# Realizarea drepturilor personalităţii din perspectiva evoluţiei digitale. Omniprezenţa inteligenţei artificale

**Ruxandra GRĂJDAN**[1]
**Aisha MAHMOOD**[2]

*Abstract*

*Dată fiind concentrarea evidentă asupra Inteligenței Artificiale în calitate de tehnologie aptă a îmbunătăți considerabil viața omului modern, inser ția acesteia în cotidian marchează o nouă etapă a evoluției speciei umane, drept care prezentul articol își propune a analiza modul în care homo digitalis se folosește cu adevărat de Inteligența Artificială. Astfel, într -o constelație a drepturilor subiective care își dispută întâietate, drepturile personalității se identifică în egală măsură promovate și atacate, aș a încât analiza cadrului legal actual relevă carențe ale viziunii legislative.*

*În acest sens, abordând protecția internațională, regională, supranațională și etatică a drepturilor personalității, câteva limite ale garanțiilor aduse acestora se vor prezenta sub forma unei tehnologii malițioase, anume, tehnologia deepfake, ale cărei origini binevoitoare vor fi prezentate în disonanță cu utilizarea actuală a acesteia, utlizare care pune în dificultate lumea dreptului. O altă limită a realizării drepturilor personalității se va înfăți șa sub analiza unei activități infracționale, anume furtul sintetic de identitate, care, prin aparenta imperceptibilitate, se înfăți șează caustic, comparativ cu alte modalități ale furtului în general. Din cauza potențialului vast al utilizării cu rea-credință a Inteligene ței Artificale, alte potențiale limite ale realizării drepturilor personalității se vor prezenta în domeniul creației și al medicinei.*

*În cele din urmă, concluziile vor compărea într -un raport al oportunității de lege lata, pentru ca, în final, propunerile de lege ferenda să ghideze demersul legislativ într-o protecție eficientă, inovatoare, vizionară și certă a drepturilor personalității din perspectiva unor restricționări sau abordări necesare în lumea digitalizată.*

**Cuvinte-cheie:** *drepturile personalității, deepfake, furt sintetic de identitate, artă, tehnologie, medicină*

## Secţiunea I
## Secţiunea introductivă

În lumina ideii că *„Știința nu inseamnă doar a scrie ecuații. Este vorba despre reconceptualizarea lumii”*[3] se dezvăluie un adevăr evident societății în

---

[1] Student, Academia de Studii Economice din București, Facultatea de Drept, e-mail: grajdanruxandra21@stud.ase.ro

[2] Student, Academia de Studii Economice din București, Facultatea de Drept, e-mail: mahmoodaisha21@stud.ase.ro

3 Henry Mance, Carlo Rovelli: *„Science is not just about writing equations. It`s about reconceptualising the world”*, 26 septembrie 202, articol disponibil la: Carlo Rovelli: 'Science is not just about writing equations. It's about reconceptualisingthe world' | Financial Times (ft.com), data ultimei accesări: 18 martie 2023.

ultimele decenii şi care ia amploare în mod sistematic prin invenţiile tehnologice care par a se îndrepta către un potenţial cândva considerat utopic. Joncţiunea de abilităţi ale inteligenţei artificiale, anume executarea de comenzi şi depăşirea acestora prin luarea de decizii[4] dovedeşte constant că este impusă o transformare inerentă a societăţii şi a individului ce îl provoacă pe acesta din urmă la a-şi trasa un nou rol social în jurul omniprezentei tehnologii. Dreptul ca ştiinţă devine astfel responsabil pentru redefinirea modului în care se desfăşoară coeziunea dintre *homo sapiens şi homo digitalis*[5] în contextul ameninţărilor aduse drepturilor personalităţii, anume dreptul la viaţă, la sănătate, la propria imagine, la demnitate, la viaţă privată, securitate, libertate, oferind un minim acces la certitudinea existenţei protecţiei juridice a omului ş i a umanităţii într-un viitor incert, astfel încât I.A. să reprezinte un instrument complet controlabil de către om, iar nu individul un supus al tehnologiei. Pentru reprezentarea corectă a ideilor propuse în prezenta lucrare, vom purcede la definirea a ceea ce reprezintă **inteligenţa artificială (I.A.),** mai exact un set de „sisteme informatice capabile să îndeplinească sarcini care în mod normal necesită inteligenţă umană, fiind bazate pe reguli decizionale”,[6] ca extensie având şi abilitatea de a genera conţinut original.

În *scopul* realizării unei analize amănunţite a termenilor anterior definiţi, în corpul lucrării vor fi expuse insuficientele texte normative existente la nivel intern şi internaţional referitoare la domeniul digital, urmând a aborda noţiunea de **deepfake** şi implicaţiile sale, inclusiv generatoarele de imagini, video şi text cu impactul lor asupra securităţii personale şi asupra **securităţii cibernetice**, precum şi problema **drepturilor de autor** derivată din acestea. Prezentarea modului de utilizare a digitalizării în domeniul **medical** va fi realizată prin prisma analizei **răspunderii juridice** a inteligenţei artificiale. Ulterior, prezenta lucrare se va concentra pe evidenţierea lacunelor legislative în materie digitală, raportate la pericolul deja infuzat în societate, precum şi la alte posibile **riscuri**, fără a exclude însă **beneficiile** evoluţiei ştiinţifice în acest domeniu. Nu în ultimul rând, anticipând o intensificare a nevoii de reglementare legislativă a I.A., vor fi expuse o serie de propuneri ***de lege ferenda.***

4 Relevant este un experiment din 2017 în care cercetătorii au învăţat calculatorul să joace un joc video cu întreceri de bărci şi, în loc să termine cursa, acesta a învăţat să lovească alte bărci întrucât obţinea astfel un scor mai bun. La fel, prin a cere inteligenţei artificiale să vindece cancerul, aceasta poate înţelege a elimina gazdele care ar putea adăposti boala. Exemplu propus de Toby Walsh în lucrarea *2062. Lumea creată de inteligenţa artificială,* Ed. RAO, 2021, p. 62.

