Incidența caracterului infracțional al fenomenului deepfake în domeniul financiar-bancar - noua formă a jafului perfect?

Sebastian-Andrei COFAS[1]
Iulia-Alexandra DIDU[2]

Abstract

Raporturile juridice s-au transformat în mod drastic, ca urmare a dezvoltării și utilizării frecvente a noilor tehnologii, fie că vorbim despre Inteligența Artificială sau Blockchain, în special în lumina utilizării excesive a acestora în fiecare activitate a vieții noastre cotidiene. Această revoluție tehnologică, plecând de la dezideratul dezvoltării socio-economice a umanității, a condus la comunicare instantanee și la informații ușor disponibile doar la un click distanță, facilitând conexiunea interumană, colaborarea și accesarea unor cunoștințe și informații la o scară fără precedent, dar și de îmbunătățire a unor aspecte esențiale indispensabile societății, precum aplicarea legii și optimizarea operațiunilor financiar-bancare atât pentru clienți, cât și pentru furnizori. Totuși acest progres poate fi asimilat unei săbii cu două tăișuri, deoarece prezintă și noi oportunități pentru activități infracționale. Fiindcă dependența umană de tehnologie este într-o continuă creștere, direct proporțional se maximizează și vulnerabilitățile care pot fi exploatate în ducerea la bun sfârșit a rezoluției infracționale și, totodată, consacrarea fenomenului "deepfake" drept cea mai nouă formă a infracțiunii de înșelăciune. Deepfake este o tehnologie cu potențial contradictoriu, chiar pozitiv în arii precum divertismentul, cultura și educația, însă abilitatea sa de a manipula realitatea ridică preocupări majore, în special în sistemul financiar-bancar. Această lucrare caracterizează și analizează din punct de vedere juridic, economic și social incidența caracterului infracțional al acestei tehnologii din perspectiva funcționării ei, dar și din cea a legislației în vigoare la momentul actual.

Legal relations have drastically transformed due to the development and widespread use of new technologies, whether we are talking about Artificial Intelligence or Blockchain, especially in light of their excessive use in every aspect of our daily lives. This technological revolution, aimed at the socio-economic development of humanity, has led to instant communication and readily available information just a click away, facilitating interhuman connection, collaboration, and access to knowledge and information on an unprecedented scale. It has also improved essential aspects of everyday life, such as law enforcement, and optimization of financial-banking operations for both clients and providers. But even this progress can be likened to a double-edged sword because it presents new opportunities for criminal activities. As human dependence on technology continues to grow, vulnerabilities that can be exploited in carrying out criminal resolutions are maximized, thus solidifying the "deepfake" phenomenon as the newest form of deception. Deepfake is a technology with contradictory, even positive potential in areas such as entertainment, culture, and education, but its ability to manipulate reality raises major concerns, especially in the financial-banking system. This paper characterizes and analyzes from a legal, economic, and social perspective the incidence of the criminal nature of this technology in terms of its functioning, as well as from the standpoint of current legislation.

[1] Student, Facultatea de Drept, Academia de Studii Economice din București, cofassebastian21@stud.ase.ro
[2] Student, Facultatea de Drept, Academia de Studii Economice din București, diduiulia19@stud.ase.ro

Cuvinte-cheie: *deepfake, caracter infracțional, înșelăciune, sistemul financiar-bancar, vulnerabilitate socială, riscuri*

1. Introducere

1.1 Definiția deepfake-ului ca formă a tehnologiei.

Conform Propunerii Legislative privind utilizarea responsabilă a tehnologiei în contextul fenomenului deepfake 471/2023, art. 2 caracterizează acest concept ca „[...] orice conținut falsificat de tip imagine, audio și/sau video realizat, de regulă, cu ajutorul inteligenței artificiale, a realității virtuale (RV), a realității augmentate (AR) sau altor mijloace, astfel încât să creeze aparența că o persoană a spus sau a făcut lucruri, pentru care nu și-a dat consimțământul, care în realitate nu au fost spuse sau făcute de acea persoană". Proiectul de Lege (PL) nr. 471/2023 privind utilizarea responsabilă a tehnologiei în contextul fenomenului deepfake reflectă o mentalitate proactivă și parțial echilibrată a legiuitorului român, care recunoaște atât potențialul, cât și riscurile asociate cu această formă de tehnologie. Considerăm că Proiectul Legislativ, care pune accent pe responsabilitate, transparență, educație și cooperare, ar putea contribui la crearea unui mediu digital mai sigur și mai informat, având capacitatea de a alinia cadrul legislativ autohton cu standardele Uniunii Europene.

Din punct de vedere practic, deepfake-ul ca tehnologie emergentă, reprezintă o sinergie a doi algoritmi complecși, bazați pe inteligența artificială, care se cuantifică într-o așa numită Rețea Generativă Adversarială (GAN) sau autoencoderi. Astfel în primul caz, „generatorul" și „discriminatorul" formează un motor dublu care creează și rafinează conținutul, dar care mai poate descifra, prin deep learning, anumite tipare autentice din elemente reale precum înfățișarea sau vocea, perfecționându-și abilitatea de a crea copii fidele și de a detecta imperfecțiunile, corectându-se singur. Totodată și cel de-al doilea caz prezintă particularități similare, inteligența artificială din spatele unui deepfake bazându-se tot pe două elemente: „encoder" (compresorul - comprimă datele de intrare într-o reprezentare mai mică, denumită spațiu latent) și „decoder" (decompresor - reconstruiește datele originale din reprezentarea latentă). Mai exact, autoencoderul încearcă să captureze caracteristicile cheie ale datelor și să le stocheze într-un format mai redus, diferențiindu-se față de Rețelele Generative Adversariale prin așa numitul „self-supervised deep learning" (învățarea profundă auto-supervizată) care permite modelului să învețe din date neetichetate. Spre deosebire de învățarea supravegheată tradițională, care are nevoie de seturi mari de date etichetate manual (de exemplu, imagini etichetate cu tipul de obiect din imagine), această tehnică AI își creează propriile etichete folosind datele în sine.

1.2 Relevanța temei pentru sistemul financiar-bancar și societate. Contextul actual

În ultima vreme, atacatorii au intensificat utilizarea rețelelor de social media pentru a promova diverse tipuri de tentative de fraudă, cele mai cunoscute fiind cele cu oferte de investiții false, care au căpătat anvergură în urma listării companiei de stat Hidroelectrica la Bursa de Valori București[3], subiectul devenind destul de răspândit în rândul populației. Astfel, în efortul lor de a fi cât mai convingători, persoanele din spatele acestor acțiuni ilicite se bazează pe conturi sau pagini de social media compromise sau nou create, din care lansează asemenea reclame sponsorizate, care de obicei includ clipuri alterate cu tehnologia deepfake. Infractorii construiesc mesajele lor într-un mod astfel încât să facă ca personalități publice din diverse sectoare să pară că susțin astfel de „scheme de îmbogățire", consolidându-si credibilitatea. Astfel, ei distorsionează și manipulează imaginea unor companii binecunoscute, astfel încât să poată obține mai ușor încrederea celor vizați în legătură cu autenticitatea ofertei respective. Această abordare include promovarea unor câștiguri imediate semnificative prin intermediul achiziționării de acțiuni care presupun dividende de zeci de mii de lei. În prezent, se constată că majoritatea companiilor a căror imagine este abuziv utilizată se concentrează în principal în domeniul energetic.

Mai preocupant este faptul că acești atacatori exploatează inițial metode legale de publicitate, precum reclamele sponsorizate pe platforme populare precum Google Ads. Problema esențială constă în faptul că unele dintre aceste platforme nu verifică în mod adecvat conținutul reclamelor, permițând astfel promovarea mesajelor frauduloase și a schemelor de înșelăciune, oferindu-le acestora un vehicul legitim pentru a-și răspândi mesajele înșelătoare, profitând de lacunele în sistemul de verificare a conținutului publicitar.

Astfel, așa cum am menționat și anterior, sectorul financiar-bancar este în principal vizat, de multe ori indirect, întrucât clienții acestor actori economici căzând în plasa acestor înșelătorii. Metoda prin care persoanele se pot îmbogăți peste noapte prin diverse investiții în companiile de stat a devenit din ce în ce mai des regăsită și preferată de către infractori, întrucât persoana în cauză, de bună voie și nesilită de nimeni, își oferă direct datele de contact și cele financiare, iar în cazul anumitor metode mai dezvoltate li se cere instalarea aplicațiilor de tipul AnyDesk[4] pe dispozitivul mobil prin intermediul cărora, persoanele rău voitoare pot controla de la distanță respectivul telefon și profitând de starea de vădită vulnerabilitate a persoanei

[3] A se vedea *Aprobarea și publicarea prospectului în legătură cu IPO-ul Hidroelectrica*, disponibil online: https://m.bvb.ro/FinancialInstruments/SelectedData/NewsItem/FP-Aprobarea-si-publicarea-prospectului-in-legatura-cu-IPO-ul-Hidroelectrica/34CFE, data ultimei accesări: 16.03.2023

[4] AnyDesk este o aplicație de control la distanță, utilizată pentru a accesa și controla un computer sau un dispozitiv de la distanță, facilitând suportul tehnic, colaborarea și accesul la fișiere și programe de la distanță. A se vedea *AnyDesk features,* disponibil online: https://anydesk.com/en/features, data ultimei accesări: 16.03.2023

care până în acel moment nu a realizat că este victima unei înşelăciuni, accesează în numele acesteia diverse produse bancare, precum credite, urmând să transfere sumele de bani către conturi terțe, pentru a le fi pierdută. De obicei, până când organele antifraudă ale instituțiilor bancare identifică aceste transferuri suspecte sau clientul se trezește cu acele rate sau alte produse active, sumele de bani şi infractorii sunt deja de negăsit.

