AUB DREPT

Forum Juridic nr. 3 / 2021

ANALELE UNIVERSITĂȚII DIN BUCUREȘTI - SERIA DREPT

Crearea de portrete fictive utilizând rețele neurale adversariale. Relația cu infracțiunile de fals

Cristian-Tiberiu Stănescu
Master Științe Penale
Facultatea de Drept, Universitatea din București

Rezumat: *Acest articol își propune să cerceteze raportul între infracțiunile de fals și generarea unor portrete ale unor persoane care nu există în realitate prin intermediul rețelelor neurale ce au la bază Inteligența Artificială, care deschide căi de săvârșire a unor infracțiuni de natură să schimbe paradigmele clasice ale dreptului penal. Astfel, prima parte reprezintă o introducere succintă în domeniul Inteligenței Artificiale și a rețelelor neurale, în cadrul căreia sunt trasate câteva clarificări terminologice și de funcționare a unor astfel de rețele, urmând o scurtă analiză a infracțiunilor de fals din actuala legislație penală, pentru a vedea care dintre acestea prezintă relevanță pentru acest context. Ulterior, sunt analizate anumite divergențe existente anterior în doctrină în legătură cu crearea de profiluri, tranșate de o decizie cu caracter obligatoriu a instanței supreme. În sfârșit sunt expuse, în lumina deciziei amintite, ipoteze în care ar putea fi reținute infracțiuni de fals prin utilizarea de portrete fictive.*

Cuvinte cheie: *Inteligență Artificială, rețele neurale, profiluri fictive, infracțiuni de fals, fals informatic.*

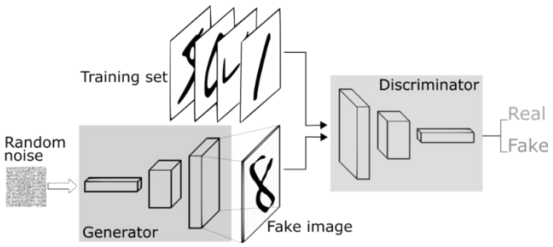
Creating fake portraits using adversarial neural networks. A correlation with crimes of forgery

Abstract: *This article aims to analyse the relation between crimes of forgery and generating portraits of people who do not actually exist using neural networks with Artificial Intelligence, which opens new ways of committing crimes that are able to change the traditional paradigm of criminal law. Therefore, the first part submits a brief introduction to Artificial Intelligence and neural net Works, in which some terminological and functioning method clarifications are made, followed by a concise review of the crimes of forgery regulated by the criminal code in force. Subsequently, some particular divergencies existing in criminal doctrine regarding the creation of fake profiles, solved by a mandatory ruling of the supreme court. Finally, in respect to the aforementioned ruling, some examples in which the crime of forgery can be committed using fake profile photos are given.*

Key words: *Artificial Intelligence, neural networks, fake profiles, crimes of forgery, computer-related forgery.*