5 Termen propus de Toby Walsh, *op. cit*. p. 9.

6 Comitetul pentru viitorul ştiinţei şi tehnologiei (STOA), *Tackling deepfakes in European policy,* 30 iulie 2021, articol disponibil PDF la: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)690039, data ultimei accesări: 18 martie 2023, p. I.

## Secţiunea a II-a
## Efectele *in concreto* ale inteligenţei artificiale

### 1. De lege lata

Cadrul legal actual în domeniul abordat vizează reglementarea internaţională conferită de Declaraţia Universală a Drepturilor Omului care, în art. 3, fixează coordonatele importante respectate de comunitatea globală, anume viaţa, libertatea şi securitatea persoanei, şi care în contextul actual tind să îşi diversifice con ţinutul prin complexitatea abordărilor. Convenţia Europeană a Drepturilor Omului, în art. 8, abordează dreptul la respectul vieţii private alături de viaţa de familie, aşa încât numai un interes public evident ar putea determina restrângerea conţinutului acestuia. Supranaţional şi regional, la nivelul Uniunii Europene, Carta drepturilor fundamentale interesează subiectul dat din perspectiva art. 6 „Orice persoană are dreptul la libertate şi la siguranţă.”[7], art. 7 „Orice persoană are dreptul la respectarea vieţii private şi de familie, a domiciliului şi a secretului comunicaţiilor.”[8], art. 8, alin. (1)-

(2) „Orice persoană are dreptul la protecţia datelor cu caracter personal care o privesc. Asemenea date trebuie tratate în scopurile precizate şi pe baza consimţământului persoanei interesate sau în temeiul unui alt motiv prevăzut de lege.”[9] Totodată, interesează, din perspectiva creatorului unui sistem computerizat inteligent şi al evoluţiei digitale, art. 11 al Cartei, anume libertatea de exprimare şi de informare, întrucât informaţia în sine poate fi tratată drept un mesaj transmis indirect de către titularul dreptului de creaţie asupra I.A., alături de art. 13, teza întâi „Artele şi cercetarea ştiinţifică sunt libere.”[10] La nivelul Uniunii Europene se regăseşte în prezent şi cea mai puternică reglementare, aşa încât sunt relevante în ansamblu Directiva 2000/31/CE (Directiva comerţului electronic)[11], Directiva 2001/29/CE[12], îndeosebi prin derogările excepţionale pe care le face prin art. 5, alin.
(3), lit. f) şi k), aşa încât statele membre pot să prevadă excepţii şi limitări de la dreptul de reproducere al diverselor opere în domenii precum „utilizarea discursurilor politice, precum şi a extraselor din prelegeri publice sau a operelor sau a altor obiecte protejate similare, în măsura justificată de scopul informativ urmărit şi cu condiţia să fie indicată sursa, inclusiv numele autorului, cu excepţia cazurilor

7 Carta drepturilor fundamentale a Uniunii Europene, art. 6, publicată în JOUE, C 326 din 26 octombrie 2012, pp. 391-407.

8 *Idem*, art. 7.

9 *Idem*, art. 8.

10 *Idem*, art. 13.

11 Transpusă prin Legea nr. 365 din 7 iunie 2002, publicată în M. Of. nr. 959 din 29 noiembrie 2006.

12 Transpusă prin Legea nr. 8 din 14 martie 1996, publicată în M. Of. nr. 489 din 14 iunie 2018.

în care acest lucru se dovedește imposibil”[13] și „utilizarea în cazul caricaturilor, parodierii sau pastișelor”[14], Directiva 2010/13/UE (a serviciilor audio-vizuale)[15], Regulamentul (UE) 2016/679 (Regulament general privind protecția datelor al Uniunii Europene „RGPD”) și Regulamentul 2022/2065 care modifică Directiva 2000/31/CE (Regulamentul privind serviciile digitale)[16].

La nivel național, cadrul normativ se armonizează cu cel supranațional și internațional identificat, ceea ce îi determină pe alocuri abordările lacunare. Trebuie deci luată în considerare Constituția României, art. 26, respectul adus vieții intime private, art. 30, libertatea de exprimare, art. 31, dreptul la informație. Totodată, Codul Civil concentrează atenția legislativă asupra drepturilor personalității care își au realizarea în art. 72, demnitatea persoanei, art. 73, dreptul la imagine, art. 74, eventualele atingeri aduse acestor drepturi ale personalității, și art. 77, prelucrarea datelor cu caracter personal. Din cauza potențialelor atingeri aduse persoanei prin digitalizare, poate fi incidentă și legea penală, Codul Penal incriminând, în art. 226, violarea vieții private. Codul Penal și Codul de Procedură penală au transpus și Directiva 2012/13/UE privind dreptul la informare în cadrul procedurilor penale.

## 2. Problema deepfake

Deepfake, înțeles din perspectiva rezultatului manipulării audio-video sau fie audio, fie video, se referă la un conținut falsificat cu ajutorul I.A., înregistrarea sau imaginea propriu-zisă dând impresia autenticității, „prezentând oameni care par că spun sau fac ceva pe care nu l-au spus sau nu l-au făcut niciodată”[17]. Astfel, metoda utilizată pentru crearea unei aparențe și rezultatul acestei activități creatoare îmbracă astăzi, din perspectiva evoluției tehnologice [18], forma unui fenomen ce pune la îndoială realitatea și provoacă lumea dreptului, împingând legiuitorul către o reglementare atentă, aprofundată și vizionară.