Pe de altă parte, deepfake-ul poate fi utilizat şi în cadrul interacțiunilor cu operatorii de call center pentru a avea acces la diverse informații sensibile, vocea clientului putând fi emulată de către această tehnologie, iar întrebările de identificare putând fi trecute cu ușurință (de obicei se referă la CNP, agenția/sucursala la care clientul a intrat prima dată în relație cu Banca etc.). Totodată şi sistemele de identificare biometrică a aplicațiilor de online banking care permit autentificarea, certificarea anumitor acțiuni sau accesarea de la distanță a produselor de banking pot fi păcălite de către aceste persoane răuvoitoare. Pe de cealaltă parte, şi clientul poate fi victima unei înşelătorii, crezând că interacționează cu o sursă autentică, spre exemplu implementarea recentă a programelor de online boarding a clienților (viitorul client completează un formular online pe care îl va valida cu adresa de email şi/sau numărul de telefon, urmând a fi contactat în format video de către un angajat al respectivei instituții bancare pentru a definitiva procesul respectiv de înrolare). În paralel, aplicații aparent inofensive permit utilizatorilor să experimenteze cu aspectul/vocea lor, dar s-au semnalat şi cazuri în care datele încărcate au fost colectate fără consimțământul utilizatorilor, devenind parte a procesului de învățare a inteligenței artificiale.

1.3 Obiectivele şi metodologia lucrării

Studiul elaborat are ca scop central oferirea unei analize aprofundate a acestei noi amenințări la adresa securității financiare. Prin metodologia sa riguroasă şi prin rezultatele obținute, ne dorim să oferim informații relevante şi actuale care să conducă la combaterea mai eficientă a infracțiunilor cu deepfake şi la protejarea atât a cetățenilor în calitate de subiecți pasivi ai infracțiunilor, cât şi a instituțiilor financiare afectate direct sau indirect de aceasta.

Prin prezenta lucrare, se doresc a se găsi răspunsuri cât mai clare şi relevante pentru domeniul abordat la întrebările: "*Ce impact are factorul cultural/social al cetățeanului în momentul în care este susceptibil unei conduite infracționale în domeniul bancar?", "Cum au evoluat infracțiunile clasice asupra patrimoniului sub impactul digitalizării?"* şi, nu în ultimul rând, *"Ce mijloace de prevenție avem la îndemână la momentul actual şi cum pot fi îmbunătățite?"*.

Astfel, ne propunem să atingem următoarele obiective:

➢ *Analiza aprofundată a fenomenului deepfake* prin studierea definiției, tehnicilor de creare şi a tipurilor de deepfake-uri relevante pentru domeniul financiar-bancar.

➢ *Evaluarea riscurilor* prin identificarea principalelor vulnerabilități ale sistemelor financiare și bancare la atacurile cu deepfake.

➢ *Analiza legislației actuale* prin studierea cadrului legal existent în România și la nivel internațional în ceea ce privește infracțiunile ce pot fi săvârșite prin utilizarea tehnologiei deepfake.

➢ *Identificarea tipologiilor infracționale*, prezentând în mod concret și la obiect modalitățile prin care deepfake-urile pot fi utilizate pentru a comite infracțiuni financiare și bancare.

➢ *Analiza de cazuri*, abordând unele exemple concrete de infracțiuni cu deepfake din domeniul financiar-bancar.

➢ *Evaluarea eficienței metodelor de combatere*, prin mijloace de prezentare și analiza soluțiilor existente pentru combaterea infracțiunilor cu deepfake.

➢ *Formularea de propuneri de lege ferenda* și adaptarea propunerii de lege actuale la ingerințele reale și integrarea coerentă a sa în legislația în vigoare

Cu privire la metodologia cercetării, *am colectat sursele de informare printr-o documentare riguroasă,* ce s-a materializat prin examinarea legislației în vigoare, atât la nivel național cât și internațional, a articolelor științifice, a rapoartelor de specialitate și a altor materiale relevante și, bineînțeles, am studiat în detaliu exemple concrete de infracțiuni comise prin deepfake din domeniul financiar-bancar, pentru a putea compara caracterul infracțional al deepfake-ului cu alte infracțiuni comise prin utilizarea sistemelor informatice, prezente în Codul Penal.

Rezultatele așteptate în urma cercetării privesc o analiză detaliată a riscurilor și a vulnerabilităților asociate cu deepfake-urile în domeniul financiar-bancar, formularea unor propuneri concrete de îmbunătățiri legislative pentru a combate mai eficient caracterul infracțional al deepfake-ului și, implicit, creșterea gradului de conștientizare a publicului cu privire la riscurile deepfake-urilor și la metodele de protecție și prevenție.

2. Deepfake

2.1 Caracterizarea juridică a deepfake-ului

Deepfake-ul, tehnologia de manipulare video și audio aflată în ascensiune, ridică o serie de provocări din punct de vedere juridic. Încadrarea utilizării deepfake-ului în scopuri malițioase în tipare infracționale existente necesită o analiză atentă a contextului și a legislației actuale și autohtone, așa cum urmează în secțiunile următoare.

2.1.1 Infracțiuni posibile facilitate de deepfake în domeniul bancar

Deepfake-ul, această tehnologie fascinantă care poate manipula imagini și videoclipuri cu o ușurință uimitoare, ridică o serie de semne de întrebare din punct de vedere juridic. *Cum se încadrează această nouă formă de manipulare în legislația existentă? Există asemănări cu alte infracțiuni deja cunoscute?*

O analiză atentă dezvăluie o legătură strânsă între deepfake și infracțiunea de fals informatic[5]. Deși distincte ca formă, ele împărtășesc o serie de caracteristici comune, precum *intenția de a induce în eroare* și *cauzarea unui prejudiciu potențial*. Atât deepfake-ul, cât și falsul implică crearea și folosirea de informații false[6] cu scopul de a induce în eroare o persoană sau o autoritate. Indiferent de metoda utilizată, fie prin manipularea imaginilor (deepfake), fie prin mijloace tradiționale (fals clasic), scopul final rămâne același: obținerea unui avantaj nejustificat prin inducerea în eroare[7]. De asemenea, ambele pot provoca prejudicii semnificative victimelor, afectând reputația, imaginea, viața personală sau chiar interesele financiare. Gravitatea prejudiciului poate varia în funcție de contextul specific al fiecărei infracțiuni, dar potențialul de a cauza daune este prezent în ambele cazuri.

Art. 244 alin. (1) din Codul Penal reglementează în mod specific forma standard a infracțiunii de înșelăciune[8], având ca element material "inducerea în eroare a unei persoane, prin prezentarea ca adevărată a unei fapte mincinoase sau ca mincinoasă a unei fapte adevărate, în scopul de a obține pentru sine sau pentru altul un folos patrimonial injust și dacă s-a pricinuit o pagubă." De asemenea, alin. (2) al aceluiași articol caracterizează forma agravată a înșelăciunii prin "prin folosirea de nume sau calități mincinoase ori de alte mijloace frauduloase". Infracțiunea de înșelăciune este caracterizată prin faptul că, fiind una contra patrimoniului, inducerea în eroare trebuie să se concretizeze prin producerea unei pagube persoanei vătămate[9]. Analizând elementele constitutive ale infracțiunii, dar și textul de incriminare, putem include deepfake-ul în forma actualizată a înșelăciunii, cunoscută și drept înșelăciune electronică, din categoria de cybercrimes, deoarece manipularea este înfăptuită asupra victimei, prin mijloace electronice[10].