I. REȚELE NEURALE ADVERSARIALE GENERATOARE DE PORTRETE UMANE

Inteligența Artificială este definită ca o soluție de tip software, dezvoltată utilizând tehnici cum ar fi cele de tip *„machine learning”* sau învățare nesupravegheată prin consolidare, care poate genera conținut de tipul unor predicții, recomandări sau decizii care influențează mediul de lucru cu care interacționează și care efectuează aceste operațiuni urmărind obiective trasate de un actor uman[1]. La baza acestor tehnici stau rețelele neurale, care se aseamănă, fără a se identifica cu structurile sinaptice ale creierului uman[2]. Un subtip al acestor tehnici este cea a rețelelor generative adversariale[3] (*generative adversarial networks – GAN*). Este vorba despre o pereche de rețele neurale care se află într-o competiție una cu cealaltă, fiind „adversari” în procesul de generare a unor date noi pe baza unui set inițial care le-a fost furnizat. Prima rețea, denumită *generator*, colectează un set de date dintr-un vector latent (o formă de compresie a datelor), iar pe baza acestora generează o imagine nereală, un portret fictiv în acest caz. Cea de-a doua rețea, denumită *discriminator*, efectuează o comparație între imaginea falsă pe care o primește de la *generator* și o imagine reală dintr-un set distinct de date cu portretele unor persoane reale. Urmare a acestei comparații, algoritmul discriminant oferă fie un rezultat pozitiv, fie unul negativ, după cum consideră că imaginea creată de *generator* este sau nu reală. Acest rezultat este trimis printr-un proces de propagare inversă *(backpropagation)*, bazat pe o funcție matematică, înapoi către *generator*, care își adaptează imaginile subsecvente pentru a putea, în cele din urmă „păcăli” *discriminatorul*. Dacă aceste operațiuni sunt derulate cu succes, la finalul procesului de antrenare a rețelei adversariale *generatorul* va fi capabil să creeze o imagine suficient de autentică astfel încât *discriminatorul* nu va putea să o clasifice ca fiind falsă[4].



Sursa: https://www.freecodecamp.org/

Dacă se accesează site-ul de internet https://www.thispersondoesnotexist.com/, întregul proces laborios descris anterior este efectuat în mai puțin de o secundă, fiind astfel

[1] A se vedea Propunerea de Regulament a Parlamentului și Consiliului privind Inteligența Artificială, disponibilă la https://ec.europa.eu/.

[2] Pentru o explicație elocventă a funcționării acestor rețele, chiar și pentru cineva fără cunoștințe de specialitate, a se vedea *A. Matthias*, Neural Networks without the Math, Joyful AI, Book *1*, Joyously Aware Media, 2018.

[3] A se vedea *L.M. Stănilă*, Inteligența artificială, dreptul penal și sistemul de justiție penală. *Amintiri despre viitor*. Ed. Universul Juridic, București, 2020, p. 54.

[4] A se vedea *I. Goodfellow et. alii*, Generative Adversarial Networks, Proceedings of the International Conference on Neural Information Processing Systems (NIPS 2014), pp. 2672–2680.

generat portretul unei persoane care nu există[5]. O ipoteză interesantă ar apărea în cazul antrenării unei astfel de rețele cu date reprezentând portretele membrilor unei familii, unde există posibilitatea ca un algoritm suficient de bine antrenat să reproducă imaginea unei persoane care nu există în prezent, dar ar avea un portret similar cu un viitor descendent al membrilor acelei familii.

II. INFRACȚIUNI DE FALS UNDE ESTE RELEVANT PORTRETUL UNEI PERSOANE

În Titlul VI al Codului penal român sunt reglementate infracțiunile de fals în trei mari categorii: falsificarea de monede, timbre sau alte valori (Capitolul I), falsificarea instrumentelor de autentificare sau marcare (Capitolul II) și falsuri în înscrisuri (Capitolul III). La o analiză atentă a conținutului acestor infracțiuni, urmează să fie excluse din analiză primele două capitole, pentru că natura obiectului falsurilor este incompatibilă cu portretul unei ființe umane. În ultimul capitol sunt reglementate opt infracțiuni de fals

Deși majoritatea acestora cunosc ipoteze unde falsul poate viza fotografia portretului unei persoane, trebuie subsecvent cercetate ipotezele unde este relevant un portret fictiv care poate produce consecințe juridice.