Tehnologia de creare a conținutului falsificat se poate referi atât la crearea unui videoclip, prin **manipularea audio-video**, cât și la **clonarea vocii**, prin care se imită vocea umană, dar și tehnologia **sintetizatorului de text** capabil să imită stilul de exprimare al unei persoane. În acest sens, o abordare extremă a tehnologiei

13 Directiva 2001/29/CE, art. 5, alin. (3), lit. f), publicată în JOUE., L 167 din 22 iunie 2001, pp. 10-19.
14 *Idem*, lit. k).
15 Transpusă prin Legea nr. 504 din 11 iulie 2002, publicată în M. Of. nr. 534 din 22 iulie 2002.
16 Regulamentul privind serviciile digitale, Regulamentul privind piețe contestabile și echitabile în sectorul digital și Codul de bune practici privind dezinformarea consolidat alcătuiesc Pachetul privind serviciile digitale.
17 STOA, *op. cit.,* p. I.
18 Primul program care a creat deepfake este Video Rewrite, în 1997, cu scopul dublării filmelor. În 2014, Ian Goodfellow inventează Generative Adversial Networks (GAN) care a permis crearea unui conținut fals îmbunătățit. A se vedea *A Quick History of Deepfakes: How It All Began*, 16 noiembrie 2022, disponibil la: https://q5id.com/blog/a-quick-history-of-deepfakes-how-it-all-began, data utlimei accesări: 17 martie 2023.

deepfake ar determina afirmația: tehnologia utilizată este malițioasă, deci ar trebui eliminată. Totuși, au fost evidențiate **beneficiile**, preponderent în industria artistică, prin dublarea conținutului cu acuratețe, contribuind la verosimilitatea în industria divertismentului. Industria jocurilor pe calculator folosește tehnologia deepfake pentru crearea personajelor tridimensionale. Deepfake înseamnă și utilizarea filtrelor capabile să modifice vocea sau fizionomia unei persoane, iar în domeniul comercial, crearea de mesaje personalizate pentru clienți pornind de la un videoclip este capabilă prin tehnologia de manipulare grafică. În scop educativ, recrearea momentelor istorice prin scene deepfake contribuie la procesul educațional. Domeniul medical beneficiază de pe urma tehnologiilor deepfake pentru reconstrucția facială a cazurilor de intervenție chirurgicală.

Totuși, utilizarea deepfake pune în lumină **riscuri** ce pot fi grupate în trei categorii, psihologice, financiare și sociale [19]. Riscurile psihologice pot fi posibilitatea defăimării și intimidarea. Furtul de identitate face capabil, din punct de vedere financiar, crearea unor pagube substanțiale, în acest sens fiind amintit cazul fraudei din 2019[20], daunele fiind evaluate la 220.000 de euro. Social, manipularea știrilor și transmiterea unor mesaje false pot afecta încrederea societății în informarea mass-media. Chiar democrația se poate clătina din cauza falsificării alegerilor, acestea fiind chiar esența sa. Securitatea națională și securitatea și relațiile internaționale pot avea de suferit, un exemplu fiind un videoclip falsificat din anul 2018 care îl înfățișa pe președintele Gabonului slăbit din punctul de vedere al sănătății, ceea ce a determinat o criză națională și chiar o lovitură de stat[21]. Exemplele pot continua, de la videoclipul fostului Președinte al S.U.A., Barack Obama, insultându-l, în 2018, pe succesorul său, Donald Trump[22], pentru ca în același an, Donald Trump, în acel moment actualul Președinte al S.U.A., să fie subiectul unui videoclip fals în care făcea solicitări Belgiei[23].

---

*19* STOA, *op. cit*., p. 29, *Tabelul II: Prezentare generală a diferitelor tipuri de riscuri ascoiate deepfake-ului.*

*20* Jesse Damiani, *A Voice Deepfake Was Used To Scam A CEO Out of $243,000*, 3 septembrie 2019, articol disponibil la: https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/? sh=2f608f982241, data ultimei accesări: 18 martie 2023.

*21* Sarah Cahlan, *How misinformation helped spark an attempted coup in Gabon*, 13 februarie 2020, articol disponibil la: https://www.washingtonpost.com/politics/2020/02/13/how-sick-president-suspect-video-helped-sparked-an-attempted-coup-gabon/, data ultimei accesări: 18 martie 2023.

*22* Kaylee Fagan, *A viral video that appeared to show Obama calling Trump a 'deep---' shows a disturbing new trand called 'deepfakes'*, 17 aprilie 2018, articol disponibil la: https://www.businessinsider.com/obama-deepfake-video-insulting-trump-2018-4, data ultimei accesări: 18 martie 2023.

*23* Hans von der Burchard, *Belgian socialist party circulates 'deep fake' Donald Trump video*, 21 mai 2018, articol disponibil la https://www.politico.eu/article/spa-donald-trump-belgium-paris-climate-agreement-belgian-socialist-party-circulates-deep-fake-trump-video/, data ultimei accesări 18 martie 2023.

Din perspectivă juridică, reglementarea actuală, interesând sfera drepturilor personalității, este substanțială, dar neîndestulătoare. De exemplu, conform RGPD datele cu caracter personal – cu relevanță pentru dreptul la imagine – utilizate pentru crearea deepfake sunt protejate din perspectiva art. 6, alin. (1), lit. a), anume consimțământul persoanei pentru prelucrarea datelor, și lit. f), existența unui interes legitim a cărei importanță se supraordonează drepturilor fundamentale. Totuși, când o persoană faimoasă este subiectul unei ironii create prin deepfake, creatorul poate invoca dreptul la exprimare în baza creării unei parodii, aflându-se astfel într-o situație excepțională prevăzută în Directiva 2001/29/CE, art. 5, alin. (3), lit. k), transpusă în legea națională prin Legea 8/1996, art. 37, lit. b). Posibilitatea tragerii la răspundere al autorului deepfake este aproape imposibilă, întrucât creatorul se prezintă adesea anonim. Și apelul la dreptul de proprietate intelectuală pare potrivnic: există restricții în ce privește identificarea unei creații protejate de dreptul de autor. Legislația arată că dreptul la imagine nu este absolut, o limită a acestuia fiind identificată prin libertatea de exprimare a celorlalți care este și ea limitată. Directiva 2000/31/CE, în art. 12 și art. 14 arată că furnizorul nu este obligat să monitorizeze informațiile. Cu toate acestea, fără a defini termenul „ilegal", actul normativ evidențiază, în paragraful 40 al expunerii de motive faptul că „Furnizorii de servicii au datoria să acționeze, în anumite împrejurări, pentru evitarea sau stoparea activităților ilegale." Problema acestei defini ții a termenului de „ilegal" nu este rezolvată nici prin intermediul Pachetului privind serviciile digitale, deși această reglementare din urmă aduce o îmbunătățire Directivei cu privire la serviciile comerțului electronic[24]. Aparținând însă de Pachetul privind serviciile digitale, Codul de bune practici privind dezinformarea consolidat a primit unele critici întemeiate, precum lipsa transparenței în ce privește implementarea Codului de către semnatari, generalitatea sporită a termenilor utilizați și a structurii, lipsa semnatarilor importanți[25]. Totuși, un aspect îngrijorător este acela că deepfake poate fi utilizat pentru a crea probe false. În acest sens, în anul 2019, într -un proces care privea custodia minorului, mama a prezentat în instanță un material audio catalogat ulterior drept deepfake din care reieșea faptul că tatăl copilului ar fi fost agresiv cu aceasta cu scopul de a demonstra nedemnitatea acestuia de a-și exercita drepturile părintești[26]. De și o comisie de experți a putut identifica falsul, existența tehnologiei performante capabile să creeze un material fals poate induce martorilor, de exemplu,