În lumea digitală, înșelăciunea poate îmbrăca forme inedite, chiar inovatoare. Una dintre cele mai răspândite metode este *phishing-ul*[11], unde atacatorii se deghizează în instituții de încredere pentru a obține date confidențiale precum parole bancare sau informații despre carduri de credit. Folosind e-mailuri sau mesaje instant false, aceștia creează o platformă credibilă, direcționând utilizatorul către site-uri web imitate perfect, pentru a fura datele introduse. *Spam-ul*[12], o altă metodă

[5] A se vedea Noul Cod Penal, Titlul VI - Infracțiuni de fals, Capitolul III - Falsuri în înscrisuri, art. 325

[6] G. Zlati, Tratat de criminalitate informatică. Vol. I, Editura Solomon, București, 2020, p. 430

[7] M. Udroiu, *Sinteze de Drept Penal. Partea Specială*, Vol. I, editura C.H. Beck, 2023, pp. 609-610

[8] A se vedea Noul Cod Penal, Titlul II - Infracțiuni contra patrimoniului, Capitolul III - Infracțiuni contra patrimoniului prin nesocotirea încrederii, art. 244

[9] T. Manea, C. N. Constantinescu-Mărunțel, H. Ș. Tiugan, *Drept penal. Partea specială. Infracțiuni contra persoanei. Infracțiuni contra patrimoniului*, editura Hamangiu, București, 2022, p. 484

[10] G. Zlati, *Criminalitatea informatică în România*, Jurnalul Baroului Cluj, nr. 1, 2021, p. 28

[11] A se vedea *National Institute of Standards and Technology Computer Security Research Center*, disponibil online: https://csrc.nist.gov, data ultimei accesări: 16.03.2023.

[12] A se vedea *National Institute of Standards and Technology Computer Security Research Center*, disponibil online: https://csrc.nist.gov, data ultimei accesări: 16.03.2023.

neplăcută, inundă utilizatorii cu mesaje electronice nesolicitate, promovând produse sau servicii nedorite. Adresele de e-mail sunt obținute adesea prin metode ilegale, transformând cutia poștală într-un spațiu aglomerat de informații inutile. *Escrow*[13], o metodă mai puțin cunoscută, implică licitații false, menite să manipuleze prețurile și să înșele utilizatorii naivi. În cele din urmă, *carding-ul*[14] folosește mesaje spam cu actualizări false pentru a fura date de conturi eBay sau Paypal. Prin modificări ale codului sursă al paginii web originale, informațiile sunt trimise către atacator, care le utilizează ulterior pentru achiziții frauduloase sau crearea de site-uri false. Aceste metode de înșelăciune electronică necesită vigilență din partea utilizatorilor și măsuri de securitate sporite din partea platformelor online. La toate acestea, se va adăuga fenomenul tehnologic al *deepfake-ului*, care poate lua diverse forme, precum imitarea vocii un client bancar real, solicitând telefonic o resetare a parolei și transferul ulterior al fondurilor către un cont fraudulos, sau crearea unui videoclip deepfake cu un CEO al unei companii mari anunțând o fuziune importantă poate manipula piața de valori, determinând creșterea artificială a prețurilor acțiunilor.

Concluzionând această secțiune, este demn de remarcat faptul că deepfake-ul poate fi privit ca o nouă formă de înșelăciune, cu valențe caracteristice infracțiunilor de fals și celor comise utilizând un sistem informatic, însă reglementarea sa clară și la obiect lipsind momentan cu desăvârșire din legislația națională. Mai mult decât atât, deepfake-ul prezintă un risc semnificativ pentru sectorul financiar-bancar, necesitând o abordare proactivă și o colaborare intersectorială, economico-juridică, pentru a combate eficient infracțiunile facilitate de această tehnologie emergentă.

2.1.2 Analiza legislației în vigoare în România și la nivel internațional. Deficiențe legislative și provocări în combaterea deepfake-ului

Dacă acum aproape 80 de ani Mihail Sadoveanu spunea faptul că „Lumina vine de la răsărit”, în prezent aceasta cu siguranță vine de la Bruxelles, în special în materia garantării și respectării drepturilor omului, dar și în ceea ce privește echitatea în transformarea digitală. Astfel, cu privire la materia deepfake-ului, la nivelul Uniunii Europene regăsim relevante izvoare legislative precum: Regulamentul general privind protecția datelor (GDPR)[15], Actul legislativ privind serviciile digitale (DSA - Digital Services Act)[16] și Actul privind Inteligența Artificială (AI Act)[17].

[13] Ibidem
[14] Ibidem
[15] A se vedea Regulamentul (UE) 2016/679 (General Data Protection Regulation) privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE
[16] A se vedea Regulamentul (UE) 2022/2065 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE
[17] A se vedea propunere de Regulament (UE) de Stabilire a unor Norme Armonizate privind Inteligența Artificială și de Modificare a anumitor Acte Legislative ale Uniuni

Cel din urmă document conține cele mai importante prevederi în ceea ce privește reglementarea dezvoltării și utilizării inteligenței artificiale (AI) în diverse sectoare. având ca scop crearea unui cadru legal armonizat la nivelul Uniunii Europene care să stimuleze inovarea responsabilă în domeniul AI și să protejeze drepturile și siguranța cetățenilor statelor membre. Actul normativ propus nu intenționează să interzică direct utilizarea deepfake-urilor, ci încearcă să reglementeze acest lucru prin impunerea unor obligații de transparență asupra creatorilor, cu excepția cazurilor în care se creează/distribuie conținut ilegal sau care poate provoca daune grave, se încearcă manipularea/influențarea pe nedrept a anumitor persoane, respectiv a imita identitatea altei persoane fără consimțământul dat prealabil. Totodată, creatorii de conținut vor fi obligați să dezvăluie prin marcarea conținutului ca fiind generat sau manipulat artificial. Cu toate că această propunere este un prim pas promițător, și ea se confruntă cu anumite provocări persistente, precum reglementarea creatorilor de conținut din afara jurisdicției Uniunii Europene, respectiv modul prin care obligațiile impuse acestora se vor răsfrânge asupra acelora care produc deepfake-uri în calitate personală (spre exemplu uz propriu ca o formă de divertisment).

Cu toate acestea, este important de menționat faptul că deja asemenea acte intră în incidența Regulamentului General privind Protecția Datelor (GDPR)[18], de obicei creatorii de conținut utilizând datele personale, inclusiv imaginea și vocea persoanelor, fără un temei legal, precum consimțământul informat al persoanei înfățișate în deepfake. Totuși, acest Regulament se prezintă a fi destul de anevoios în momentul în care se dorește tragerea la răspundere a persoanelor care au utilizat în mod ilegal aceste tehnologii[19], cât și limitat prin aria pe care o reglementează, un regulament/act separat fiind un deziderat.

Un alt cadru legal relevant este Actul legislativ privind Serviciile Digitale (DSA)[20], care are ca scop reglementarea pieței serviciilor digitale din Uniunea Europeană în special prin combaterea răspândirii conținutului ilegal și dezinformării pe platformele online. De asemenea, prin această directivă furnizorii au responsabilitatea de a elimina cât mai rapid conținutul ilegal atunci când sunt notificați, fie de utilizatori sau de organele competente și li se solicită o mai mare transparență în funcționarea algoritmilor platformelor online, pentru a identifica și contracara informațiile false de orice fel, prin verificarea faptelor și etichetarea conținutului sponsorizat.

Pe plan autohton, pe lângă reglementările de ordin penal, care cuprind în mod extensiv și utilizarea deepfake-ului în mod negativ, se observă apetența legiuitorului român de a reglementa de sine stătător fenomenul deepfake-ului și sancționarea acestuia într-un mod destul de drastic, date fiind consecințele pe care le poate avea asupra victimelor. în special prin inducerea „în eroare a opiniei publice

[18] A se vedea Regulamentul (UE) 2016/679 (General Data Protection Regulation).

[19] Dr. M. G. Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis*, Editura Bloomsbury Publishing, Colecția Hart Publishing, Londra, 2023

[20] A se vedea Regulamentul (UE) 2022/2065 (Digital Services Act)

cu privire la autenticitatea mesajului transmis”[21]. În același timp, legiuitorul a oferit și o definiție a conceptului destul de extensivă, dar a cărei formulare poate indica incriminarea tuturor actelor în care există „aparența că o persoană a spus sau a făcut lucruri, pentru care nu şi-a dat consimţământul, care în realitate nu au fost spuse sau făcute de acea persoană”[22]. Cu toate acestea, este permisă utilizarea și difuzarea unor asemenea materiale în spațiul public atâta timp cât există „un avertisment redat pe cel puțin 10% din suprafața expunerii şi pe toată durata difuzării respectivului conținut vizual sau de un mesaj sonor la începutul și la finalul conținutului audio: „Acest material conține ipostaze imaginare”[23].

O noutate o poate reprezenta reconfirmarea dobândirii a unor noi competențe de către Consiliul Național al Audiovizualului, conform propunerii legislative acestuia revenindu-i rolul de a verifica dacă acel conținutul distribuit sau difuzat „pe internet”[24] sau în „mass-media”[25] încalcă dispozițiilor legii, putând apela și la expertiza tehnică din partea Institutului Naţional de Cercetare – Dezvoltare în Informatică – ICI București[26].

