făptuitorul folosește conținutul** digital astfel creat ori modificat **ori îl încredințează altei personae spre folosire**, precum și **folosirea de către altă persoană a unui conținut** digital falsificat prin inteligența artificială, cunoscând caracterul său neautentic, cu scopul de a induce în eroare publicul ori de a produce o consecință juridică, se pedepsește cu închisoare de la 1 la 5 ani.

(2) Dacă fapta prevăzută la alin. (1) a fost săvârșită în una dintre următoarele împrejurări:

a) fără consimțământul persoanei reprezentate și a avut ca urmare lezarea demnității, reputației ori vieții private;

b) prin diseminarea publică a conținutului digital falsificat;

c) în scopul obținerii unui folos patrimonial;

d) în scopul influențării procesului electoral;

limitele speciale ale pedepsei se majorează cu jumătate.

(3) Dacă fapta prevăzută la alin. (1) a fost săvârșită în scopul afectării securității naționale, pedeapsa este închisoarea de la 10 la 20 de ani.

(4) Tentativa se pedepsește.

Concluzii

Transformările accelerate generate de inteligența artificială au forțat dreptul penal să se confrunte, poate pentru prima dată în istoria sa recentă, cu o realitate pe care nu o mai poate controla prin instrumentele tradiționale. În timp ce provocarea secolului XX a fost criminalitatea economică digitală, realitatea prezentă conturează o nouă categorie: criminalitatea algoritmică, acea zonă gri în care voința umană și decizia automată se contopesc.

Această simbioză ridică o întrebare esențială: unde regăsește vinovăția, dacă fapta este rezultatul unei interacțiuni între om și sistemul inteligent?

Codul penal actual, chiar și în forma sa modernizată, nu oferă încă o infrastructură normativă capabilă a răspunde unor conduite precum manipularea deliberată a datelor de antrenament ale unui model AI, falsificarea ieșirilor generate de un sistem algoritmic autonom sau crearea de conținuturi digitale apte să producă consecințe juridice.

Din această perspectivă, propunerea legislative de completare a Titlului VI din Codul penal nu reprezintă doar un exercițiu conceptual, ci o necesitate practică. Introducerea unei infracțiuni de tipul „Falsificarea digitală prin inteligență artificială” ar constitui o armonizare a realității tehnologice și a valorilor fundamentale pe care dreptul penal le protejează: adevărul, siguranța, încrederea socială. Într-un univers dominat de date, falsul nu mai este un simplu act material, ci o distorsiune a realității digitale, o alterare invizibilă dar profundă a informației care guvernează decizia umană.

Mai mult, această nouă dimensiune a falsului transcende noțiunea clasică de *fals intelectual* sau *fals material*. Algoritmii pot genera, modifica și disimula date într-o manieră care eludează percepția senzorială și controlul rațional. Așadar, nu mai putem vorbi doar despre intenția de a induce în eroare o autoritate publică sau o persoană determinată, ci despre o intenție extinsă, orientată spre subminarea sistemului de încredere digitală care stă la baza societății moderne.

De aceea, abordarea penală trebuie să se repoziționeze, să părăsească granițele riguroase și să admită că obiectul protecției juridice se extinde dincolo de relațiile interumane, către relațiile om–mașină și chiar mașină–mașină. Această realitate impune chiar și o reinterpretare a noțiunilor de autor, participant, instigator, atunci când acțiunea delictuală este mediată de un sistem algoritmic.

Pe de altă parte, dimensiunea morală a tehnologiei nu poate fi separată de cea juridică. Inteligența artificială nu este doar o chestiune de eficiență sau precizie, ci și una de responsabilitate. Moralitatea trebuie să ghideze nu doar modul în care pedepsim abuzurile tehnologice, ci și felul în care permitem dezvoltarea lor, pentru ca progresul să rămână un mijloc în slujba omului, nu o forță care îl depășește. Pe măsură ce aceste tehnologii continuă să evolueze, profesioniștii dreptului trebuie să rămână gardienii vigilenți ai justiției, asigurându-se că inovația servește legea, și nu o subminează.[38]

Urmare aceste logici, dreptul penal rămâne, paradoxal, cea mai umană dintre științele juridice, pentru că el nu sancționează mașinile, ci intențiile, nu algoritmii, ci valorile care sunt trădate prin intermediul lor.

Astfel, legea propusă nu urmărește o reacție punitivă oarbă, ci reafirmarea unui principiu de echilibru: tehnologia trebuie să servească omul, nu să îl substituie. Doar printr-o reinterpretare lucidă, interdisciplinară și profund etică a noilor forme de criminalitate, dreptul penal își va putea păstra vocația originară: aceea de a proteja omul, chiar și atunci când amenințarea nu mai are chip, ci algoritm.