24 Legea 357/2002 nu definește termenii de „activitate sau informație nelegală", folosiți în art. 14, alin. (1), lit. a), iar prin raportare la lit. b) optica legislativă a termenului „nelegal" părând a nu include vătămările aduse drepturilor terților.

25 Este vorba despre platformele precum Tik-Tok, WhatsApp, Messenger. A se vedea ERGA, *ERGA Report on Disinformation: Assessment of the Implementation of the Code of Practice*, 2020, disponibil la: https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf, data ultimei accesări 18 martie 2023, p. 3.

26 Patrick Ryan, *'Deepfake' audio evidence used in UK court to dicredit Dubai dad*, 8 februarie 2020, articol disponibil la: https://www.thenationalnews.com/uae/ courts/deepfake-audio-evidence-used-in-uk-court-to-discredit-dubai-dad-1.975764, data ultimei accesări: 18 martie 2023.

aparența cunoașterii unui fapt în realitate inexistent, așa încât aceștia nu se mai pot baza nici măcar pe propriile simțuri. Directiva 2012/13/UE privind dreptul la informare în cadrul procedurilor penale face posibilă încadrarea probelor rezultate din deepfake în sfera probelor materiale, a șa cum reiese din expunerea de motive, paragraful 31 „accesul la materiale cum ar fi documente și, dacă este cazul, fotografii și înregistrări audio sau video." La nivel internațional, Ghidul privind facilitarea utilizării probelor electronice adoptat de Comitetul de Miniștri al Consiliului Europei tratează problema mijloacelor de probă electronice. Totuși, până și acest document s-a dovedit limitat din perspectiva abordării lacunare, astfel încât „principiul cheie al drepturilor omului ar trebui reafirmat ca principiu fundamental al Ghidului."[27], precum și abordarea evazivă a unor mijloace de probe utilizate în justiției care „sunt îndeosebi o provocare pentru instanțe și pentru practicienii dreptului."[28]

### 3. Furtul sintetic de identitate

Amintind de extensiile deepfake, ne oprim asupra unei alte fațete a I.A. generatoare de conținut ce implică un grad de accesibilitate crescut, precum și unul de risc care este însă disimulat sub forma unei practici inofensive cu rol de divertisment. Din această perspectivă analizăm o serie numeroasă de aplicații capabile să creeze imagini realiste, imposibil sau aproape imposibil de identificat ca fiind false ș i care prezintă fizionomii umane noi, de persoane inexistente, așa-zisele *random face generators* (generatoare de fețe aleatorii). Folosindu-se de informa ții reale, aplicațiile pot oferi oricărui individ mai mult sau mai puțin bine intenționat accesul la crearea de identități digitale noi printr-o simplă căutare pe Internet. În ciuda anumitor utilități pe care unul dintre site-uri le enumeră și care justifică parțial existența unei astfel de tehnologii (ca exemplu menționăm posibilitatea de a crea *avataruri pentru jocuri, cărți sau filme*[29]), chiar descrierea oferită de site dezvăluie cu nonșalanță practicile ilegale pe care serviciile sale le poate promova, anume crearea de *poze de profil pentru conturile de social media sau diverse site-uri, poze utilizate în artă și în securitate, poze false pentru ID imposibil de distins de cele reale.*[30] Valențe ale ilegalității prezintă chiar utilizarea pozelor reale pentru a le genera pe cele false, întrucât sunt astfel lezate drepturi fundamentale ale personalității.

Consecințele accesului nelimitat la astfel de tehnologii se prezintă a fi negative printr-o formă periculoasă de fraudă ce amenință securitatea individului atât în mediul digital, cât și, cu precădere, în afara sa prin grave prejudicii aduse

---

27 Remigijus Jokubauskas și Marek Świerczyński, *Is Revision of the Council of Europe Guidelines on Electronic Evidence Already Needed?*, în „Utrecht Law Review", Vol. 16, no. 1, 26 mai 2020, pp. 13-20, articol disponibil la: https://doi.org/10.36633/ulr.525, p. 16.

28 Este vorba, printre altele, de I.A. *Idem*, p. 19.

29 Random Outputs, disponibil la: https://randomoutputs.com/random-face-generator, 20 octombrie 2022, data ultimei accesări: 19 martie 2023.

30 *Ibidem*.

siguranței, datelor personale ș i vie ții private. Astfel, **furtul sintetic de identitate** este un tip de fraudă prin care este creată o nouă identitate digitală prin imixtiunea de informații reale și false[31] (imagini sau date personale, adeseori aparținând copiilor sau persoanelor decedate) utilizate ulterior în deschiderea de conturi false pe rețele de socializare în scopuri ilegale sau la diferite instituții bancare în vederea retragerii de numerar din conturi bancare deja existente sau a obținerii de împrumuturi ce nu vor fi restituite niciodată întrucât "individul" va dispărea fără urmă[32]. Această metodă poate rămâne nedetectată ani întregi, în timp ce identitatea reală a făptuitorului poate rămâne permanent necunoscută. Pentru rezolvarea problematicii expuse menționăm că există inclusiv soluții juridice, fără a limita neapărat accesul liber al individului la un element digital ce poate fi atât util, cât și utilizat în scopuri pașnice. În primul rând, imaginile generate de I.A. ar trebui să prezinte semne distinctive (de exemplu, un text pe fundal) care să atenționeze celelalte persoane că individul din imagine nu există cu adevărat în realitate. Aceasta este și soluția propusă de Uniunea Europeană în Propunerea de Regulament al Parlamentului European și al Consiliului de Stabilire a unor norme armonizate privind inteligența artificială (legea privind inteligența artificială) și de modificare a anumitor acte legislative ale uniunii din 21 aprilie 2021 ce dispune astfel: „*În cazul în care un sistem de IA este utilizat pentru a genera sau a manipula imagini, conținuturi audio sau video care seamănă în mod semnificativ cu conținutul autentic, ar trebui să existe obligația de a divulga faptul că respectivul conținut este generat prin mijloace automatizate, sub rezerva unor excepții în scopuri legitime."*[33] În al doilea rând, învederăm asupra interzicerii postării pozelor copiilor pe rețelele de socializare, chiar și de către reprezentanții lor legali, întrucât vârsta sau discernământul nu le permite să își dea acordul în acest sens, ei fiind cei mai susceptibili de a fi victimele unor astfel de atacatori. Interesul superior al minorului trebuie să primeze, cu atât mai mult cu cât practică amintită pune într-un pericol grav chiar siguranța acestora.

