Evoluția infracțiunii de fraudă informatică. Scurte considerații.

The Evolution of Computer-Related Fraud. Brief Considerations.

Cristian-Tiberiu STĂNESCU[1]

Rezumat: Articolul prezintă câteva ipoteze de comitere a infracțiunii de fraudă informatică în contextul dezvoltării tehnologiei informației. Având în vedere caracterul preponderent tehnic, dar și de noutate al acestor ipoteze, raportat la dificultățile deja existente în doctrina și practica judiciară cu privire la sfera infracțiunii de fraudă informatică, articolul nu oferă soluții general valabile, ci expune anumite situații la care mai devreme sau mai târziu doctrina și jurisprudența ar trebui să reflecteze. În prima parte sunt menționate aspecte introductive cu privire la infracțiunea de fraudă informatică în dreptul penal român, iar în cea de-a doua sunt avute în vedere două domenii din sfera tehnologiei informației ce prezintă interes prin particularitățile acestora.

Cuvinte-cheie: fraudă informatică, sistem informatic, date informatice, Inteligență Artificială, blockchain.

Abstract: *The article presents some hypotheses for committing the crime of computer-related fraud in the context of the development of information technology. Given the predominantly technical, but also novel nature of these hypotheses, in view of the difficulties already existing in doctrine and judicial practice regarding computer-related fraud, the article does not offer generally valid solutions, but displays certain situations upon which sooner or later doctrine and case law should reflect. In the first part, introductory aspects of the offence of computer related-fraud in Romanian criminal law are mentioned, and in the second*

[1] Auditor de justiție, anul I (e-mail: cristian.stănescu@inm-lex.ro).

part, two areas in the field of information technology which are of interest due to their specific features are considered.

Keywords: *computer-related fraud, computer system, computer data, Artificial Intelligence, blockchain*

1. Sfera infracțiunii de fraudă informatică

În legislația penală română frauda informatică apare pentru prima dată în art. 49 din Legea nr. 161/2003[2] privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției. Reglementarea infracțiunii a fost impusă de obligația asumată de statul român prin ratificarea la 12 mai 2004 prin Legea nr. 64/2004[3] a Convenției privind Criminalitatea Informatică adoptată la Budapesta la 23 noiembrie 2001, de a adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a incrimina, potrivit dreptului intern, fapta comisă „prin orice introducere, alterare, ștergere sau suprimare a datelor informatice, prin orice formă care aduce atingere funcționării unui sistem informatic, cu intenția frauduloasă sau delictuală de a obține fără drept un beneficiu economic pentru el însuși sau pentru altă persoană."

Incriminarea a fost preluată de noul Cod penal intrat în vigoare la 1 februarie 2014, la art. 249 și are în prezent următoarea configurație: „[i]ntroducerea, transmiterea, modificarea sau ștergerea de date informatice, restricționarea accesului la aceste date ori împiedicarea în orice mod a funcționării unui sistem informatic, în scopul de a obține un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane, se pedepsește cu închisoarea de la 2 la 7 ani.". Ultima modificare adusă textului a fost introducerea unei noi modalități de săvârșire a elementului material, transmiterea, prin Legea nr. 207/2021[4] care prevede măsuri de transpunere a Directivei (UE) 2019/713 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar și de înlocuire a Deciziei-cadru 2001/413/JAI a Consiliului[5].

---

[2] M.Of. nr. 279 din 21 aprilie 2003.

[3] M.Of. nr. 343 din 20 aprilie 2004.

[4] M.Of. nr. 720 din 22 iulie 2021.

[5] JO L 123, 10.5.2019, p. 18-29.

Pentru înțelegerea sferei de incriminare sunt necesare și definițiile conceptelor de sistem informatic și date informatice cuprinse în art. 181 C.pen. Astfel, potrivit art. 181 alin. (1) C.pen., „[p]rin 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".

În doctrină s-a arătat că printre sistemele informatice relevante în sfera infracțiunii de fraudă informatică se pot menționa[6]: bancomatul (ATM), terminalul POS (Point of Sale), casele de marcat de tip *self-scan*, servere ale instituțiilor publice, ale instituțiilor financiare, precum și diverse alte dispozitive care permit achiziții de bunuri și servicii, cum ar fi: automatele de cafea și mâncare (tonomate), automatele de eliberare a cartelelor de călătorie cu mijloacele de transport, de încărcare a cartelelor de telefonie sau plata facturilor de utilități. Jurisprudența în materia infracțiunii de fraudă informatică cunoaște exemple similare, cele mai multe fiind în domeniul aplicațiilor informatice bancare[7].