În același timp, din punct de vedere al sancționării acestui act ilicit, se realizează o delimitare între infracțiunile grave din al căror cuprins poate face parte deepfake-ul și acele situații în care în care să nu fie considerate infracțiuni, ci contravenții, fiind sancționată utilizarea acestei tehnici cu o amendă între „10.000 lei la 100.000 lei”[27], iar „dacă fapta are caracter repetat în cel puțin două acțiuni distincte”, se va sancționa „cu amendă de la 20.000 lei la 200.000 lei”[28].

În ceea ce privește constatarea nerespectării dispozițiilor legale, legiuitorul a decis ca aceasta să debuteze fie de la „sesizarea persoanelor prejudiciate ori din oficiu, de către reprezentanţii împuterniciți ai Consiliului Național al Audiovizualului”[29]. Totuși, date fiind implicațiile acestei tehnologii și gradul însemnat al populației care poate fi afectată, considerăm că actul de sesizare ar putea fi realizat atât în mod direct de către persoana vătămată, cât și de către orice persoană interesată care ia la cunoștință de respectivul material. Ulterior acesta poate decide eliminarea[30] conținutului care nu respectă condițiile impuse de propunerea de lege.

2.2 Vulnerabilități ale sistemelor bancare expuse la atacuri deepfake

Atacurile deepfake pot reprezenta o amenințare semnificativă pentru sistemul bancar, expunându-l la diverse vulnerabilități care pot afecta atât instituțiile financiare, cât și pe clienții lor. Impactul acestor atacuri poate fi devastator, deoarece

[21] Propunere Legislativă 471/2023, art. 1
[22] Propunere Legislativă 471/2023, art. 2
[23] Propunere Legislativă 471/2023, art. 3
[24] Ibidem
[25] Ibidem
[26] Propunere Legislativă 471/2023, art. 4, alin. (1)
[27] Propunere Legislativă 471/2023, art 4, alin. (2)
[28] Propunere Legislativă 471/2023, art 4, alin. (3)
[29] Propunere Legislativă 471/2023, art 4, alin. (4)
[30] Propunere Legislativă 471/2023, art 4, alin. (6)

deepfake-urile sunt tot mai sofisticate şi pot fi utilizate în moduri variate pentru a compromite securitatea şi integritatea sistemelor bancare. Conform unui studiu realizat de Centrul de Soluționare Alternativă a Litigiilor în domeniul Bancar, 43% dintre consumatori interacționează cu serviciile bancare atât în biroul băncii, cât şi online, în timp ce 40% doar online, prin aplicații mobile de banking[31], astfel încât peste 80% dintre aceştia pot fi supuşi riscului de a ajunge victime ale unor forme de fraudă utilizând deepfake. În prezenta secțiune, vom prezenta riscurile cele mai semnificative, atât prin prisma instituțiilor bancare, cât şi a consumatorului de servicii în acest domeniu.

Autentificarea bazată pe biometrie: Autentificarea bazată pe biometrie a devenit din ce în ce mai populară în industria bancară datorită nivelului ridicat de securitate şi comodității pe care o oferă. Cu toate acestea, deepfake-urile reprezintă o amenințare semnificativă pentru aceste sisteme, deoarece pot imita cu precizie trăsăturile biometrice ale unei persoane, cum ar fi vocea, aspectul facial sau irisul. Unul dintre cele mai mari riscuri este că un atacator poate utiliza un deepfake video pentru a imita un client bancar şi a accesa contul acestuia prin intermediul unei aplicații mobile de banking. De exemplu, un deepfake video care imită clientul poate fi folosit pentru a înşela sistemul de recunoaştere facială sau vocală al aplicației, permițând accesul neautorizat la informațiile şi fondurile din contul bancar al persoanei respective. Această vulnerabilitate este extrem de periculoasă, deoarece sistemele de autentificare bazate pe biometrie sunt concepute să ofere un nivel ridicat de securitate, iar utilizatorii se bazează pe ele pentru a-şi proteja informațiile financiare şi personale. Atunci când aceste sisteme sunt compromise de deepfake-uri, încrederea clienților în securitatea sistemului bancar poate fi grav afectată, iar pierderea fondurilor şi a datelor personale devine o posibilitate reală.

Canale de comunicare online: Canalele de comunicare online, cum ar fi e-mailul, chat-ul online sau apelurile video, sunt esențiale pentru interacțiunile dintre clienți şi personalul bancar. Cu toate acestea, aceste canale devin vulnerabile în fața atacurilor deepfake, care pot manipula şi falsifica informațiile transmise pentru a induce în eroare personalul bancar şi a obține acces neautorizat la conturi sau informații sensibile. Un exemplu concret ar fi utilizarea unui deepfake audio pentru a imita vocea unui client bancar şi pentru a solicita o resetare a parolei sau transferul de fonduri. În această situație, un atacator ar putea trimite un apel telefonic sau un mesaj vocal către un angajat bancar, folosind o înregistrare deepfake a vocii clientului, solicitând efectuarea unei acțiuni financiare, cum ar fi transferul de bani către un cont controlat de atacator. Această tactică poate fi extrem de eficientă, deoarece personalul bancar poate fi indus în eroare să creadă că ar fi implicat într-o discuție cu un client autentic în rolul interlocutorului şi să execute solicitările acestuia fără a avea suspiciuni. În plus, deepfake-urile audio sau video pot fi utilizate pentru a crea o presiune emoțională sau pentru a induce frică sau panică în rândul

[31] A se vedea *Studiul Centrului de soluționare alternativă a litigiilor în domeniul bancar (CSALB) cu privire la interacțiunea consumatorilor cu băncile* https://www.linkedin.com/posts/csalb_csalb-isensesolutions-banking-activity-7173244337957318657-lqP2?utm_source=share&utm_medium=member_ios, data ultimei accesări: 15.03.2024

angajaților bancari, determinându-i să acționeze rapid și fără a verifica autenticitatea solicitării.

Sisteme de procesare automată: Sistemele de procesare automată sunt esențiale în operațiunile bancare moderne, fiind folosite pentru a analiza și valida o gamă largă de documente, cum ar fi cererile de credite, extrasele de cont sau alte documente financiare. Cu toate acestea, deepfake-urile reprezintă o amenințare gravă pentru aceste sisteme, deoarece pot crea documente false extrem de realiste, care pot păcăli sistemele automate de analiză a documentelor. De pildă, se poate lua în calcul utilizarea unui deepfake video pentru a crea un act de identitate fals, care să fie folosit pentru a obține un credit bancar în mod fraudulos. În acest scenariu, un atacator ar putea folosi tehnologia deepfake pentru a crea o înregistrare video care să arate o persoană falsă prezentând un act de identitate fals în fața camerei, inducând în eroare sistemul bancar automat și obținând astfel acces la un credit pentru care nu este îndreptățit. Această tactică poate fi extrem de periculoasă, deoarece documentele false create cu ajutorul deepfake-urilor pot fi extrem de realiste și dificil de detectat cu ochiul liber, iar sistemele automate de procesare a documentelor pot fi induse în eroare să creadă că documentele sunt autentice și să accepte tranzacții sau cereri care ar trebui să fie respinse în mod normal.

Lipsa de conștientizare: Lipsa de conștientizare în ceea ce privește riscurile asociate deepfake-urilor poate reprezenta o vulnerabilitate majoră atât pentru clienți, cât și pentru personalul bancar. Deepfake-urile sunt tot mai sofisticate și pot fi utilizate pentru a manipula și a induce în eroare atât persoanele obișnuite, consumatorii serviciilor bancare, cât și profesioniștii din domeniul bancar. Un efect concret al impactului lipsei de conștientizare este posibilitatea ca un client să fie convins să divulge informații sensibile, cum ar fi datele de autentificare sau detalii financiare, prin intermediul unui deepfake video care imită un oficial bancar. Atacatorii pot crea deepfake-uri credibile, care să pară că provin de la instituția bancară sau de la un angajat bancar respectabil, și să folosească aceste înregistrări pentru a manipula și a obține informații sensibile de la clienți neștiutori. În plus, chiar și personalul bancar poate fi vulnerabil la atacurile deepfake din cauza lipsei de conștientizare a modului în care aceste tehnologii pot fi folosite în scopuri frauduloase. Angajații care nu sunt familiarizați cu riscurile asociate deepfake-urilor pot fi mai predispuși să cadă în capcana acestor mijloace frauduloase și să furnizeze involuntar informații confidențiale sau să execute tranzacții neautorizate.

2.3 Cazuri concrete de fraude bancare cu deepfake

2.3.1 Frauda de 25 de milioane de dolari din Hong Kong[32]

Un exemplu relevant din practică îl constituie frauda de 25 de milioane de dolari cu deepfake care a avut loc în Hong Kong, la începutul acestui an. În acest

[32] A se vedea *Articolul „Finance worker pays out $25 million after video call with deepfake 'chief financial officer'"* https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html, data ultimei accesări: 16.03.2024

caz, un angajat din departamentul financiar al companiei a fost ținta infractorilor, care i-au trimis inițial un e-mail solicitând o tranzacție secretă de o sumă considerabilă, alertându-l asupra posibilității de phishing. Cu toate acestea, planul infractorilor a continuat, angajatul fiind ulterior convocat într-o ședință virtuală de către Directorul Financiar al companiei și alte persoane din conducere, pentru a confirma decizia de a efectua plata respectivă. Astfel, folosind tehnologia deepfake, imaginile cu membrii de top ai conducerii companiei, disponibile în spațiul public, au fost manipulate pentru a finaliza această înșelăciune extrem de sofisticată. Această scenă falsă a reușit să înșele chiar și un angajat cu o pregătire profesională solidă.