---

*31* Experian, *Synthetic ID Fraud*, articol disponibil la: Protecting Yourself Against Synthetic Identity Fraud | Experian, data ultimei accesări: 18 martie 2023.

*32* Frauda sintetică de identitate este tipul de criminalitate financiară cu cea mai rapidă creștere din SUA, 61% din pierderile de fraudă pentru băncile mari provin din frauda de identitate și 20% din frauda de identitate suferită de aceste bănci mai mari este fraudă de identitate sintetică. Glenn Larson, *Synthetic Identity Fraud Is The Fastest Growing Financial Crime -- What Can Banks Do To Fight It?,* 8 octombrie 2019, disponibil la: Synthetic Identity Fraud Is The Fastest Growing Financial Crime -- What Can Banks Do To Fight It? (forbes.com), data ultimei accesări: 19 martie 2023.

*33* Propunere de Regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind Inteligența Artificială (Legea Privind Inteligența Artificială) și de modificare a anumitor acte legislative ale Uniunii, 21 aprilie 2021, COM/2021/206 final.

## 4. *Variae*: I.A. şi drepturile personalităţii în creaţie şi medicină

Abilitatea I.A. de a crea conținut constituie o controversă și prin raportarea la protecția **proprietății intelectuale**, dat fiind faptul că, în prezent, calculatoarele pot genera artă digitală, tablouri, muzică, piese de teatru și nu numai prin prelucrarea operelor originale deja existente ale artiştilor. Este dificil de cuantificat în ce măsură poate fi amintită originalitatea a ceea ce calculatorul a generat, dar cu atât mai dificilă este protecția drepturilor de autor ale artiștilor în contextul imposibilității tragerii la răspundere a I.A. Rezultă astfel o nevoie imperioasă de a stabili dacă în cazul acestor opere generate digital se poate aminti noțiunea de c*opyright,* iar dacă răspunsul este afirmativ, stabilirea cui aparține dreptul amintit din moment ce munca este creația exclusivă a unei mașinării ce nu poate fi subiect de drept și care nu poate fi deci titulară de drepturi subiective. În cazul unui răspuns negativ, rămâne încă nesoluționată dilema apărării dreptului de autor al artistului. În urma oricărei concluzii considerăm necesară aplicabilitatea în acest sens a art. 2 din Directiva 2001/29/CE oferă autorului dreptul exclusiv de a permite sau interzice utilizarea creației sale. Analizând dintr-o altă perspectivă, nu este creația digitală susceptibilă a leza chiar **valori sociale**, arta fiind o expresie a sensibilității umane, esență a culturii?

Apelând la noțiunea de omniprezență a I.A. descoperim că evoluția acesteia *a* influențat considerabil inclusiv **domeniul medical**, ceea ce, dintr-o abordare juridică, reprezintă un sprijin generos în vederea protecției drepturilor personalității, accentuându-l pe acela la viață și pe cel la sănătate. În acest sens, printre evidentele progrese pot fi amintite *scanarea creierului uman pentru detectarea pierderilor de memorie și a persoanelor predispuse la a dezvolta Alzheimer*[34], prezicerea apariției de stop cardiac, alte asemenea diagnostice și realizarea de operații complexe. Seriozitatea ariei de aplicabilitate implică însă și riscuri dintre cele mai grave, limitele I.A. manifestându-se deja în repetate cazuri ale căror consecințe se răsfrâng nemărginit asupra mai multor drepturi inerente ființei umane. În continuare, pornind de la lezarea dreptul la viață privată ca urmare a limitelor securității cibernetice în domeniul medical și ulterior de la erorile digitalizării cu impact asupra egalității și integrității fizice și psihice, vom aborda însăși protecția dreptului la viață în contextul unei eventuale greșeli sau decizii fatale a inteligenței artificiale. Infrastructura în domeniul medical se dovedește a fi o primă provocare tangențială celor analizate anterior în cuprinsul prezentei lucrări. Dincolo de dificultatea colectării datelor cu relevanță medicală, se distinge și în această situație dificultatea apărării împotriva atacurilor cibernetice, chiar pentru motivele prezentate deja, anume generarea de identități false. Odată cu implementarea digitalizării în sistemele de sănătate internaționale, statele nu au putut asigura mijloacele necesare de securitate cibernetică, motiv ce a dus la o stagnare a acestui domeniu, pe de o parte, și la o neîncredere vădită din partea pacienților, pe de altă parte. Reticența de a permite

34 Daisy Yuhas, *Doctors have trouble diagnosing Alzheimer's. AI doesn't, NBC NEWS,* 30 octombrie 2017, disponibil la: https://www.nbcnews.com/mach/science/doctors-have-trouble-diagnosing-alzheimer-s-ai-doesn-t-ncna815561%20[https://perma.cc/6DJU-8S4B], data ultimei accesări: 20 martie 2023.