Dintre elementele ce compun această definiție, merită făcute câteva precizări despre noțiunile de „prelucrare automată a datelor" și „program informatic".

Prima este definită în mod tautologic de Legea nr. 161/2003, unde la art. 35 alin. (1) lit. b) se menționează că „prin *prelucrare* automată a datelor se înțelege procesul prin care datele dintr-un sistem informatic sunt *prelucrate* prin intermediul unui program informatic" (s.n.).

Având în vedere caracterul deficitar al acestei definiții legale, consider că se poate avea în vedere ca reper definiția noțiunii de prelucrare cuprinsă în Regulamentul nr. 679 din 27 aprilie 2016 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 (GDPR)[8], unde art. 4 pct. 2 prevede că prelucrare înseamnă „orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau

---

[6] A se vedea G. Zlati, *Tratat de criminalitate informatică*. Vol. I, Ed. Solomon, 2020, p. 333.

[7] A se vedea C.A. Cluj, secția penală. decizia 6/A/2022, disponibilă pe www.lege5.ro; C.A. Cluj, secția penală, decizia nr. 1245/A/2021, disponibilă pe www.lege5.ro.

[8] JO L 119, 4.5.2016, p. 1-88.

distrugerea". Rezultă că oricare dintre aceste operațiuni va constitui o prelucrare automată atunci când este realizată prin intermediul unui program informatic.

Programul informatic este un ansamblu de instrucțiuni care pot fi executate de un sistem informatic în vederea obținerii unui rezultat determinat, potrivit art. 35 alin. (1) lit. c) din Legea nr. 161/2003. În dreptul penal german se precizează că instrucțiunile trebuie să fie fixate sub formă de date și să privească modul în care trebuie să se desfășoare etapele individuale de prelucrare a datelor informatice[9]. Dreptul penal italian le definește în mod similar ca seturi de instrucțiuni, exprimate într-un limbaj utilizabil de către calculator, conceput și asamblat în scopul de a obține anumite performanțe specifice[10]. Aceste instrucțiuni nu pot fi oferite sistemului informatic în orice modalitate, ci trebuie comunicate într-un anumit limbaj de programare, recunoscut de sistemul informatic[11].

Este important de menționat că fără un astfel de program nu am putea discuta despre o prelucrare automată, pentru că acesta este construit în așa manieră încât să acționeze independent de acțiunea utilizatorului. Acest lucru nu este incompatibil cu situația în care sistemului îi sunt oferite inițial date sau instrucțiuni de către utilizator, pentru că programul va funcționa ulterior fără intervenție umană. De exemplu, o aplicație de *mobile banking* este un program informatic, care a fost creat și care prelucrează datele informatice cu ajutorul unui limbaj de programare numit Swift, de pe un iPhone care reprezintă un sistem informatic.

Articolul 181 alin. (2) C.pen. prevede că „[p]rin date informatice se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic." Tot literatura de specialitate oferă și exemple cu privire la date informatice relevante în sfera infracțiunii de fraudă informatică, respectiv datele de acces pentru contul de internet banking, monedele electronice, baze de date[12] etc.

În dreptul penal german, aceste date sunt văzute ca reprezentări de informație prin semne sau funcții continue, care pot fi codificate ca obiecte sau mijloace de procesare de către un dispozitiv sau care este rezultatul unei operațiuni de prelucrare. Cu privire la obținerea ilegală de date, în Codul penal german cerința

---

[9] A se vedea D. Bock, *Strafrecht Besonderer, Teil 2*, Ed. Spinger-Legrbuch, Berlin, 2018, p. 436.

[10] A se vedea Alberto Cappelinni în A. Cadoppi, S. Canestrari, A. Manna, M. Papa (coord.), *Diritto Penale*, Ed. UTET Giuridica, Milano, 2022, p. 7136.

[11] A se vedea R. Dumitrașcu, „Programele pentru calculator: istorie și definiție", 2017, *Revista română de dreptul proprietății intelectuale*, nr. 2, p. 159.

[12] A se vedea G. Zlati, *Tratat...*, p. 333.

este restrânsă doar la datele care sunt stocate sau transmise pe cale electronică, magnetică sau care nu sunt direct perceptibile în alt mod[13].