În ceea ce privește infracțiunea de fals material în înscrisuri oficiale, în doctrină s-a arătat că aceasta poate viza, spre exemplu, actele de stare civilă[6]. Sunt de părere că mai pot fi menționate și alte acte oficiale cum ar fi, spre exemplu, permise de conducere, de vânătoare sau de călătorie pe căile ferate, pentru că și acestea au fotografia titularului printre elementele de identificare. În această modalitate, apare în discuție comiterea infracțiunii de fals privind identitatea. Această infracțiune se comite, de regulă, prin falsificarea altor elemente de identificare a actului, cum ar fi numele, domiciliul, adresa, cetățenia[7]. Utilizarea acestor înscrisuri oficiale se face în situații în care titularul este și el prezent fizic în momentul utilizării, astfel că o infracțiune de fals privind identitatea apare ca fiind improbabil de comis în această manieră, pentru că ar fi greu de imaginat motivul pentru care un conducător auto ar prezenta agentului de poliție rutieră un permis cu o fotografie fictivă. Înainte de a declara această categorie inaplicabilă acestui demers, merită menționate acele situații în care accesul la un anumit serviciu este condiționat de prestatorul acestuia de prezentarea, de la distanță, a unui act de identitate. Spre exemplu, platforma *fintech* Revolut solicită unui nou utilizator atât o fotografie a cărții de identitate, cât și o fotografie personală pentru comparație. Dacă ce-a de-a doua condiție ar lipsi, cum se întâmpla în trecut, s-ar putea imagina situații în care falsificarea unui act de identitate incluzând o fotografie fictivă generată pe site-ul menționat *supra* să fie posibilă. În viitor, sistemul ar putea fi indus în eroare prin utilizarea fotografiei fictive atât pe actul de identitate, cât și pe fotografia de comparație, la un nivel suficient de ridicat încât să nu trezească suspiciunea sistemului sau administratorului platformei ce realizează verificarea. Este de precizat că în această modalitate nu ar mai fi vorba de falsul privind identitatea, care are drept cerință ca prezentarea să se facă unui funcționar public sau unei unități în care

[5] A se vedea *T. Karras et alii*, Analyzing and improving the image quality of StyleGAN, disponibil la https://arxiv.org/abs/1912.04958.
[6] A se vedea *M. Udroiu*, Sinteze de Drept penal. Partea specială, Ediția 2, Vol. II, Ed. C.H. Beck, București, 2021, p. 1033.
[7] Pentru o speță în care fictivitatea privea Codul Numeric Personal, a se vedea C.A. Cluj, dec. pen. nr. 1025/2021 din 15 iulie 2021, disponibilă pe *www.sintact.ro*.

aceasta își desfășoară activitatea, fiind vorba de un fals material în înscrisuri oficiale în concurs cu infracțiunea de uz de fals pentru actul de identitate și de un fals în înscrisuri sub semnătură privată (care absoarbe uzul de fals) pentru fotografia de comparație.

Infracțiunea de fals material în înscrisuri sub semnătură privată e susceptibilă de o sferă ceva mai largă de înscrisuri ce presupun o fotografie, care ar putea fi utilizată în scopul producerii de consecințe juridice[8]. Astfel, poate fi vorba de un card de acces într-un anumit club sportiv, card de fidelitate al unui lanț de magazine, un *curriculum vitae* precum și orice act ce servește la identificare și nu emană de la o autoritate sau instituție publică. Dificultatea de a imagina un exemplu vizând o fotografie fictivă subzistă însă și în acest caz, deși pot fi imaginate exemple similare celor de mai sus.