accesul la datele lor genetice[35] este deci justificată, studiile arătând în ultimii ani o creştere continuă a atacurilor cibernetice, sistemele medicale fiind printre cele mai vizate, realizându-se astfel o încălcare a principiilor enunţate de Regulamentul UE 2016/679, anume prelucrarea *în mod legal, echitabil şi transparent faţă de persoana vizată* (art. 5 alin. (1) lit. a)) şi colectarea *în scopuri determinate, explicite ş i legitime (...) în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile iniţiale* (art. 5 alin. (1) lit. (b)). Un exemplu care arată pericolul celor menţionate este un caz din Irlanda ce a afectat atât de puternic sistemul unei clinici încât toate procedurile realizate de aceasta au fost blocate, inclusiv tratamentul pentru cancer al unei paciente, durata de refacere a sistemului fiind de ordinul lunilor.[36] Remarcăm că în acest domeniu se poate produce o prejudiciere atât a protecţiei datelor personale, cât şi a accesului la sănătate. Diagnosticarea pacienţilor, în ciuda rezultatelor bune oferite de I.A., există în prezent obstacole ce nu pot fi ignorate în contextul analizei asigurării unor drepturi fundamentale ale omului. Independent de voinţa programatorilor, unele sisteme ale I.A. au prezentat cazuri de discriminare, oferind diagnostice şi tratamente mai bune unor anumite categorii de persoane, situaţie faţă de care a fost deja exprimată îngrijorarea că va accentua lipsa de echitate în domeniul sanitar[37]. În plus, însăşi diagnosticarea corectă pare a fi uneori dificilă, cu atât mai mult în contextul apariţiei programelor de diagnosticare online. Referitor la aceasta apare problema răspunderii juridice în caz de erori şi dacă poate fi vorba chiar despre malpraxis în acele situaţii în care, fie printr -un diagnostic sau plan de tratament greşit, fie prin operaţia efectuată de către sau cu ajutorul I.A. are loc prejudicierea sănătăţii sau vieţii persoanei. Până în prezent, ordinea juridică nu a oferit un răspuns în faţa acestor probleme presante, existând pe de altă parte un număr restrâns de teorii enunţate cu privire la persoana împotriva căreia se îndreptă răspunderea juridică, ce au susţinut fie teoriile aplicabile altor sisteme digitale (de exemplu, pilotul automat la maşini) ce consideră eroarea un defect al produsului, situaţie în care răspunderea revine producătorului[38], fie teorii înrădăcinate în etică şi filosofie, potrivit cărora răspunderea este mixtă ce revine tuturor celor implicaţi[39].

35 „Date genetice" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective şi care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză. Potrivit Regulamentul (UE) 2016/679.

36 HSE cyber-attack: *Irish health service still recovering months after hack*, 5 septembrie 2021, disponibil la: HSE cyber-attack: Irish health service still recovering months after hack - BBC News, data ultimei accesări: 20 martie 2023.

37 Ben Leonard, Ruth Reader, *Artificial intelligence was supposed to transform healthcare. It hasn`t, 15 august 2022, disponibil la:* Artificial intelligence was supposed to transform health care. It hasn't. - POLITICO, data ultimei accesări: 28 martie 2023.

38 Frank Griffin, *Artificial intelligence and liability in healthcare,* Health Matrix, Volume 31, 2021, pp. 78-80.

39 Victoria Maria Deliu, *Interviu cu doamna profesoara Mihaela Constantinescu*, 31 iulie 2022, disponibil la: Interviu cu doamna profesoară Mihaela Constantinescu:

## Secţiunea a III-a
## Concluzie

În cele din urmă, realizarea drepturilor personalităţii se remarcă a fi o provocare în complexitatea digitală pe care omul a integrat-o în existenţa sa, văzându-se nevoit, într-un anumit punct al evoluţiei, să se integreze chiar el în lumea pe care a creat-o. Astfel, o analiză a oportunităţilor legale actuale se impune în final, fiind evident în acest punct al lucrării că un echilibru decizional presupune opţiuni prudente din partea legiuitorului, alături de reglementări vizionare, vehemente, certe.

Pe de o parte, se poarte remarca interesul sporit al lumii dreptului pentru crearea unui cadru juridic exhaustiv care să permită realizarea drepturilor subiective ale indivizilor. Progresul, deşi lent, se remarcă ş i prin Propunerea de Regulament al Parlamentului European şi al Consiliului de Stabilire a unor norme armonizate privind inteligenţa artificială (legea privind inteligenţa artificială) şi de modificare a anumitor acte legislative ale uniunii din 21 aprilie 2021 care nu s-a concretizat încă într-o normă a Uniunii. Pentru România, stat a cărei legislaţie preferă imixtiuni ale reglementării supranaţionale în dauna unei reglementări proprii, etatice, acest aspect se întrevede benefic, întrucât este imprecisă rata criminalităţii în domeniul manipulărilor prin I.A., victimele acestor fapte având o atitudine pasivă. Tehnologiile amintite, oricum, prezintă, aşa cum s-a arătat, consecinţe benefice în special pentru manifestarea creativităţii umane, prin urmare investiţiile şi interesul tehnologizării permiţând chiar realizarea a numeroase drepturi ale personalităţii şi nu numai.

Pe de altă parte, impactul negativ a fost deja subliniat. Legislaţia însă se arată sceptică şi, adesea, refuză să numească precis pericolul, neataşând o sancţiune evidentă unor fapte ce ar trebui văzute ca infracţiuni de sine stătătoare, nu parte a conţinutului unor alte infracţiuni existente, conţinut supus interpretării. Din nefericire, clemenţa legii instituie excepţii nepermise în contextul alarmant al perfecţionării I.A., putând lua în considerare chiar Propunerea mai sus amintită care, în art. 52, alin. (3) prevede că obligaţia de etichetare a conţinutului deepfake „nu se aplică (...) pentru exercitarea dreptului la libertatea de exprimare şi a dreptului la libertatea artelor şi ştiinţelor garantate în Carta drepturilor fundamentale a UE şi sub rezerva unor garanţii adecvate pentru drepturile şi libertăţile terţilor.” Exemplele care denotă provocări ale realizării drepturilor personalităţii pot continua, chiar în domeniul securizării prezen ţei online a individului, a unei lipse evidente de control a platformelor care nu îşi ascund finalitatea contrară legii, alături de evidenta neglijenţă cu care se operează în domeniul medical. Cât priveşte drepturile de autor, proprietatea intelectuală care implică într-o formă sau alta I.A. este interesul actual al societăţ ii, totuşi, aşa cum se remarcă, este mai degrabă tratat în manieră ambiguă, fără a lua în considerare potenţialul contemporan al relaţiilor juridice existente.