Din definiția programului informatic evocată anterior rezultă că acesta intră în categoria datelor informatice. De altfel, se poate considera că programele informatice sunt cele mai importante date informatice. Acest lucru se datorează faptului că prin intermediul programelor informatice se prelucrează în mod automat și celelalte categorii de date informatice. Programul informatic rezolvă o anumită „problemă" prin setul de instrucțiuni care se află la baza acestuia. După scopul spre care tinde rezolvarea acestei probleme, programele informatice pot fi clasificate în licite și malițioase. Acestea din urmă au la bază o utilizare în scop ilicit. Printre exemplele oferite în literatura de specialitate se numără virușii informatici, viermii informatici și programele de tip cal troian[14].

În realitate, majoritatea sistemelor informatice din prezent funcționează printr-o succesiune de prelucrări între programe informatice. Spre exemplu, pentru ca un computer să pornească, sistemul de operare (de exemplu, Windows) al acestuia parcurge un șir de prelucrări, începând de la BIOS[15], pentru ca la rândul lui sistemul de operare să prelucreze programul informatic constând în browser-ul de internet (de exemplu, Google Chrome), în cadrul căruia utilizatorul introduce adresa unei pagini web[16] pentru a accesa, fără drept, contul bancar al victimei prin intermediul aplicației de internet banking, unde se introduc alte date informatice constând în numele și parola de acces a acelui cont, pentru ca în final să fie modificate printr-o altă prelucrare datele informatice constând în soldul contului, printr-un transfer fraudulos în scopul obținerii unui beneficiu material, realizându-se astfel conținutul constitutiv al infracțiunii de fraudă informatică.

Raportând modalitatea de incriminare a fraudei informatice la restul infracțiunilor existente în legislația penală, se poate constata că aceasta se află la intersecția între infracțiunile contra patrimoniului și infracțiunile informatice, în Recomandarea

---

[13] A se vedea D. Bock, *Strafrecht Besonderer, Teil 1,* Ed. Spinger-Legrbuch, Berlin, 2018, p. 292.

[14] A se vedea M. Bulancea, G. Zlati, R. Slăvoiu în M. Udroiu (coord.), *Codul de procedură penală. Comentariu pe articole*, ed. a II-a, Ed. C.H. Beck, București, 2017, p. 641.

[15] Acronim pentru *Basic Input Output System*, un program informatic care este uneori plasat și în sfera sistemului informatic, fiind un firmware. Pentru detalii despre aceste noțiuni, a se vedea G. Zlati, *Tratat...*, p. 65, p. 104.

[16] În doctrină, pagina web este oferită tot ca un exemplu de date informatice. A se vedea G. Zlati, *Tratat...*, p. 102.

nr. R (89) 9 a Consiliului Europei privind infracțiunile informatice[17] arătându-se că infracțiunea vine să suplinească lacuna anterior constatată în ceea ce privește infracțiunile de tipul înșelăciunii, respectiv cerința impusă de legislațiile statelor cu privire la conduita de inducere în eroarea a unei persoane, iar în ceea ce privește infracțiunile de tipul furtului sau delapidării, cerința existenței unui obiect material corporal. Mai mult, diferența între frauda informatică și înșelăciune a generat multă vreme o practică judiciară neunitară, care a fost în cele din urmă înlăturată, după cum voi arăta *infra.*

2. Relevanța infracțiunii de fraudă informatică în contextul noilor tehnologii

Odată cu apariția unor noi sisteme, concepte sau soluții în domeniul informaticii, modalitățile de comitere a infracțiunii de fraudă informatică s-au diversificat, existând unele situații în care reținerea acestei infracțiuni poate genera probleme. Dintre aceste exemple merită analizate domeniul Inteligenței Artificiale, respectiv domeniul tehnologiei *blockchain* și criptoactivele.

2.1. Inteligența Artificială

În ceea ce privește domeniul Inteligenței Artificiale, trebuie menționat încă de la început că această tehnologie aparține componentei *software*[18], deși are o sursă de inspirație materială, respectiv modul de funcționare al rețelelor neuronale ale creierului uman. Așadar, discuția se plasează în sfera conceptului de date informatice[19]. De pildă, în literatura de specialitate s-a analizat cazul în care sunt create portrete artificiale ale unor persoane care nu există în realitate utilizând această tehnologie, statuându-se că imaginile constând în fotografii tip portret, oferite inițial sistemului pentru prelucrare, constituie date informatice[20]. Fără îndoială, algoritmul de tip rețea neurală adversarială[21] utilizat în acest caz este un

---

[17] Disponibilă la http://www.oas.org/juridico/english/89-9&final%20report.pdf.