ABREVIERI:

- AI – Artificial Inteligence (inteligența artificială);
- DDOS - Distributed Denial of Service;
- DoS/DdoS - Denial of Service;
- DNSC - Directoratul Național de Securitate Cibernetic;
- ENISA - Agenția Uniunii Europene pentru Securitate Cibernetică;
- IBM - International Business Machines Corporation;
- OCDE - Organizația pentru Cooperare și Dezvoltare Economică;
- SRI – Serviciul Român de Informații.

Referințe bibliografice:

- Hussein Jassim Akeiber, "A comprehensive study of Cybercrime and Digital Forensics through Machine Learning and AI", *Rafidain J. Eng. Sci.*, vol. 3, no. 1, pp. 369–395, Feb. 2025;

[38] NiaLena Caravasos - Law Office of NiaLena Caravasos, 11.05.2025, https://nialena.com/ai-in-criminal-law-benefits-risks-ethical-issues/?utm_source=chatgpt.com, pagină web consultată la data de 15.10.2025;

- Regner Sabillon, Jeimy Cano, Victor Cavaller, jordi Serra - Cybercrime and Cybercriminals: A Comprehensive Study, International Journal of Computer Networks and Communications Security, vol. 4, no. 6, June 2016, p. 166;
- Regner Sabillon, Jeimy Cano, Victor Cavaller, jordi Serra - Cybercrime and Cybercriminals: A Comprehensive Study, International Journal of Computer Networks and Communications Security, vol. 4, no. 6, June 2016, p. 166;
- Waqas. "The Evolution of Cybercrime Investigation". Jul 2024;
- Waqas- The evolution of cybercrime investigation, 14 July 2024, https://hackread.com/the-evolution-of-cybercrime-investigations;
- European Parliament policies – Insight - Understanding cybercrime, European Union, 2024, p. 2;
- European Parliament policies – Insight - Understanding cybercrime, European Union, 2024, p. 4,5;
- Mekhail Mustak et al. - Deepfakes: Deceptions, mitigations, and opportunities, Journal of Business Research, Volume 154, January 2023, 113368, https://www.sciencedirect.com/science/article/abs/pii/S0148296322008335 , pagină web consultată în data de 12.10.2025;
- Mohamed Lazzouni - Voice Cloning: What It Is and Why It's Scary, 14.06.2023, https://builtin.com/artificial-intelligence/what-is-voice-cloning, pagină web consultată la data de 12.10.2025;
- Tim Cotten - Autonomous Virtual Beings, Jan 5, 2024, https://blog.cotten.io/autonomous-virtual-beings-aaef7cbbe5de, pagină web consultată la data de 12.10.2025;
- João Phillipe Cardenuto et al., The Age of Synthetic Realities: Challenges and Opportunities, Fri, 9 Jun 2023, arXiv:2306.11503, pagină web consultată la data de 12.10.2025;
- European Parliament policies – Insight - Understanding cybercrime, European Union, 2024, p. 3,4;
- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32001F0413, pagină web consultată la data de 12.10.2025;
- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32004F0068, pagină web consultată la data de 12.10.2025;
- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32005F0222, pagină web consultată la data de 12.10.2025;
- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32011L0093, pagină web consultată la data de 12.10.2025;
- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32013L0040, pagină web consultată la data de 12.10.2025;
- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32019L0713, pagină web consultată la data de 12.10.2025;
- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555, pagină web consultată la data de 12.10.2025;
- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022R2554, pagină web consultată la data de 12.10.2025;
- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R2847, pagină web consultată la data de 12.10.2025;
- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R0903, pagină web consultată la data de 12.10.2025;

- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2557, pagină web consultată la data de 12.10.2025;
- https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng?utm_source=chatgpt.com pagină web consultată la data de 12.10.2025;
- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32013L0040, pagină web consultată la data de 12.10.2025;
- https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32019L0713, pagină web consultată la data de 12.10.2025;
- Art. 52 din Regulamentul (UE) 2024/1689 privind inteligența artificială (AI Act);
- Floridi, L., *The Logic of Information: A Theory of Philosophy as Conceptual Design*, Oxford University Press, 2019;
- ENISA, *AI-driven Disinformation and Deepfake Threat Landscape Report*, European Union Agency for Cybersecurity, 2024;
- Advancing accountability in AI, Governing and managing risks throughout the lifecycle for trustworthy AI, https://www.oecd.org/en/publications/advancing-accountability-in-ai_2448f04b-en.html?utm_source=chatgpt.com;
- NiaLena Caravasos - Law Office of NiaLena Caravasos, 11.05.2025, https://nialena.com/ai-in-criminal-law-benefits-risks-ethical-issues/?utm_source=chatgpt.com, pagină web consultată la data de 15.10.2025.