III. PORTRETELE FICTIVE ȘI INFRACȚIUNEA DE FALS INFORMATIC

Infracțiunea de fals informatic apare ca fiind cea mai relevantă din perspectiva acestui demers. Este fapta de a introduce, modifica sau șterge, fără drept, date informatice ori de a restricționa, fără drept, accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice. Rațiunea reglementării acestei infracțiuni a fost adaptarea cadrului juridic penal al infracțiunilor tradiționale de fals în înscrisuri la domeniul criminalității informatice, prin crearea unui paralelism cu acestea[9]. Pentru început, trebuie cercetat dacă portretele generate potrivit metodei amintite *supra* sunt circumscrise noțiunii de date informatice, definite de legiuitor în art. 181 C. pen[10]. Răspunsul nu poate fi decât afirmativ, faptul că o imagine digitală intră în această categorie fiind confirmat și de literatura de specialitate[11]. Deși contrafacerea și alterarea nu au mai fost prevăzute de legiuitor ca modalități ale elementului material similar infracțiunilor anterior amintite, în doctrină se face distincția între aceste două acțiuni[12]. În contextul analizat, este relevantă acțiunea de contrafacere a datelor, dat fiind modul în care funcționează algoritmul cu Inteligență Artificială, explicat *supra.* Față de cele expuse până în acest moment, se impune a fi făcută o distincție. Astfel, la o primă vedere pare că funcționarea în sine a acestui algoritm s-ar încadra în sfera de tipicitate a infracțiunii de fals informatic. Programatorul algoritmului realizează într-adevăr o introducere de date informatice, în urma căreia rezultă date necorespunzătoare adevărului, ca urmare a operațiunilor efectuate. Cu toate acestea, fapta nu este săvârșită fără drept[13] și nici în scopul producerii de consecințe juridice, ci în scop experimental, eventual didactic,

[8] În doctrină au fost excluse din această categorie cărțile de vizită care nu produc prin ele însele, consecințe juridice. A se vedea *C. Rotaru, A.-R. Trandafir, V. Cioclei*, Drept penal. Partea specială II. Curs tematic, Ediția 5, Ed. C.H. Beck, 2021, p. 396.

[9] A se vedea Raportul explicativ al Convenției privind criminalitatea informatică, p. 81, *apud G. Zlati*, Tratat de criminalitate informatică, Vol. I, Ed. Solomon, 2020, p. 479.

[10] Art. 181 alin. (2) C.pen.: *„Prin date informatice se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic*", iar potrivit alin. 1 al aceluiași articol *„Prin sistem informatic se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic".*

[11] A se vedea *G. Zlati*, op. cit., p. 102.

[12] A se vedea *G. Zlati*, op. cit., p. 490.

[13] Doar în ipoteza în care portretele unor persoane au fost utilizate fără consimțământul acestora, s-ar putea pune în discuție lipsa unui „drept".

academic. Totuși, nu este mai puțin adevărat că datele rezultate în urma acestui proces ar putea face la rândul lor obiectul unei introduceri, fără drept, în scopul producerii unei consecințe juridice. Este vorba despre crearea unui profil pe rețelele de socializare utilizând date care nu corespund adevărului. Inițial, în doctrină s-au formulat două opinii în legătură cu această situație. Într-o primă abordare[14], s-a considerat că această conduită nu întrunește elementele de tipicitate ale falsului informatic. În argumentarea acestui punct de vedere s-a plecat de la rațiunea textului de lege, paralela cu falsul tradițional, pentru a trage concluzia că fapta la care am făcut referire nu îndeplinește nici condiția *„fără drept”*, nici condiția ca datele să fie „necorespunzătoare adevărului”, cerute de norma de incriminare. Consider că relevantă pentru acest demers este cu precădere cea de-a doua cerință. S-a considerat că datele necorespunzătoare adevărului trebuie întregite de cerința aptitudinii de a genera consecințe juridice. Astfel, crearea unui cont pe rețelele de socializare utilizând date necorespunzătoare adevărului nu este, *per se*, o conduită generatoare de consecințe juridice, prin urmare, fapta nu este tipică din această privință.

Această opinie se regăsește și în practica judiciară spre exemplu Decizia nr. 234/Ap din 03.06.2020 pronunțată de Curtea de Apel Brașov[15].