---

„Înţelepciunea practică este ceva ce sistemele de IA nu pot ajunge să dezvolte” - Syntopic, data ultimei accesări: 20 martie 2023.

## Secţiunea a IV-a
## Propuneri *de lege ferenda*

Astfel, prezentarea ocurenţelor ameninţătoare în privinţa realizării drepturilor personalităţii presupune ş i eviden ţierea posibilelor ameliorări ale sistemului legislativ existent în ce priveşte **problema deepfake** , a **furtului de identitate sintetic** şi a **diverselor domenii** în care tehnologia I.A. are un potenţial evident de interferenţă cu protecţia drepturilor omului.

În România, cât priveşte **fenomenul deepfake** şi **al furtului de identitate sintetic**, acestea nu au atins cotele alarmante ale situaţiilor din alte state, totuşi atingeri ale drepturilor personalităţii există şi la nivelul statului, mai ales prin atingeri aduse dreptului la imagine şi demnităţii persoanei. În acest sens, cu titlu preventiv nu numai la nivel supranaţional sau internaţional trebuie luate măsuri, dar şi la nivel etatic. În principal, trebuie luată în considerare **investiţia în tehnologie I.A. capabilă să detecteze conţinutul falsificat**, şi nu numai, complementar acestei măsuri punându-se cu adevărat problema unei evidenţe a acestei tehnologii benefice, aşa încât **accesul la aceasta să fie prudent şi selectiv**. Accentuăm astfel propunerea Uniunii Europene de legiferare astfel încât să devină obligatorie **existenţa unui semn distinctiv** aplicat fotografiilor generate digital. De altfel, pe lângă cerinţa pregnantă a **transparenţei** platformelor şi a creatorilor online, poate fi luată în considerare chiar **diminuarea considerabilă a anonimităţii** oferite de anumite aplicaţii şi platforme online. „În China, de exemplu, utilizatorii platformelor online trebuie să se înregistreze utilizând cartea de identitate”[40]. Totuş i, o astfel de abordare pune în discuţie chiar beneficiile anonimităţii, inclusiv faptul că anonimitatea este adesea o metodă a securităţii cibernetice. În altă ordine de idei, cu referire la legislaţ ia curentă, **o revizuire a RGPD** ar fi oportună, astfel încât să existe fie un ghid de aplicare a RGPD conţinutului fals rezultat din deepfake, fie o extindere explicită a aplicării RGPD la datele cu caracter personal colectate prin intermediul vocii şi al trăsăturilor faciale. Totodată, ar fi oportună **existenţa incriminării** punctuale a creării materialelor false; în acest sens, se poate observa cum, în Germania, de exemplu, „distribuirea materialelor deepfake care violează datele personale (...) este prohibită, dar nu şi producţia lor.”[41] În acela şi timp, în Franţa este prohibită în Codul Penal publicarea unui material editat al unei persoane dacă nu există consimţământul acesteia[42], ceea ce face posibilă incriminarea însă şi a deepfake-ului. Astfel, dacă în exemplele date legea fie nu incriminează modalităţi ale unei activităţi ilicite, în dauna salvgardării garanţiilor oferite, în primul rând, dreptului la imagine, fie reuşeşte să proiecteze vizionar aceasta, legea penală română omite cu desăvârşire să

40 STOA, *op. cit*., p. 62.
41 *Idem*, p. 61.
42 Code pénal, art. 226-8, version au vigueur 22 mars 2023, https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/: „Est puni d'un an d'emprisonnement et de 15.000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention.”

prevadă existența unui posibil deepfake. Art. 226, alin. (1)-(2) din Codul Penal, care vizează violarea vieții private, se exprimă astfel: „Atingerea adusă vieții private, fără drept, prin fotografierea, captarea sau înregistrarea de imagini, ascultarea cu mijloace tehnice sau înregistrarea audio a unei persoane aflate într-o locuință sau încăpere ori dependin ța ținând de aceasta sau a unei convorbiri private se pedepsește (...) Divulgarea, difuzarea, prezentarea sau transmiterea, fără drept, a sunetelor, convorbirilor ori a imaginilor prevăzute în alin. (1), către o altă persoană sau către public, se pedepsește (...)", urmând a prezenta generos excepțiile. Răspunderea I.A. poate viza și **sancțiunea utilizării de către sistemele computerizate inteligente a operelor autentice**, venind adesea cu o compilație care încalcă în realitate drepturile de autor ale artiștilor. Problema răspunderii I.A. este însă una sensibilă care ar trebui să se bucure cu atât mai mult de atenția legiuitorului, cu atât mai mult **în domeniul medical**, așa cum a fost arătat deja, unde potențialul benefic pare compromis de incertitudinea repercusiunilor asupra dreptului la sănătate al persoanei. Nu în ultimul rând, dat fiind faptul că Internetul și re țelele de socializare au devenit spații publice, recunoscute astfel jurisprudențial, legiuitorul național ar trebui să ia în considerare **restrângerea** justificată a **dreptului părinților de a face publică imaginea copilului** acestora, întrucât, în acest caz, este clară lipsa consimțământului acestuia și poten țialul actual de încălcare a drepturilor personalității acestora. Problema se poate întinde simetric și în ce privește manipularea imaginilor cu cei decedați, încât să se realizeze „introducerea unui **registru** în care oamenii **să declare cum vor ca datele lor să fie utilizate** după moartea acestora ar putea fi luată în considerare."[43]

În concluzie, atitudinea activă a legiuitorului în domeniul combaterii fenomenelor periculoase generate de I.A. ar trebui plusată de **inserția în educație a unei discipline cu un profund caracter etic** în tehnologie, astfel încât copilul modern, implicit adultul lumii tehnologizate de mâine să fie conș tient în principal de consecințele periculoase ale faptelor sale, acest aspect determinând, probabil, o atitudine grijulie în ce privește manifestarea creativității sale, manifestare care trebuie să aibă în vedere drepturile semenilor.