[18] A se vedea C. T. Stănescu, „Crearea de portrete fictive utilizând rețele neurale adversariale. Relația cu infracțiunile de fals*",* 2021*, AUBD – Forum Juridic,* nr. 3, p. 2.

[19] În sensul că Inteligența Artificială este un sistem informatic, a se vedea G.-M. Husti, „Acțiunea, inacțiunea și legătura de cauzalitate în cazul inteligenței artificiale*"*, 2021, *Revista Themis* nr. 1-2, p. 45.

[20] A se vedea G. Zlati, *Tratat...,* p. 102., C.T. Stănescu, *op. cit.*, p. 4.

[21] Pentru modalitatea în care funcționează acest tip de rețea, a se vedea A. Matthias, *Neural Networks without the Math, Joyful AI, Book 1*, Joyously Aware Media, 2018; I. Goodfellow et. alii*, Generative Adversarial Networks*, Proceedings of the International Conference on Neural Information Processing Systems (NIPS 2014), p. 2672–2680; C.T. Stănescu, *op. cit.*, p. 2.

ansamblu de instrucțiuni care pot fi executate de un sistem informatic în vederea obținerii unui rezultat determinat, ca atare putem vorbi de un veritabil program informatic.

Esența acestei tehnologii se regăsește în modalitatea de rulare a programelor informatice: spre exemplificare, cu ajutorul Inteligenței Artificiale, un telefon mobil poate clasifica fotografiile efectuate după ceea ce este surprins în acestea, fără a primi vreo instrucțiune din partea utilizatorului. Tot astfel, pot fi create materiale sau medicamente prin perfecționarea structurii moleculare, identificate structuri de celule cu potențial cancerigen, defecte în procesul de fabricație al materialelor[22] etc.

În sfera infracțiunii de fraudă informatică, Inteligența Artificială este folosită cu precădere în scop preventiv. Până la introducerea acestor sisteme, instituțiile financiare realizau măsurile de prevenție utilizând un set de reguli definite pe baza istoricului de tranzacționare frauduloasă, pentru ca ulterior sistemul să emită o avertizare în caz că o tranzacție respectă aceste reguli și apare astfel ca fiind o formă de fraudă. Dezavantajul acestui tip de mecanism este lipsa flexibilității, caracterul cronofag și faptul că funcționează în mod reactiv. De exemplu, am putea constata pe baza experienței anterioare că atunci când dintr-un cont bancar se efectuează un tip de tranzacție către un anumit alt cont bancar, această tranzacție este frauduloasă pentru ca cel de-al doilea cont bancar a apărut în mai multe cazuri de fraudă de-a lungul timpului. Tot astfel, am putea identifica un tipar în conduita unui autor al infracțiunii de fraudă pentru că de fiecare dată își transferă o sumă foarte mică de bani în contul propriu, cu ajutorul unui program informatic malițios care „rotunjește" tranzacțiile efectuate. Dificultatea apare atunci când autorul evadează din acest tipar și își schimbă modul de operare. Arătam anterior că un program informatic soluționează o problemă determinată cu ajutorul setului de instrucțiuni. Atunci când problema ce trebuie soluționată variază în timp sau își schimbă parametrii în funcție de circumstanțele date, programul inițial se dovedește insuficient. În întâmpinarea acestor neajunsuri pot fi utilizate soluțiile cu Inteligență Artificială[23].

---

[22] A se vedea Malik, E.F. Khaw, K.W. Belaton, B.; Wong, W.P., Chew, X., *Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture*. Mathematics 2022, 10, 1480, disponibil la https://doi.org/10.3390/math10091480 și exemplele citate acolo.

[23] A se vedea E. Alpaydın*, Introduction to Machine Learning*, 2nd ed.; The MIT Press: Cambridge, MA, USA, 2014, p. 2.