2.3.2 Tentativă de fraudă financiară care a folosit imaginea Guvernatorului Băncii Naționale a României (BNR)

Un al doilea exemplu care denotă amploarea fenomenului deepfake este acela privitor la „schemele de îmbogățire”[33] prin care cetățenii români sunt îndemnați să investească sume modice, care în decursul a câtorva zile se pot dubla. Astfel, în contextul unei intensificări a discuțiilor în spațiul public despre listarea Hidroelectrica la bursă și mediatizarea subiectului pieței de capital, indivizii necinstiți au profitat de această oportunitate, dar și de gradul scăzut de educație financiară la nivel național, aceste scheme atrăgând în principal persoanele vulnerabile, fie din cauza vârstei sau al statutului social. Prin utilizarea numelui și imaginii unei figuri publice importante din domeniul financiar-bancar sau cel guvernamental al României, aceste înșelăciuni au dobândit o eficiență și mai mare, profitând de această legitimitate falsă pe care imaginea respectivei persoane o conferea respectivei platforme. Doar în ultima perioadă, pe mai multe platforme și rețele de socializare, au apărut postări tip deepfake care îl implică pe guvernatorul Băncii Naționale a României, Mugur Isărescu, videoclipuri ce încurajau publicul să facă investiții financiare pe o platformă fictivă. La scurt timp a apărut și reacția oficială a BNR[34] care a atras atenția asupra acestei forme de înșelăciune actualizată, bazată pe tehnologia deepfake, și a îndemnat ca persoanele vizate de asemenea anunțuri să rămână vigilente.

2.4 Impactul deepfake-ului asupra sectorului bancar

În cursul anului 2022, Centrul Alternativ de Soluționare a Litigiilor Bancare a înregistrat un total de 46 de cereri fundamentate pe fraude de cont, iar numărul acestora a crescut semnificativ în luna decembrie, acest fenomen fiind influențat de

[33] A se vedea *Articolul „Recomandările Băncii Transilvania pentru a evita tentativele de fraudă online”* https://www.bancatransilvania.ro/news/comunicate-de-presa/recomandarile-bancii-transilvania-pentru-evita-tentativele-de-frauda-online, data ultimei accesări: 16.03.2024

[34] A se vedea *Comunicatul de Presă BNR din 05.03.2024* https://www.bnr.ro/page.aspx?prid=23800, data ultimei accesări: 16.03.2024

creşterea tranzacţiilor online. Din cele 46 de solicitări, doar 14 cazuri au fost acceptate de către bănci pentru negociere, în timp ce celelalte au fost respinse. Motivele respingerii includ invocarea de către bănci a faptului că acestea sunt terţe în obligaţia de restituire şi argumentele conform cărora plăţile au fost efectuate de către consumatori care au dezvăluit informaţiile personale şi au introdus singuri datele de securitate[35].

2.4.1 Pierderi financiare

Utilizarea tehnologiei deepfake în scopuri maliţioase care vizează sectorul bancare poate duce la pierderi financiare semnificative, precum şi la riscuri reputaţionale substanţiale pentru indivizi şi organizaţii. În acelaşi timp şi punerea la dispoziţie a cât mai multe servicii digitale, de la distanţă, sporeşte posibilitatea ca asemenea fraude să aibă loc. Acest tip de conţinut falsificat poate determina persoanele vizate să ia decizii financiare eronate, încredinţându-se unor informaţii manipulate şi manipulatoare, până şi cele mai pregătite persoane putând fi luate prin surprindere de ingeniozitatea acestor forme de fraudă şi să cadă în capcana lor. Pe lângă pierderile financiare, care pot fi considerabile în cazul unor tranzacţii frauduloase sau a deciziilor eronate luate pe baza informaţiilor false, există şi riscul de sancţiuni legale. De exemplu, ANSPDCP[36] (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal), poate impune sancţiuni drastice pentru încălcarea legislaţiei privind protecţia datelor în cazul în care măsurile tehnice şi organizatorice a operatorului respectiv nu previn posibilitatea unor asemenea incidente de securitate, fiind implicare şi date cu caracter personal care sunt utilizate fără consimţământ în vederea contractării unor produse bancare, de regulă credite.

2.4.2 Riscuri reputaţionale

În plus, în cazul organizaţiilor, consecinţele pot fi extrem de grave, deoarece astfel de incidente pot eroda încrederea investitorilor, clienţilor şi partenerilor de afaceri. De exemplu, în cazul unei instituţii financiar-bancare, o astfel de situaţie care implică tehnologia deepfake ar putea avea un impact negativ asupra cotaţiei sale pe piaţa financiară, determinând investitorii să-şi reevalueze încrederea în instituţie şi să-şi reanalizeze angajamentele financiare. O scădere bruscă a încrederii

[35] A se vedea *Articolul Centrului de soluţionare alternativă a litigiilor în domeniul bancar (CSALB) „Attempts to defraud bank accounts have increased!"* https://csalb.ro/en/press-releases/attempts-to-defraud-bank-accounts-have-increased/, data ultimei accesări: 16.03.2024

[36] A se vedea Legea nr. 363 din 28 decembrie 2018 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date

investitorilor ar putea conduce la o diminuare a valorii acțiunilor băncii pe piața de capital, ceea ce ar putea avea un efect cascador asupra stabilității financiare a instituției.

De asemenea, clienții băncilor ar putea fi afectați în mod semnificativ fie în mod direct (ei să fi fost victimele unor astfel de atacuri sau înșelăciuni) sau indirect (Banca în sine a avut mai multe probleme interne, serviciile ei digitale și cele operaționale au fost păcălite prin utilizarea de deepfake-uri) în cazul unui incident care a avut la bază tehnologia deepfake. Astfel, atunci când apar astfel de situații, clienții ar putea să-și piardă încrederea în siguranța și confidențialitatea informațiilor lor financiare, determinându-i să-și reevalueze relația cu instituția bancară. În consecință, clienții ar putea decide să-și transfere activele către alte instituții financiare în care au mai multă încredere. fie ele bancare sau non-bancare. Această pierdere de clienți ar putea avea un impact semnificativ asupra veniturilor și profitabilității băncii afectate, pe lângă pierderea încrederii publicului și a reputației instituției pe piața financiară.

2.5 Metode de prevenție. Conceptele „Uncanny Valley" și „Efectul Streisand". Importanța factorului uman

2.5.1 Uncanny Valley în contextul fenomenului deepfake

Deepfake-urile reprezintă o provocare din ce în ce mai mare pentru om, calitatea și perfecționarea continuă a acestui conținut împiedicând de multe ori, la o primă vedere, identificarea falsului respectiv. În acest sens, factorului vizual care nu alertează ceva în neregulă cu respectiva înfățișare a persoanei vizate, îi vine în ajutor factorul psihologic și mental, conceptul psihologic cunoscut ca și „Uncanny Valley"[37] acționând ca o linie de apărare naturală. Teoria postulează că la un nivel de asemănare ridicat între entități artificiale și umane, spectatorii resimt un anumit disconfort. În contextul deepfake-urilor, acest lucru se manifestă prin subtilități care trădează natura artificială: mimică facială nenaturală, mișcări corporale rigide sau imperfecțiuni vizuale. Aceste semnale pot avertiza publicul atent asupra conținutului neverosimil, oferind astfel o oportunitate de a combate dezinformarea. Totuși, pe măsură ce tehnologia deepfake avansează, rolul „Uncanny Valley" ca factor de prevenție poate scădea, depinzând de multe ori și de factorul cultural sau social al persoanei țînte. Mici imperfecțiuni în mimică, expresia ochilor sau mișcarea corpului pot trăda natura artificială a unei imagini sau a unui videoclip. Astfel, pentru a răspunde întrebării adresate în capitolul introductiv, suntem de părere că nivelul social și cultural pe care îl are o persoană joacă un rol esențial în caracterul infracțional aferent fenomenului deepfake, victimele fiind în general persoane care au cunoștințe minime spre zero în domeniul tehnic și care nu sunt la curent cu

[37] S. Wang, P. Rochat, *Human Perception of Animacy in Light of the Uncanny Valley Phenomenon*, 2017, Perception, 46(12), disponibil online: https://journals.sagepub.com/doi/10.1177/0301006617722742?icid=int.sj-full-text.similar-articles.1, data ultimei accesări: 16.03.2024

impactul pe care îl au noile tehnologii asupra operațiunilor financiar-bancare. Persoanele cu un nivel cultural și social mai ridicat sunt adesea mai conștiente de riscurile și amenințările legate de securitatea informației și au tendința să fie mai bine informate despre tactici și tehnici de fraudă online și să fie mai dispuși să adopte măsuri de protecție împotriva acestora. Cu toate acestea, este important a sublinia că niciun nivel cultural sau social nu oferă o protecție completă împotriva criminalității informatice. Indiferent de gradul de educație sau de statut social, toți utilizatorii online sunt expuși la riscuri de securitate și ar trebui să adopte măsuri de precauție adecvate pentru a se proteja împotriva acestora.