Cea de-a doua opinie este în sensul întrunirii condițiilor de tipicitate, având la bază argumente diferite, anume includerea acestei conduite în sfera mai largă a *„furtului de identitate”* care este inclus în sfera ilicitului penal atât de reglementarea falsului informatic, dar și de alte incriminări, cum ar fi accesul neautorizat la un sistem informatic, transferul neautorizat de date informatice sau interceptarea ilegală a unei transmisii de date informatice[16]. Cât privește crearea unui cont pe o rețea de socializare, această opinie distinge între contul fals și contul fictiv[17]. Contul fals este rezultatul introducerii unor date de identificare uzurpate de la o persoană reală (nume și prenume, fotografie, pregătire academică, profesie etc.), pe când un cont fictiv este creat utilizând date de identificare care nu aparțin nimănui sau care sunt atribuite unor personaje fictive din cărți, filme sau jocuri video. Această distincție pune problema liniei de demarcație între fictiv și fals, din perspectiva minimului de date necesare unui cont fictiv pentru a trece în categoria contului fals. Înainte de această analiză, se impune precizarea evidentă că fotografiile generate cu ajutorul site-ului *thispersondoesnotexist.com* se încadrează in categoria datelor fictive. Problema apare în momentul creării unui cont unde toate datele de identificare mai puțin fotografia aparțin unei persoane reale. Este acesta un cont fals? Răspunsul negativ pare ușor de dat în ipotezele în care fotografia este cea vizată, dar pe baza acestuia nu poate fi trasă concluzia că pentru a fi în prezența unui cont fals trebuie ca toate datele cuprinse de acesta să aparțină unei persoane reale. Față de această constatare, nu cred că un cont care conține toate datele reale ale unei persoane, dar un loc de muncă fictiv sau un prenume fictiv adăugat poate fi încadrat fără dubii în categoria conturilor fictive. În orice caz, fapta se consideră a fi tipică doar în ceea ce privește conturile false. Un argument suplimentar adus în susținerea acestei opinii este legat de alte conduite infracționale, unanim acceptate ca subsumate falsului informatic. Este vorba, spre exemplu de *„phishing”* și *„pharming”*. Într-o succintă și simplă definiție, aceste situații aflate în relație de întreg-parte presupun crearea

[14] A se vedea *D. Pârgaru*, Despre limitele falsului informatic în cazul rețelelor de socializare. Opinie cu privire la dezlegarea unei chestiuni de drept în materie penală, disponibil pe www.juridice.ro.
[15] Disponibilă pe www.rolii.ro *apud D. Pârgaru*, cit. supra.
[16] A se vedea *G. Zlati*, op. cit., p. 593.
[17] *Idem,* p. 531.

unei aparențe utilizând date informatice pentru a induce în eroare un utilizator că un e-mail sau un site de internet este autentic, pentru ca acesta să introducă date cum ar fi numărul și pinul unui card de credit sau adresa de e-mail. De cele mai multe ori, scopul acestora se subsumează infracțiunii de înșelăciune, activitatea fiind întreprinsă în scopul producerii unei pagube, dar această cerință nu este necesară pentru întrunirea tipicității infracțiunii de fals informatic. Se consideră că aceeași ar trebui să fie situația și în cazul creării unui cont fals pe rețelele de socializare.

La rândul ei și această a doua opinie a fost exprimată în jurisprudență, Curtea de Apel Târgu Mureș considerând fapta de a deschide diverse conturi utilizând datele de identitate (inclusiv adresa de e-mail) a unei persoane fără drept și fără știința acesteia ca întrunind tipicitatea falsului informatic[18]. Această diferență de orientare jurisprudențială a fost tranșată de o hotărâre prealabilă pentru dezlegarea unor chestiuni de drept pronunțată de Înalta Curte de Casație și Justiție, care prin decizia nr. 4 din 25 ianuarie 2021[19] a considerat că a doua opinie este cea corectă, stabilind cu caracter obligatoriu că *„fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului, folosind ca nume de utilizator numele unei alte persoane și introducând date personale reale care permit identificarea acesteia, întrunește două dintre cerințele esențiale ale infracțiunii de fals informatic prevăzută în art. 325 din Codul penal, respectiv cea ca acțiunea de introducere a datelor informatice să fie realizată fără drept și cea ca acțiunea de introducere a datelor informatice să aibă ca rezultat date necorespunzătoare adevărului”*. Pentru a pronunța această soluție, cu referire la cerința *„fără drept”*, instanța supremă a reținut că în crearea unui cont cu datele altei persoane, agentul *„acționează prin încălcarea manifestării de voință a persoanei a cărei identitate și-a uzurpat-o”,* pentru că nu există nicio dispoziție legală sau contractuală care să permită acest lucru. Cât privește condiția ca datele să fie necorespunzătoare adevărului, s-a dat prevalență teoriei intelectuale a falsului, care acordă o importanță superioară falsificării manifestării de voință, iar nu neapărat a materialității unui înscris[20]. *„Așadar, datele necorespunzătoare adevărului rezultate privesc emitentul acestora și constau în lipsa concordanței între făptuitorul care introduce date ca fiind datele proprii și persoana căreia acestea îi aparțin în realitate. Între datele informatice astfel contrafăcute (în modalitatea introducerii fără drept) și realitatea obiectivă nu există corespondență, manifestarea de voință reflectată de aceste date aparținând unei alte persoane (făptuitorului) decât celui care aparent este titular al contului (voința de publicare a datelor nu este reală)*”.[21]