Într-o definiție foarte simplă, în cazul Inteligenței Artificiale are loc un proces de învățare, fără ca un sistem informatic să fie programat în acest sens[24]. Necesitatea procesului de învățare mai apare și în acele cazuri în care nu se poate folosi în mod direct un program informatic pentru rezolvarea unei probleme, astfel că se apelează la un set de date exemplificative care să constituie un punct de plecare. În literatura de specialitate[25] s-a oferit drept exemplu situația în care o persoană transcrie ceea ce comunică verbal o alta. Recunoașterea cuvintelor pentru scrierea lor ulterioară este un proces mental ce nu poate fi explicat sub forma unor instrucțiuni dintr-un program informatic. Mai mult, chiar dacă am admite posibilitatea creării unui astfel de mecanism, el ar funcționa doar pentru recunoașterea vocii unei singure persoane, prin schimbarea vorbitorului, accentului acestuia, sistemul devenind ineficient. Acest lucru nu este valabil și în cazul unei persoane, care poate transcrie vocea unei persoane pe care o înțelege indiferent de accent sau tonalitate. Un exemplu similar poate fi construit și în sfera infracțiunilor de fraudă informatică. Analiza făcută de un membru al echipei de audit al unei instituții bancare ar putea releva o potențială fraudă, însă procesul de gândire, comparație și probabil chiar intuiție bazată pe experiența anterioară nu ar putea fi niciodată transpusă într-un program informatic, pentru că implică prea mulți parametri variabili. Tot astfel, analiza manuală umană necesită la rândul ei o perioadă substanțială de timp, odată cu costuri aferente ridicate. Aceste neajunsuri pot fi combătute prin antrenarea sau învățarea unui program cu Inteligență Artificială ca pe baza unei cantități mari de date reprezentate de vocile multor persoane, respectiv tranzacții efectuate, să recunoască datele relevante pentru demersul în legătură cu care a fost programat.

Cu toate acestea, programele informatice ce funcționează pe baza Inteligenței Artificiale prezintă neajunsuri în activitatea de prevenție a fraudei, neajunsuri ce pot facilita comiterea infracțiunii de fraudă informatică.

Un prim dezavantaj este dezechilibrul datelor. Am văzut că programele cu Inteligență Artificială învață după un anumit set de date. Ceea ce este esențial în acest proces de învățare este capacitatea acestora de a generaliza, adică de a recunoaște date care, deși nu sunt similare celor oferite inițial, au caracteristici

---

[24] Pentru detalii și alte definiții mai cuprinzătoare, a se vedea Recomandarea OCDE privind Inteligența Artificială, disponibilă la https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm.; Propunerea de Regulament a Parlamentului și Consiliului privind Inteligența Artificială, disponibilă la https://ec.europa.eu/; L.M. Stănilă, *Inteligența artificială, dreptul penal și sistemul de justiție penală. Amintiri despre viitor*. Ed. Universul Juridic, București, 2020, p. 36, C.T. Stănescu, *op. cit.*, p. 2.

[25] A se vedea E. Alpaydın, *op. cit.*, prefață.

generale asemănătoare. S-a arătat în literatura de specialitate[26] că în cazul în care datele oferite pentru a învăța sunt insuficiente ca număr, programul informatic nu va mai fi capabil să generalizeze, ci va memora aceste date, similar unui program informatic care nu prezintă Inteligență Artificială. Este și cazul tranzacțiilor frauduloase, care sunt prezente într-un număr substanțial mai redus față de cele licite[27]. Prin instalarea unui program informatic malițios care citește toate cazurile de fraudă memorate, autorul ar putea crea o nouă modalitate de tranzacție diferită, comițând astfel infracțiunea de fraudă fără a fi detectată de sistem. Printre soluțiile care pot fi gândite pentru îmbunătățirea acestui sistem ar fi diminuarea datelor cu tranzacții licite și creșterea, chiar artificială, a cazurilor de fraudă pentru îmbunătățirea procesului de detecție. Însă, autorul ar putea introduce în mod ilicit un set de date care ar perturba algoritmul cu Inteligență Artificială, astfel că, riscul infracțional nu este înlăturat prin utilizarea Inteligenței Artificiale.

Exemplele de mai sus vin în susținerea ideii că, în prezent, există o intersecție între infracțiunea de fraudă informatică și Inteligența Artificială, având în vedere că aceste rețele neurale sunt programe informatice care prelucrează în mod automat date informatice în cadrul unor sisteme informatice. O perspectivă problematică există în legătură cu evoluția sistemelor cu Inteligență Artificială. Această tehnologie a reușit să „transforme" entități pe care anterior le vedeam în mod sceptic ca fiind sisteme informatice, cum ar fi vehiculele. Fără doar și poate, Vehiculele Autonome sunt veritabile sisteme informatice, care pot comite chiar infracțiuni[28]. Spre deosebire de sistemele informatice tradiționale, care sunt simple unelte în mâna unui utilizator, sistemele ce funcționează pe bază de Inteligență Artificială încep treptat să își piardă acest caracter.

Luând exemplul robotului umanoid Sofia[29], care a devenit cetățean al Arabiei Saudite în 2017, distincția între infracțiunea de fraudă informatică și înșelăciune comisă în dauna acesteia devine problematică. Într-o decizie privind dezlegarea

---

[26] A se vedea A. Matthias, *op. cit.*, p. 49.