2.5.2 Efectul Streisand în contextul fenomenului deepfake

Efectul Streisand[38], numit după incidentul în care Barbra Streisand a încercat să ascundă o fotografie a casei sale, evidențiază paradoxul în care încercarea de cenzură sau ascundere a unei informații atrage, de fapt, mai multă atenție și vizibilitate asupra ei. În contextul deepfake-urilor, acest efect poate avea consecințe semnificative. Cenzurarea sau eliminarea deepfake-urilor poate provoca un interes sporit din partea publicului și poate contribui la proliferarea lor pe scară mai largă. Acest lucru poate alimenta scepticismul și dezinformarea, erodând încrederea în informații și autorități.

În domeniul de interes pentru această lucrare, atunci când instituțiile financiar-bancare încearcă să suprime sau să cenzureze deepfake-uri care le implică, aceste acțiuni ar putea avea un efect contrar și ar putea atrage chiar mai multă atenție asupra lor. De exemplu, dacă o bancă încearcă să suprime un deepfake care pretinde că unul dintre oficialii săi este implicat într-un comportament fraudulos sau compromițător, această acțiune ar putea duce la o creștere a interesului public și media pentru subiect. Mai mult, utilizatorii de pe internet ar putea fi motivați să distribuie și să disemineze deepfake-ul într-o măsură mai mare, ceea ce ar putea submina încrederea publică în instituția financiară în cauză. De asemenea, Efectul Streisand poate contribui la creșterea conștientizării cu privire la amenințările aduse de deepfake-uri în domeniul financiar-bancar. Atunci când instituțiile financiare sunt implicate în incidente legate de deepfake-uri, acest lucru poate determina alte instituții și consumatori să fie mai vigilenți și mai precauți în ceea ce privește autenticitatea informațiilor și comunicărilor online.

Prin urmare, în contextul fenomenului deepfake, instituțiile financiare ar trebui să fie proactive în gestionarea și răspunsul la deepfake-uri, adoptând strategii care să abordeze nu numai conținutul fals, ci și impactul pe care îl pot avea acțiunile lor în propagarea și distribuirea acestui conținut. De asemenea, consolidarea măsurilor de securitate cibernetică și educația clienților și angajaților cu privire la riscurile deepfake-urilor ar putea fi apte să contribuie la protejarea reputației și integrității instituțiilor bancare în fața acestor amenințări.

[38] A se vedea *Cazul SC077257 Streisand v. Adelman et. al.*

2.5.3 Importanța factorului uman

În materia prevenirii și gestionării deepfake-urilor, este crucial a fi recunoscut rolul pe care factorul uman îl are, alături de metodele tehnice de detectare care au început a fi implementate. Educația publicului joacă un rol fundamental în sensibilizarea și pregătirea indivizilor pentru a identifica și a contracara impactul negativ al acestor conținuturi manipulate. În acest sens, se pot contura câteva strategii de educație publică, după cum urmează în rândurile de mai jos.

În primul rând, campaniile de informare reprezintă o modalitate eficientă de a evidenția riscurile și pericolele asociate deepfake-urilor. Aceste campanii ar trebui să ofere publicului informații relevante și actualizate despre modul în care deepfake-urile pot influența opinia maselor și pot distorsiona realitatea. De asemenea, dezvoltarea de materiale educaționale interactive poate facilita învățarea și înțelegerea conceptelor legate de deepfake-uri. Astfel de materiale ar trebui să permită publicului să înțeleagă și să identifice caracteristicile specifice ale conținutului manipulat, precum și să își consolideze abilitățile de discernământ între informațiile reale și cele falsificate. Promovarea unor resurse online de încredere reprezintă, de asemenea, o componentă importantă a strategiei de educație publică. Aceste resurse ar trebui să ofere instrumente și metode prin care utilizatorii să poată verifica informațiile suspecte și să își confirme autenticitatea sau să identifice posibile manipulări.

Totodată, deși cazuistica din ultima vreme a demonstrat tiparul victimizării unor astfel de înșelăciuni, în momentul în care discutăm despre sectorul financiar-bancar, tendința este să credem că profesionalismul și pregătirea angajaților reprezintă un element esențial în prevenirea și gestionarea riscurilor asociate tehnologiei deepfake. În acest domeniu, unde se lucrează cu sume mari de bani și informații sensibile, este de datoria organizației să prevadă o instruire temeinică a angajaților săi. Relevantă în acest sens este Hotărârea civilă definitivă nr. 9 din 13.04.2022[39], a Curții de Apel Cluj prin care s-a confirmat aplicarea amenzii în cuantum de 100.000 de euro de către Autoritatea de Supraveghere, Băncii Transilvania, în urma unui incident de securitate comis de către angajații acesteia. Deși această amendă a fost aplicată în materia protecției datelor, modul prin care instanța a argumentat menținerea acesteia este de interes mai ales în contextul actual, dându-se naștere conceptului de „instruire efectivă”[40] a angajaților. Astfel, în ciuda eforturilor Băncii de a organiza cursuri și de a stabili reglementări interne privind protecția datelor personale, aceasta nu a putut dovedi că angajații săi au participat efectiv la aceste cursuri sau că au fost implementate mecanisme de verificare a înțelegerii și respectării regulilor. Faptele constatate de către Autoritate, inclusiv divulgarea neautorizată a datelor cu caracter personal prin intermediul aplicației

[39] A se vedea *Comunicatul de Presă al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal din data de 14.04.2022*_https://www.dataprotection.ro/?page=Comunicat_Presa_14_04_2022&lang=ro, data ultimei accesări: 16.03.2024

[40] A se vedea *Hotărârea civilă definitivă nr. 9 din 13.04.2022*.

WhatsApp, în opinia Instanței au sugerat o lipsă de instruire efectivă a personalului și incapacitatea acestora de a identifica și gestiona corespunzător datele sensibile.

Combaterea eficientă a deepfake-urilor necesită o abordare holistică, care să includă o combinație de metode tehnice de detectare, reglementare legală, educație publică și colaborare între diversele părți interesate. Factorul uman este esențial în această luptă, iar prin cultivarea unei gândiri critice și a unei atitudini responsabile în mediul online, fiecare persoană, fie că a fost victimă a unei asemenea înșelăciuni sau a luat la cunoștință de aceasta, poate contribui la limitarea impactului negativ al deepfake-urilor asupra societății.

O pregătire adecvată a angajaților poate ajuta la recunoașterea semnelor de avertizare ale unei tentative de fraudă și la adoptarea măsurilor preventive pentru a proteja activele și informațiile instituției. În plus, promovarea unei culturi organizaționale orientate către securitatea cibernetică și educația continuă a personalului în ceea ce privește noile amenințări tehnologice sunt elemente cheie în asigurarea unei protecții adecvate împotriva riscurilor deepfake în sectorul financiar-bancar. Prin integrarea acestor aspecte în strategiile de securitate cibernetică, organizațiile pot reduce vulnerabilitatea la atacuri de acest tip și pot contribui la combaterea fenomenului deepfake în ansamblu.

3. Propuneri de lege ferenda

3.1 Modificări necesare a fi aduse Proiectului de Lege 471/2023

Conform Proiectului de Lege 471/2023 adoptat de către Senatul României la data de 26.06.2023 a stârnit în spațiul public o mare polemică din cauza formei inițiale a sale, dar și din pricina celei adoptate și trimise la raport la Comisiile de specialitate.