Aceste două cerințe de tipicitate au fost singurele cu care instanța supremă a fost sesizată și cu privire la care s-a pronunțat, scopul activităților desfășurate fără drept și care au ca rezultat date necorespunzătoare adevărului să fie acela de a utiliza datele informatice în vederea producerii de consecințe juridice, au fost lăsate a fi apreciate *in concreto* în fiecare caz în parte. Consider că aceasta ar fi fost soluția corectă chiar dacă obiectul dezlegării ar fi inclus și aceste aspecte pentru că, în caz contrar, consecințele ar fi fost în sensul că orice persoană care își deschide un cont pe o rețea de socializare și furnizează o

[18] A se vedea C.A. Târgu Mureș, Secția penală, pentru cauze cu minori și de familie., dec. pen. nr. 123/A/2016, *apud G. Zlati*, op. cit., p. 532.
[19] M. Of. nr. 171/19.02.2021.
[20] A se vedea, pentru detalii despre teoria materială și intelectuală a falsului, *C. Rotaru, A.-R. Trandafir, V. Cioclei*, op. cit., p. 383.
[21] A se vedea I.C.C.J., Completul pentru dezlegarea unor chestiuni de drept, Decizia nr. 4/2021, X.2 B.

informație contrară realității (fie în datele de identificare, fie în postări ulterioare) ar fi comis infracțiunea de fals informatic[22].