[27] A se vedea A. D. Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, IEEE Trans. *Neural Netw. Learn. Syst*., vol. 29, no. 8/2017, p. 3784.; A. A. Taha, S. J. Malebary, *Intelligent Approach to Credit Card Fraud Detection Using an OLightGBM*, IEEE Access 2020, 8, p. 25579; Malik, E.F. Khaw, K.W. Belaton, B.; Wong, W.P., Chew, X, *op.cit.*, p. 2.

[28] A se vedea Forbes, https://www.forbes.com/sites/meriameberboucha/2018/05/28/uber-self-driving-car-crash-what-really-happened/?sh=2cff24264dc4, accesat ultima dată la 09.08.2022.

[29] A se vedea Jesús Retto, *Sophia, First Citizen Robot of the World*, 2017, http://bitly.ws/xQvB, accesat ultima oară la 09.08.2022.

unor chestiuni de drept în materie penală[30], Înalta Curte de Casație și Justiție a reținut că „[d]iferența dintre infracțiunea de înșelăciune și infracțiunea de fraudă informatică decurge din faptul că, în timp ce frauda informatică se săvârșește asupra unui sistem informatic, înșelăciunea săvârșită [....] prin plasarea unor anunțuri fictive care a avut drept consecință producerea unei pagube, are loc prin intermediul unui sistem informatic în care sunt introduse date informatice (anunțul fictiv), rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice, respectiv creării unui prejudiciu subiectului care acceptă oferta fictivă. În cazul infracțiunii de fraudă informatică, prejudiciul se produce ca o consecință directă a introducerii datelor informatice, iar în cazul infracțiunii de înșelăciune, prejudiciul se produce prin determinarea persoanei vătămate să adopte o conduită păgubitoare". Prin aceeași decizie s-a reținut de asemenea că „în timp ce frauda informatică se săvârșește asupra unui sistem informatic, a cărui structură este modificată, înșelăciunea prin plasarea unor anunțuri fictive care a avut drept consecință producerea unei pagube are loc prin intermediul unui sistem informatic, a cărui structură este folosită de subiectul activ al infracțiunii". Așadar, distincția între infracțiunea de înșelăciune (art. 244 C.pen.) și infracțiunea de fraudă informatică (art. 249 C.pen.) se face după criteriul „subiectului" indus în eroare: dacă inducerea în eroare operează față de o persoană vorbim despre infracțiunea de înșelăciune, în schimb dacă se acționează asupra sistemului informatic, e incidentă infracțiunea de fraudă informatică, aspect confirmat și de literatura de specialitate[31]. Dacă în acest moment, putem formula cu certitudine concluzia că inducerea în eroare a acestui robot în scopul obținerii unui beneficiu material constituie infracțiunea de fraudă informatică, pe măsură ce astfel de sisteme cu Inteligență Artificială dobândesc un caracter din ce în ce mai autonom față de un programator sau utilizator, încadrarea juridică nu va mai fi atât de ușor de efectuat. Asta pentru că, în cele din urmă, odată cu trecerea de la Inteligența Artificială specializată la cea generală, aceasta din urmă având conștiință proprie și un comportament similar omului, se pune problema în ce măsură mai constituie ea un sistem sau program informatic. Consider că vor exista reticențe în a reține infracțiunea de înșelăciune în acest caz, având în vedere că o astfel de entitate ar îndeplini în continuare condițiile prevăzute de lege pentru a fi inclus în categoria sistemelor informatice care datelor informatice, însă soluția poate depinde în egală măsură de acceptarea conceptului de „personalitate juridică" în materia Inteligenței Artificiale, pentru că doar în acest caz determinarea

---

[30] A se vedea ICCJ, Completul privind dezlegarea unor chestiuni de drept în materie penală, Decizia nr. 37/2021 publicată în M.Of. nr. 707 din 16 iulie 2021.