Astfel, considerăm faptul că Legiuitorul ar trebui să abordeze cu atenție echilibrul delicat dintre protecția libertății de exprimare și gestionarea riscurilor asociate utilizării deepfake-urilor în diverse contexte. Prezentul text nu prevede anumite excepții în vederea protejării formelor de expresie artistică și culturală, precum utilizarea unor asemenea creații în scop de pamflet, artistic, comercial sau cinematografic. Această omisiune contravine legislației europene în curs de adoptare și pune în pericol libertatea artistică și satira. Prin sintagma „orice conținut falsificat", de la bun început se generalizează caracterul infracțional al unei asemenea creații, restul articolului indicând anumite condiții, precum lipsa consimțământului persoanei vizate, realizarea unor acțiuni sau spunerea unor anumitor discursuri pe care persoana respectivă nu le-a realizat în realitate. Problematică este și simultaneitatea acestor condiții, spre exemplu în cazul unui pamflet este normal că persoana care va fi reprezentantă în acel conținut nu-și va da acordul sau vor fi spuse/făcute lucruri asupra cărora nu și-a dat acordul, dar prin articolul următor se derogă derogă de la această „incriminare" dacă vă fi redat un avertisment sonor sau vizual pe cel puțin 10% din suprafața expunerii pe toată durata difuzării respectivului conținut. Astfel, deși ar putea părea că textul prezintă o

excepție prin permiterea folosirii legale a deepfake-urilor, acestea prin propria lor „substanță" vor fi considerate că au „scopul inducerii în eroare a opiniei publice cu privire la autenticitatea mesajului transmis". Chiar și așa, dacă respectivul material ar cuprinde aceste avertismente, creatorul, dacă este rău intenționat, poate să ascundă/să limiteze vizibilitatea asupra respectivului marcaj, dar să susțină că a respectat legea. Astfel, legiuitorul român nu a luat în considerare metodele de avertizare luate de anumite platforme de social media, care vizează atât informarea mult mai rapidă, dar neintruzivă a utilizatorului, în timp ce creatorul nu se mai simte limitat de aceste prevederi.

Un alt punct important îl reprezintă adaptarea sancțiunilor penale la efectul negativ pe care îl pot avea asemenea materiale malițioase asupra societății, luând în considerare amenințările la adresa integrității informaționale și a securității publice. Dat fiind faptul că în sine, adaptat la nivelul tehnologic actual, deepfake-ul nu constituite în mod direct o infracțiune, ci un facilitator al unor infracțiuni deja reglementate de Codul Penal, legiuitorul nu ar trebui să prevadă noi sancțiuni, ci din contră, în cadrul altor infracțiuni să prevadă un alt mod realizarea acestuia (spre exemplu în cazul infracțiunii de hărțuire).

Nu în ultimul rând, conform art. 4 alin. (4) al Proiectului de Lege, "Contravențiile prevăzute de prezenta lege se constată la sesizarea persoanelor *prejudiciate* ori din oficiu, de către reprezentanții împuterniciți ai Consiliului Național al Audiovizualului". Suntem de părere că orice persoană care intră în contact cu orice formă a deepfake-ului, indiferent dacă a fost prejudiciată sau, având idee de acest fenomen, a trecut peste nevătămată, ar trebui să aibă dreptul să sesizeze problema prin denunț. Așadar, textul de lege ar trebui să fie reformulat în "Contravențiile prevăzute de prezenta lege se constată la sesizarea persoanelor *vizate/targetate de forma deepfake-ului* ori din oficiu, de către reprezentanții împuterniciți ai Consiliului Național al Audiovizualului".

Astfel, textul de lege ar trebui să ofere o definiție clară și cuprinzătoare a deepfake-urilor și să abordeze subtilitățile manipulării conținutului, pentru a preveni exploatarea lacunelor legislative de către creatorii rău intenționați. În același timp, este important să se permită utilizarea deepfake-urilor în scopuri culturale, educative și de divertisment, în conformitate cu valorile democratice și cu drepturile fundamentale ale fiecărui individ, în contextul acestei era a digitalizării. În același timp, recomandă, ca legislativul român să aștepte adoptarea regulamentului european privind inteligența artificială, care va include prevederi specifice referitoare la deepfake-uri. Transpunerea legislației europene ar putea oferi un cadru mai echilibrat și mai eficient de combatere a deepfake-urilor.

3.2 Modificări necesare a fi aduse legislației privind publicitatea online și adaptarea companiilor din domeniu la aceste reglementări

În contextul propunerilor de reglementare la nivel european privind drepturile online, s-a remarcat o tendință crescândă în ceea ce privește reglementarea activităților online. Este evident faptul că publicitatea pe internet joacă un rol crucial

în influențarea preferințelor consumatorilor, iar lipsa unor reglementări specifice în acest domeniu generează confuzie pentru comercianți. În absența unor legi dedicate, publicitatea online se supune regulilor generale de publicitate și legislației conexe care vizează comerțul electronic, comunicațiile electronice și protecția consumatorilor.

Ca principiu fundamental regăsit în legislația deja implementată[41], reglementările privind publicitatea online ar trebui să promoveze decența, corectitudinea și responsabilitatea socială, interzicând în mod explicit publicitatea înșelătoare sau subliminală. Pe lângă aceste principii sunt prevăzute și anumite categorii de produse sau servicii (spre exemplu tutunul, alcoolul, armele, substanțele etnobotanice, medicamentele) care necesită restricții suplimentare.

Din punctul nostru de vedere, legislația ar trebui să includă, de asemenea, dispoziții care să vizeze deepfake-urile, având în vedere potențialul lor de a induce în eroare și de a afecta percepția publicului. Astfel, este esențial ca orice afirmație publicitară care nu poate fi susținută de dovezi să fie considerată în mod automat ca fiind înșelătoare, indiferent de tehnologia utilizată pentru realizarea ei, inclusiv deepfake-urile. Persoanele sau entitățile responsabile pentru publicitatea înșelătoare ar trebui să fie supuse unor sancțiuni adecvate, cu amenzi proporționale la gravitatea încălcării, în conformitate cu principiile de protecție a consumatorului și de combatere a practicilor comerciale incorecte. În același timp, nici raportările pe care utilizatorii le fac nu au rezultatul scontat, companiile invocând faptul că nu se încalcă termenii și condițiile acestora, deși există mai multe indicii care relevă caracterul fals al acestor anunțuri. Astfel, în contextul activității comerciale online, utilizarea deepfake-urilor în publicitate ar trebui să fie reglementată strict, pentru a asigura transparența și integritatea în comunicarea comercială și pentru a proteja consumatorii de manipulare și înșelăciune.

De asemenea, în conformitate cu noile prevederi ale Legii Audiovizualului[42], Consiliul Național al Audiovizualului (CNA) și-a extins atribuțiile pentru a include și reglementarea conținutului disponibil pe platformele de partajare a materialelor video. Cu toate acestea, rolul său rămâne unul de îndrumare în ceea ce privește conținutul furnizat prin aceste servicii digitale. Prin intermediul coreglementării și autoreglementării, se urmărește ca fiecare organizație din acest domeniu să implementeze termeni și condiții care să țină cont de drepturile utilizatorilor și de legislația națională sau europeană. Ele trebuie să prevină difuzarea sau acceptarea conținutului pornografic, violent sau incitant la ură împotriva anumitor grupuri. În acest context și având în vedere necesitatea asigurării conformității cu aceste principii, considerăm că CNA-ul ar trebui să obțină competențele prevăzute în Propunerea de Lege 471/2023, nu doar la solicitarea persoanelor ale căror imagini au fost utilizate în mod abuziv sau în mod oficios, ci

[41] A se vedea Legea nr. 148/2000 privind publicitatea, Legea nr. 158/2008 privind publicitatea înșelătoare și publicitatea comparativă.

[42] A se vedea Legea nr. 217/ 2023 pentru modificarea și completarea Legii nr. 286/2009 privind Codul penal, a Legii nr. 135/2010 privind Codul de procedură penală, precum și a Legii audiovizualului nr. 504/2002.

și la raportarea oricărei persoane interesate, care a fost afectată de astfel de reclame frauduloase.

Concluzii

În încheiere, proliferarea deepfake-urilor în domeniul financiar-bancar ridică provocări fără precedent pentru detectarea fraudei și menținerea integrității sistemului financiar, incidența acestui fenomen necesitând o abordare multifațetată. Din punct de vedere legislativ, este esențială elaborarea unor reglementări specifice care să definească acțiunile frauduloase bazate pe deepfake ca infracțiuni distincte, cu sancțiuni proporționale gravității daunelor potențiale.

Reiterând ideile din corpul lucrării, considerăm că răspunsul la prima întrebare din secțiunea introductivă: "*Ce impact are factorul cultural/social al cetățeanului în momentul în care este susceptibil unei conduite infracționale în domeniul bancar?"* este acela că, într-adevăr, abilitățile și discernământul uman reprezintă un elemente cruciale în materia prevenției realizării unor asemenea acte malițioase cu ajutorul tehnologiei deepfake. În ciuda dezvoltării continue a unor sisteme care să mitigheze efectele negative ale unor asemenea acte, capacitatea individului de a recunoaște semnele unei înșelăciuni, de a lua decizi informate și de a acționa în mod responsabil în mediul online contribuite la limitarea ratei de succes a acestor conținuturi manipulatoare. Deși inițial s-ar putea presupune că persoanele vulnerabile, cum ar fi cele în vârstă sau cu un nivel scăzut de pregătire, sunt cele mai susceptibile de a deveni victime ale acestor înșelătorii, practica demonstrează contrariul. Grupurile infracționale vizează o gamă largă de indivizi, inclusiv pe cei din medii mai înstărite sau din sectorul corporativ, adaptându-și constant metodele pentru a viza și asemenea ținte, iar pagubele cauzate fiind din ce în ce mai mari, multe dintre acestea fiind comise chiar de către persoana vizată, ceea ce nu permite sistemelor bancare să detecteze la timp anumite anomalii sau doar în urma sesizării victimei să se constate actul ilicit respectiv. Prin urmare, rămâne de datoria atât a organelor guvernamentale și a sectorului bancar, ca pe lângă măsurile reactive împotriva acestor acte, să promoveze campanii de educație publică privind riscurile deepfake-urilor și să susțină responsabilizarea consumatorilor financiari pentru a adopta un comportament prudent în vederea limitării impactul negativ al acestei tehnologii emergente.