## Secțiunea a V-a
## Bibliografie


*A Quick History of Deepfakes: How It All Began*, 16 noiembrie 2022, disponibil la: https://q5id.com/blog/a-quick-history-of-deepfakes-how-it-all-began, data utlimei accesări: 17 martie 2023.

Ben Leonard, Ruth Reader, Artificial intelligence was supposed to transform healthcare. It hasn`t, 15 august 2022, disponibil la: Artificial intelligence was supposed to transform health care. It hasn't. - POLITICO, data ultimei accesări: 28 martie 2023.

Code pénal, art. 226-8, version au vigueur 22 mars 2023, https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/.


43STOA, *op. cit*., p. 64.

Comitetul pentru viitorul științei și tehnologiei (STOA), *Tackling deepfakes in European policy,* 30.
iulie2021, articol disponibil PDF la: https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)690039, data ultimei accesări: 18 martie 2023.
Carta drepturilor fundamentale a Uniunii Europene, publicată în JOUE, C 326 din 26 octombrie 2012, pp. 391-407.
Daisy Yuhas, *Doctors have trouble diagnosing Alzheimer's. AI doesn't, NBC NEWS,* 30 octombrie 2017, disponibil la: https://www.nbcnews.com/mach/science/ doctors-have-trouble-diagnosing-alzheimer-s-ai-doesn-t-ncna815561%20[https://perma.cc/6DJU-8S4B], data ultimei accesări: 20 martie 2023.
Directiva 2001/29/CE publicată în J.O.U.E., L 167 din 22 iunie 2001, pp. 10-19.
ERGA, *ERGA Report on Disinformation: Assessment of the Implementation of the Code of Practice*, 2020, disponibil la: https://erga-online.eu/wp-content/uploads/2020/05/ERGA -2019-report-published-2020-LQ.pdf, data ultimei accesări 18 martie 2023.
Experian, *Synthetic ID Fraud*, articol disponibil la: Protecting Yourself Against Synthetic Identity Fraud | Experian, data ultimei accesări: 18 martie 2023.
Frank Griffin, *Artificial intelligence and liability in healthcare,* Health Matrix, Volume 31, 2021, pp. 78-80.
Glenn Larson, *Synthetic Identity Fraud Is The Fastest Growing Financial Crime -- What Can Banks Do To Fight It?,* 8 octombrie 2019, disponibil la: Synthetic Identity Fraud Is The Fastest Growing Financial Crime -- What Can Banks Do To Fight It? (forbes.com), data ultimei accesări: 19 martie 2023.
Hans von der Burchard, *Belgian socialist party circulates 'deep fake' Donald Trump video*, 21 mai 2018, articol disponibil la https://www.politico.eu/article/spa-donald-trump-belgium-paris-climate-agreement -belgian-socialist-party-circulates-deep-fake-trump-video/, data ultimei accesări 18 martie 2023.
Henry Mance, *Carlo Rovelli: "Science is not just about writing equations. It`s about reconceptualising the world"*, 26 septembrie 202, articol disponibil la: Carlo Rovelli: 'Science is not just about writing equations. It's about reconceptualising the world' | Financial Times (ft.com), data ultimei accesări: 18 martie 2023.
HSE cyber-attack: *Irish health service still recovering months after hack*, 5 septembrie 2021, disponibil la: HSE cyber -attack: Irish health service still recovering months after hack - BBC News, data ultimei accesări: 20 martie 2023.
Jesse Damiani, *A Voice Deepfake Was Used To Scam A CEO Out of $243,000*, 3 septembrie 2019, articol disponibil la: https://www.forbes.com/ sites/jessedamiani/2019/09/03/a-voice-deepfake-was -used-to-scam-a-ceo-out-of-243000/?sh=2f608f982241, data ultimei accesări: 18 martie 2023.

Kaylee Fagan, *A viral video that appeared to show Obama calling Trump a 'deep---' shows a disturbing new trand called 'deepfakes'*, 17 aprilie 2018, articol disponibil la: https://www.businessinsider.com/obama-deepfake-video-insulting-trump-2018-4, data ultimei accesări: 18 martie 2023.

Legea nr. 8 din 14 martie 1996, publicată în M. Of. nr. 489 din 14 iunie 2018.

Legea nr. 365 din 7 iunie 2002, publicată în M. Of. nr. 959 din 29 noiembrie 2006;

Legea nr. 504 din 11 iulie 2002, publicată în M. Of. nr. 534 din 22 iulie 2002.

Patrick Ryan, *'Deepfake' audio evidence used in UK court to dicredit Dubai dad*, 8 februarie 2020, articol disponibil la: https://www.thenationalnews.com/uae/courts/deepfake-audio-evidence-used-in-uk-court-to-discredit-dubai-dad-1.975764, data ultimei accesări: 18 martie 2023.

Propunere de Regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind Inteligența Artificială (Legea Privind Inteligența Artificială) și de modificare a anumitor acte legislative ale Uniunii, 21 aprilie 2021, COM/2021/206 final.

Random Outputs, disponibil la: https://randomoutputs.com/random-face-generator, 20 octombrie 2022, data ultimei accesări: 19 martie 2023;

Remigijus Jokubauskas și Marek Świerczyński, *Is Revision of the Council of Europe Guidelines on Electronic Evidence Already Needed?*, în „Utrecht Law Review", Vol. 16, no.1, 26 mai 2020, pp. 13-20, articol disponibil la: https://doi.org/10.36633/ulr.525.

Sarah Cahlan, *How misinformation helped spark an attempted coup in Gabon*, 13 februarie 2020, articol disponibil la: https://www.washingtonpost.com/politics/2020/02/13/how-sick-president-suspect-video-helped-sparked-an-attempted-coup-gabon/, data ultimei accesări: 18 martie 2023.

Toby Walsh în lucrarea *2062. Lumea creată de inteligența artificială,* Ed. RAO, 2021.

Victoria Maria Deliu, *Interviu cu doamna profesoară Mihaela Constantinescu*, 31 iulie 2022, disponibil la: Interviu cu doamna profesoară Mihaela Constantinescu: „Înțelepciunea practică este ceva ce sistemele de IA nu pot ajunge să dezvolte" - Syntopic, data ultimei accesări: 20 martie 2023.