[31] A se vedea în acest sens G. Zlati, *Tratat...*, p. 454 și urm.; Recomandarea nr. R (89) 9 a Consiliului Europei privind infracțiunile informatice, *cit. supra.*, p. 37.

persoanei vătămate să adopte o conduită păgubitoare ar putea fi analizată în sfera infracțiunii de înșelăciune

2.2. Tehnologia blockchain și criptoactivele

Tehnologia blockchain cuprinde prin complexitatea sa atât componente *hardware*, cât și *software*. Această tehnologie are la bază un registru descentralizat, în care tranzacțiile înregistrate pot fi accesate și verificate de către oricare dintre sisteme informatice care participă la rețea. Cu toate acestea, trebuie precizat că rețea formată din mai multe sisteme informatice nu devine prin asociere un sistem informatic distinct. Așadar, în cazul tehnologiei blockchain nu putem vorbi despre un sistem informatic distinct, ci tehnologia este pusă în comun de toate sistemele informatice participante. Blocurile care alcătuiesc registrul sunt însă, fără îndoială, date informatice, fiind un șir unic de caractere într-o formă ce permite prelucrarea prin intermediul proceselor de minare și tranzacționare de sistemele informatice din rețea, utilizându-se programe informatice specifice[32]. Monedele virtuale au fost calificate în literatura de specialitate ca fiind o aplicație care rulează în sistemul blockchain, adică având natura unor programe informatice și, implicit, a unor date informatice[33].

Atacul de 51%[34] este o conduită infracțională ce constă într-un atac asupra sistemului blockchain de către „minerii[35]" ce dețin peste 50% din puterea computațională a sistemelor informatice (*hashrate*)[36]. În condiții normale, minerii se află în competiție pentru a soluționa problema matematică și de a descoperi[37] un nou bloc, iar de îndată ce este descoperită combinația corectă[38], blocul cel nou este adăugat în registrul blockchain. Consecința efectuării atacului este

---

[32] Spre exemplificare, minarea (crearea de noi monede virtuale) se realizează prin programe informatice cum ar fi CGMiner, MultiMiner etc. A se vedea pentru detalii Investopedia, https://www.investopedia.com/best-bitcoin-mining-software-5095403, accesat ultima oară la 10.08.2022.

[33] A se vedea G. Zlati, *Tehnologia blockchain...*, p. 21.

[34] A se vedea L. Phan, S. Li, K. Mentzer, „Blockchain and the current discussion on fraud*",* 2019, *Issues in Information Systems Volume 20*, Issue 4, p. 11.

[35] Acest termen poate desemna atât sistemele informatice utilizate în procesul de minare, dar și utilizatorul acestui sistem.

[36] A se vedea G. Zlati*, Tehnologia blockchain...,* p. 30.

[37] Prin această precizare se înțelege mai facil de unde vine denumirea de minare a activității, fiind similară cu activitatea desfășurată într-o mină de cărbune, spre exemplu.

[38] Combinația este considerată ca fiind corectă prin intermediul mecanismului de consens, despre care am amintit *infra*.

posibilitatea de blocare a noilor tranzacții efectuate, astfel că ceilalți mineri din rețea se află în imposibilitate de a-și primi recompensa. Tot astfel, tranzacțiile deja efectuate se pot modifica prin alterarea blocurilor, căpătând astfel un caracter reversibil și readucând în discuție problema tranzacționării multiple, care se dorea a fi depășită prin tehnologia *blockchain*. În concluzie, în această ipoteză s-ar putea reține frauda informatică prin restricționarea accesului la date informatice, respectiv prin modificarea acestora. În cazul criptomonedelor cu putere computațională mare cum ar fi Bitcoin sau Ethereum, riscul unui asemenea atac este redus substanțial, datorită costurilor foarte ridicate pe care le presupune achiziția a peste 50% din puterea computațională[39].

Minarea egoistă (*selfish mining*[40]) este situația în care un miner efectuează operațiunile de rezolvare a problemelor în mod ascuns, distinct de registrul principal. Spre deosebire de cea anterioară această modalitate necesită doar 25% din puterea computațională[41]. Se creează prin bifurcare un *blockchain* privat, paralel față de cel public și pe care intenționează să îl unească, la momentul potrivit, cu cel principal, în scopul validării anticipate a tranzacțiilor și obținerii unui beneficiu material pe nedrept. Aceasta are loc în momentul în care *blockchain*-ul privat devine cu un singur bloc mai mare decât cel public, astfel că prin publicarea acestuia are loc o veritabilă inducere în eroare a celorlalți „mineri", care vor considera că acesta este *blockchain*-ul principal, iar prin validarea acestuia, minerul „egoist" obține recompensa[42]. Apreciez că această conduită întrunește elementele constitutive ale infracțiunii de fraudă informatică în modalitatea introducerii datelor informatice.

Criptoactivele au fost definite în literatura de specialitate ca fiind „o reprezentare digitală a valorii sau a drepturilor care pot fi transferate și stocate electronic, utilizând tehnologia registrelor distribuite sau o tehnologia similară."[43]. Cele mai

---

[39] A se vedea Investopedia, https://www.investopedia.com/terms/1/51-attack.asp, accesat ultima dată la 10.12.2022.