Întrebarea *"Cum au evoluat infracțiunile clasice asupra patrimoniului sub impactul digitalizării?"* poate fi soluționată prin afirmația că deepfake-ul poate fi considerat o formă actualizată a înșelăciunii clasice, cu valențe subtile provenite de la infracțiunile de fals și cele comise folosind un sistem informatic. Așa cum am putut observa de-a lungul lucrării, reglementarea clară și precisă a acestei tehnologii lipsește cu desăvârșire din legislația națională în prezent. De asemenea, cu privire la *incertitudinea mijloacelor de prevenție actuale și modalităților de îmbunătățire a acestora*, deepfake-ul reprezintă un risc semnificativ pentru sectorul financiar-bancar, necesitând o abordare proactivă și o colaborare intersectorială, atât din punct de vedere economic, cât și juridic, pentru a combate eficient infracțiunile facilitate

de această tehnologie emergentă. Instruirea și educarea factorului uman prin oferirea de către instituțiile bancare a unor programe de formare și conștientizare pentru a-i ajuta pe angajați și clienți să recunoască și să raporteze potențialele cazuri de deepfake, implementarea unor metode de autentificare mai avansate și mai sigure, cum ar fi autentificarea multifactorială și utilizarea biometriei și, nu în ultimul rând, implementarea unor politici și proceduri clare în conformitate cu standardele internaționale de securitate cibernetică pot contribui la reducerea riscului de expunere la deepfake a persoanelor vizate.

Colaborarea strânsă între instituțiile financiare, autoritățile competente și alte entități din sectorul financiar-bancar poate juca un rol crucial în combaterea activităților infracționale și în protejarea integrității sistemului bancar. Această colaborare poate include schimbul de informații despre amenințările cibernetice, practicile frauduloase și alte activități ilicite, facilitând astfel identificarea și contracararea acestora într-un mod mai eficient și coordonat. Prin stimularea schimbului de informații și colaborarea între instituții, autorități și alte părți interesate, se poate promova descoperirea de metode proactive de prevenire și mitigare a riscurilor asociate infracțiunilor financiare și cybercrime-urilor. Aceasta poate include implementarea de tehnologii avansate de securitate cibernetică, dezvoltarea de politici și proceduri robuste de protecție a datelor și educația clienților și a angajaților cu privire la riscurile și amenințările existente în mediul financiar digital.

În lumina cercetării noastre asupra incidenței caracterului infracțional al fenomenului deepfake în domeniul financiar-bancar, este clar că acesta reprezintă o amenințare serioasă și în creștere pentru securitatea și integritatea instituțiilor bancare. Această tehnologie oferă infractorilor o nouă modalitate de a comite fraude sofisticate, cu potențialul de a genera pierderi semnificative pentru instituțiile financiare și clienții lor. În multe privințe, deepfake-ul poate fi considerat o formă modernă a "jafului perfect", datorită capacității sale de a manipula realitatea și de a induce în eroare sistemele de securitate și autentificare. Pentru a contracara această amenințare, este crucial ca instituțiile bancare să adopte o abordare proactivă, bazată pe colaborare intersectorială și implementarea unor măsuri avansate de securitate cibernetică. De asemenea, reglementările și standardele legale ar trebui actualizate și adaptate pentru a ține pasul cu evoluția tehnologică și pentru a asigura o protecție adecvată împotriva riscurilor asociate deepfake-ului în sectorul financiar-bancar. Prin implementarea acestor măsuri și abordări, putem spera să reducem impactul și frecvența infracțiunilor facilitate de deepfake și să asigurăm o mai mare securitate și încredere în sistemul nostru financiar și în instituțiile bancare.

Bibliografie

Legislație în vigoare

Noul Cod Penal, Titlul VI - Infracțiuni de fals, Capitolul III - Falsuri în înscrisuri, art. 325

Noul Cod Penal, Titlul II - Infracțiuni contra patrimoniului, Capitolul III - Infracțiuni contra patrimoniului prin nesocotirea încrederii, art. 244

Regulamentul (UE) 2016/679 (General Data Protection Regulation) privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE

Regulamentul (UE) 2022/2065 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE

Propunerea de Regulament (UE) de Stabilire a unor Norme Armonizate privind Inteligența Artificială și de Modificare a anumitor Acte Legislative ale Uniunii

Regulamentul (UE) 2022/2065 (Digital Services Act)

Propunere Legislativă 471/2023 privind utilizarea responsabilă a tehnologiei în contextul fenomenului deepfake

Legea nr. 363 din 28 decembrie 2018 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date

A se vedea Legea nr. 217/ 2023 pentru modificarea și completarea Legii nr. 286/2009 privind Codul penal, a Legii nr. 135/2010 privind Codul de procedură penală, precum și a Legii audiovizualului nr. 504/2002.

Cărți și lucrări științifice

G. Zlati, Tratat de criminalitate informatică. Vol. I, Editura Solomon, București, 2020, p. 430

M. Udroiu, *Sinteze de Drept Penal. Partea Specială*, Vol. I, editura C.H. Beck, 2023, pp. 609-610

T. Manea, C. N. Constantinescu-Mărunțel, H. Ș. Tiugan, *Drept penal. Partea specială. Infracțiuni contra persoanei. Infracțiuni contra patrimoniului*, editura Hamangiu, București, 2022, p. 484

E. Fahey, *The EU as a Global Digital Actor. Institutionalising Global Data Protection, Trade, and Cybersecurity*, Editura Bloomsbury Publishing, Colecția Hart Publishing, Londra, 2024

Dr. M. G. Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis*, Editura Bloomsbury Publishing, Colecția Hart Publishing, Londra, 2023

G. Zlati, *Criminalitatea informatică în România*, Jurnalul Baroului Cluj, nr. 1, 2021, p. 28

S. Wang, P. Rochat, *Human Perception of Animacy in Light of the Uncanny Valley Phenomenon*, 2017, Perception, 46(12), disponibil online: https://journals.sagepub.com/doi/10.1177/0301006617722742?icid=int.sj-full-text.similar-ar ticles.1, data ultimei accesări: 16.03.2024

Cauze

Cazul SC077257 Streisand v. Adelman et. al.
Hotărârea civilă definitivă nr. 9 din 13.04.2022

Variae

Aprobarea și publicarea prospectului în legătură cu IPO-ul Hidroelectrica, disponibil online: https://m.bvb.ro/FinancialInstruments/SelectedData/NewsItem/FP-Aprobarea-si-publicarea-prospectului-in-legatura-cu-IPO-ul-Hidroelectrica/34CFE, data ultimei accesări: 16.03.2023

AnyDesk features, disponibil online: https://anydesk.com/en/features, data ultimei accesări: 16.03.2023

National Institute of Standards and Technology Computer Security Research Center, disponibil online: https://csrc.nist.gov

Tackling deepfakes in European policy, disponibil online: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690 039_EN.pdf, data ultimei accesări: 15.03.2024

Studiul Centrului de soluționare alternativă a litigiilor în domeniul bancar (CSALB) cu privire la interacțiunea consumatorilor cu băncile https://www.linkedin.com/posts/csalb_csalb-isensesolutions-banking-activity-7173244337957318657-lqP2?utm_source=share&utm_medium=member_ios, data ultimei accesări: 15.03.2024

Articolul „Finance worker pays out $25 million after video call with deepfake 'chief financial officer'" https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html, data ultimei accesări: 16.03.2024

Articolul „Recomandările Băncii Transilvania pentru a evita tentativele de fraudă online" https://www.bancatransilvania.ro/news/comunicate-de-presa/recomandarile-bancii-transilva nia-pentru-evita-tentativele-de-frauda-online, data ultimei accesări: 16.03.2024

Comunicatul de Presă BNR din 05.03.2024 https://www.bnr.ro/page.aspx?prid=23800, data ultimei accesări: 16.03.2024

Articolul Centrului de soluționare alternativă a litigiilor în domeniul bancar (CSALB) „ATTEMPTS TO DEFRAUD BANK ACCOUNTS HAVE INCREASED!" https://csalb.ro/en/press-releases/attempts-to-defraud-bank-accounts-have-increased/, data ultimei accesări: 16.03.2024

Comunicatul de Presă al Autorității Naţionale de Supraveghere a Prelucrării Datelor cu

Caracter Personal din data de 14.04.2022 https://www.dataprotection.ro/?page=Comunicat_Presa_14_04_2022&lang=ro, data ultimei accesări: 16.03.2024