Cu toate acestea, este important de menționat că instanța supremă nu a făcut referirea în motivarea deciziei la distincția cont fals-cont fictiv, cu toate că dezlegarea vizează folosirea drept *„nume de utilizator numele unei alte persoane”* și introducerea unor *„date personale reale care permit identificarea acesteia”*. Pe baza acestui argument urmează să fie identificate ipoteze în care chiar utilizarea unor date de identificare fictive ar putea atrage reținerea infracțiunii de fals informatic. Așa cum am arătat, este incontestabil în literatura de specialitate că activitatea de *phishing/pharming* intră sub incidența falsului informatic[23]. Se poate imagina un exemplu în care agentul creează o pagină de internet pentru a oferi sau promova un anumit bun sau serviciu, licit (consultanță financiară, juridică) sau ilicit (vânzarea de permise de conducere[24]), pagină pe care sunt inserate elemente pentru a spori încrederea potențialilor clienți, de tipul unor recenzii sau opinii de la așa-ziși clienți mulțumiți, unde pot fi folosite fotografii fictive, generate cu site-ul amintit anterior. Iată așadar, o primă ipoteză în care portretele fictive ar putea întruni cerințele de tipicitate ale infracțiunii de fals informatic, independent de reținerea și a altei infracțiuni precum înșelăciunea, în legătură cu inducerea în eroare decurgând din conduita descrisă. Suplimentar, cu referire și la dezlegarea de drept care viza crearea de conturi, pentru o încredere sporită în serviciul oferit, agentul ar putea insera un link către profilul de Facebook al clientului fictiv, conduită ce întrunește condițiile unui act de executare suplimentar al aceleiași infracțiuni de fals informatic. Păstrând cadrul rețelei de socializare Facebook, în anumite circumstanțe un cont fictiv ar putea căpăta o relevanță în ceea ce privește producerea de consecințe juridice. Spre exemplu, anumite premii de tip *giveaway* ar putea fi condiționate de numărul de aprecieri strânse la o anumită postare a participantului sau de numărul de prieteni etichetați în comentarii, caz în care o persoană care utilizează procedeul descris pentru a crea o multitudine de conturi false pentru a-și spori șansele de câștig, încălcând astfel condițiile de participare. Alte exemple vizează infracțiuni contra libertății psihice, cum ar fi amenințarea, șantajul sau hărțuirea unei persoane de pe astfel de conturi, faptă ce prezintă un pericol social mai ridicat dacă este comisă în acest mod, din cauza dificultății de a stabili o legătură între conturile fictive și cel care le-a creat. Argumentul contrar reținerii falsului informatic în aceste situații s-ar putea pune pe temeiul cerinței *„fără drept”*. Sensul acestei sintagme în contextul folosirii datelor informatice este oferit de dispozițiile art. 35 alin. (2) din Legea nr. 161/2003[25], care prevede că: *„(...) acționează fără drept persoana care se află în una dintre următoarele situații: a) nu este autorizată, în temeiul legii sau al unui contract; b) depășește limitele autorizării; c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic”*. Din analiza site-ului *thispersondoesnotexist.com* și a resurselor pe care acesta la prevede, care vizează articolul de specialitate redactat de autor și codul-sursă al algoritmului se poate trage

[22] La această concluzie s-a ajuns și în opiniile trimise de specialiști către Înalta Curte. A se vedea *D. Pârgaru*, cit. *supra.*
[23] A se vedea *G. Zlati*, op. cit., p. 417.
[24] A se vedea https://www.profit.ro/stiri/social/permise-auto-la-vanzare-fara-examen-cat-costa-si-cum-sunt-descoperite-falsurile-19632895, consultat la 10.08.2021.
[25] Monitorul Oficial, Partea I, nr. 279/21.04.2003.

concluzia că fotografiile de portret ale unor persoane reale pe care a fost antrenat sistemul au fost utilizate cu consimțământul acestora. Cu toate acestea, trebuie verificată existența a două manifestări de voință suplimentare pentru a nu fi în ipoteza cerinței folosirii fără drept: manifestarea de voință suplimentară a persoanelor din care a fost generat noul portret, ceea ce apare ca fiind excesiv și dificil, respectiv manifestarea de voință a titularului site-ului și a codului-sursă cu care au fost generate. În măsura în care acesta interzice utilizarea acestor date informatice pentru utilizarea lor în cazurile amintite, fapta se încadrează pe litera c) din textul de lege. Având în vedere că este puțin probabilă oferirea unei permisiuni cu valoarea unui consimțământ valabil din partea acestuia pentru utilizarea portretelor fictive în scopuri ilicite, fapta va îndeplini, de cele mai multe ori, condițiile de tipicitate.

IV. CONCLUZII

Rețelele neurale adversariale sunt pe cât de inovative, pe atât de periculoase din perspectiva facilității cu care pot fi deturnate în scopuri infracționale. Infracțiunile informatice reprezintă o categorie consacrată recent în domeniul dreptului penal, dar care pare să evolueze la un nivel mai ridicat decât toate celelalte, datorită progresului exponențial al tehnologiei. Exemplul oferit de acest articol este doar una dintre modalitățile de utilizare care au un risc extrem de ridicat să intre în sfera ilicitului penal. Din acest motiv, cercetarea noilor metode în care pot fi comise infracțiuni informatice utilizând Inteligența Artificială apare mai mult decât necesară.