[40] A se vedea L. Phan, S. Li, K. Mentzer, *op.cit.*, p. 11.

[41] *Ibidem.*

[42] A se vedea I. Eyal, E.G. Sirer*, Majority is not Enough: Bitcoin Mining is Vulnerable*, Cornell Bowers Computer Science, 2013, p. 436-454

[43] A se vedea A.-R. Trandafir, G. Zlati, *op. cit.*, p. 60. Definiția este preluată din art. 3 alin. (2) din Propunerea de Regulament privind piețele criptoactivelor și de modificare a Directivei (UE) 2019/1937 (propunerea de regulament MiCA), despre care autorii arată că este, în prezent, într-un continuu proces de modificare. De altfel, în această propunere nu se face trimitere la noțiunea de „monedă virtuală, fiind utilizată doar noțiunea de „cripto-activ". A se vedea și G. Zlati, *Tehnologia blockchain...*, p. 23.

importante criptoactive sunt monedele virtuale și NFT-urile (acronim pentru *non-fungible token*). În strânsă legătură cu aceste concepte se află și contractele inteligente (*smart contracts*), care rulează tot în sistemul *blockchain*. Acestea sunt calificate în mod expres de literatura de specialitate ca subsumându-se categoriei programelor informatice, fiind un ansamblu de instrucțiuni care rulează în mod automat un set de reguli, odată ce condițiile definite sunt îndeplinite executând, practic, contractul[44].

Pe baza contractelor inteligente pot funcționa Organizații Autonome Descentralizate (OAD), care ar putea fi considerate corespondentul societăților pe acțiuni în domeniul blockchain. Organizația funcționează prin intermediul criptomonedei Ether, prin achiziționarea acesteia utilizatorii dobândind *„tokens"* – un corespondent al părților sociale. Acestea permit votarea propunerilor de investiții și oportunitatea încasării unor recompense provenind de la rezultatul activității contractorilor – similar dividendelor. Principala diferență între o societate clasică este lipsa necesității condiției de încredere între membrii acesteia, alături de caracterul automat care permite lipsa unor poziții de administrare sau conducere, în sensul obișnuit al funcționării societății. Dincolo de viziunea optimistă care prin caracterul preponderent automat pare să excludă anumite conduite infracționale din sfera nesocotirii încrederii, pericolul săvârșirii de infracțiuni informatice încă subzistă.

De exemplu, printr-un atac asupra sistemului, s-a reușit producerea unei pagube de 60 de milioane de dolari în forma monedelor virtuale[45]. Prin cereri repetate de transfer către o clonă a sistemului, autorii au reușit să exploateze o eroare care nu înregistra la timp transferul de fonduri săvârșind astfel infracțiunea de fraudă informatică prin transmiterea de date informatice[46].

CONCLUZIE

Ipotezele prezentate constituie doar un punct de plecare al evoluției modalităților de comitere a infracțiunii de fraudă informatică. Inteligența Artificială este un

---

[44] *Ibidem*, p. 45; M. Lacity, „Crypto and Blockchain fundamentals", 2020, *Arkansas Law Review*, vol. 73, p. 366.

[45] A se vedea Planet Compliance, https://www.planetcompliance.com/nutshell-dao-steal-60-million-worth-cryptocurrency/, accesat ultima oară la 14.12.2022.

[46] A se vedea L. Phan, S. Li, K. Mentzer, *op.cit*., p. 11; G. Zlati, *Tehnologia blockchain...,* p. 46. Acest din urmă autor analizează exploatarea vulnerabilităților acestui sistem atât în contextul infracțiunii de fraudă informatică, dar și a celei de efectuare de operațiuni financiare în mod fraudulos.

domeniu ce are în prezent relevanță predominant în latura preventivă a dreptului penal, dar acesta trebuie studiat și în contextul dezvoltării modalităților de comitere a infracțiunii de fraudă informatică. Tehnologia *blockchain* este relevantă în sfera infracțiunii de fraudă informatică pentru că, deși caracterul descentralizat îi sporește siguranța, nu este o soluție lipsită în totalitate de vulnerabilități. Revine doctrinei și jurisprudenței sarcina de a se adapta la această evoluție și de a găsi soluții eficiente în vederea soluționării cauzelor având ca obiect sfera criminalității informatice în general, respectiv infracțiunea de fraudă informatică în special.