LIBRIS | We know books

CAIETE DE DREPT PENAL

Criminal Law Writings

Publicație trimestrială

Nr. 3/2025

LIBRIS | We know books

Cuprins

Abrevieri 7

I. DOCTRINĂ

George Zlati, Înșelăciunea comisă prin tehnologia informației și comunicațiilor 9
Ana Maria Cara Drăgănescu, Munca neremunerată în folosul comunității. Impedimente în executare din perspectiva reglementărilor în vigoare și a jurisprudenței recente 29

II. CONFERINȚA NAȚIONALĂ A DOCTORANZILOR ÎN DREPT PENAL ȘI PROCEDURĂ PENALĂ (II)

Mihai Popa, Compatibilitatea prezumțiilor de culpabilitate cu protecția dreptului la un proces echitabil. Implicații în plan probatoriu 54
Adrian-Florin Coșa, Incongruențe între cauțiunea aplicabilă persoanei juridice și cauțiunea aplicabilă persoanei fizice – perspectiva națională, europeană, nord-americană 78
Gabriela Ola, *Nulla poena sine lege* – influența „dreptului contravențional" unional asupra principiului legalității sancțiunii penale 95
Ionuț-Daniel Vîlceanu, Interpretarea și (re)definirea infracțiunii de acțiuni împotriva ordinii constituționale. Spre un model francez? 119

III. JURISPRUDENȚĂ

Radu Slăvoiu, Mihail Udroiu, Spălarea banilor. Lipsa tipicității obiective. Notă critică la sentința definitivă nr. 35/F/2025 a Curții de Apel București, secția a II-a penală 145
Cristian-Valentin Ștefan, Omor calificat. Elementele circumstanțiale agravante referitoare la săvârșirea infracțiunii cu premeditare (I) și prin cruzimi (II) 152

LIBRIS | We know books

Înșelăciunea comisă prin tehnologia informației și comunicațiilor

DOI:10.24193/CDP.2025.3.1

Lect. univ. dr. ***George ZLATI****
Facultatea de Drept și Științe Sociale,
Universitatea „1 Decembrie 1989" din Alba Iulia
Avocat, Baroul Cluj

Fraud committed by means of information and communications technology

❑ *ABSTRACT*

The offence of fraud committed by means of information and communications technology represents one of the most prevalent forms of cyber-enabled crime worldwide. Unlike cyber-dependent offences, where information systems or data are the direct target, this form of fraud involves the use of technology as an instrument to facilitate deceit.

The article highlights the exponential growth of online investment fraud and other technology-enabled scams, such as Business Email Compromise (BEC), deepfake-enabled impersonation, and identity theft. Special attention is given to the role of crypto-assets as either the object or the proceeds of fraudulent conduct. In this regard, particular emphasis is placed on fraudulent schemes such as investment frauds, pump-and-dump operations, wash trading, and the use of counterfeit tokens or test tokens (faucets).

The article argues that the current legal framework under Romanian law is largely sufficient to address fraud committed through information technology, primarily by applying the aggravated form of fraud under Article 244 par. (2) of the Criminal Code. However, it suggests that de lege ferenda discussions should focus on harmonising sanctioning regimes, particularly with respect to the overlap between fraud and computer-related fraud, and on addressing legislative gaps concerning market abuse in the crypto-asset market. Ultimately, the article underscores the importance of a nuanced doctrinal and jurisprudential approach, as the technological sophistication of perpetrators continues to evolve at a rapid pace.

* zlati.george@uab.ro.

LIBRIS | We know books

❑ ***Keywords:*** *cybercrime, fraud, information and communications technology, cyber-enabled crime, crypto-assets, investment fraud, market manipulation, social engineering.*

I. Aspecte introductive și delimitări conceptuale

1. Prevalența înșelăciunilor comise prin tehnologia informației și comunicațiilor

Înșelăciunea comisă prin tehnologia informației și comunicațiilor[1] (în continuare, *înșelăciunea comisă prin mijloace informatice*) reprezintă una dintre principalele infracțiuni la nivel global în care datele și sistemele informatice constituie instrumente pentru înlesnirea săvârșirii infracțiunii (în eng., *cyber-enabled offence*), și nu ținta acesteia (în eng., *cyber-dependent offence*)[2].

Sintagma „comisă prin tehnologia informației și comunicațiilor" provine din art. 13 lit. c) din Convenția Națiunilor Unite împotriva criminalității informatice (adoptată prin consens în anul 2024), conform căreia statele semnatare au obligația pozitivă de a incrimina *orice inducere în eroare cu privire la împrejurări de fapt, realizată prin intermediul unui sistem de tehnologie a informației și comunicațiilor, care determină o persoană să facă sau să nu facă un act pe care, în lipsa acestei induceri în eroare, nu l-ar fi făcut sau nu l-ar fi omis, cu intenția frauduloasă sau cu rea-credință de a obține, pentru sine ori pentru altă persoană, fără drept, un folos material sau alt bun.* Această abordare este discutabilă în primul rând prin prisma faptului că într-o Convenție privind criminalitatea informatică sunt inserate prevederi referitoare la infracțiuni comise prin mijloace informatice, fără ca acestea să intre în sfera conceptului de criminalitate informatică în sens restrâns[3].

Conduita avută în vedere nu se referă la frauda informatică, reglementată distinct la art. 13 lit. a)-b) din Convenție. În ceea ce ne privește, art. 244 C. pen.

---

[1] Denumită inclusiv „înșelăciune online" sau „fraudă în mediul online" (în eng., *online fraud* sau *online scam*).

[2] J.-J. Oerlmans, A. de Hingh, W. van der Wagen, *Types of cyber-enabled crime and their criminalisation*, în W. van der Wagen, J.-J. Oerlmans, M. Weulen Kranenbarg (coord.), *Essentials in cybercrime. A criminological overview for education and practice*, 2nd ed., Eleven International Publishing, 2024, p. 115; A. Bhupendra, T. Holz, *An Explorative Study of Pig Butchering Scams*, *arXiv preprint arXiv:2412.15423*, 2024, p. 1-2, disponibil pe *https://arxiv.org/pdf/2412.15423*, accesat la 14 august 2025; M.-G. Maras, E.R. Ives, *Deconstructing a form of hybrid investment fraud: Examining 'pig butchering' in the United States*, în Journal of Economic Criminology, vol. 5, 2024, p. 3; S.L. Burton, P.D. Moore, *Pig Butchering in Cybersecurity: A Modern Social Engineering Threat*, în SocioEconomic Challenges, vol. 8, nr. 3/2024, p. 47. Pentru o analiză generală a evoluției fenomenului criminalității informatice în România, a se vedea G.-I. Ioniță, *Particularități ale evoluției fenomenului criminalității informatice în România*, în Curierul Judiciar nr. 11/2021, p. 631 și urm. De asemenea, pentru o analiză criminologică a infracțiunii de înșelăciune, a se vedea M.C. Dobrilă, *Analiză criminologică a infracțiunii de înșelăciune*, în Analele Științifice ale Universității „Alexandru Ioan Cuza" din Iași, seria Științe Juridice, nr. 1/2011, p. 49-64.

[3] Pentru definirea acestui concept, a se vedea: S. Gordon, R. Ford, *On the definition and classification of cybercrime*, în Journal of Computer Virology nr. 2/2006; P. Kleve, R. de Mulder, K. van Noortwijk, *The definition of ICT Crime*, în Computer Law & Security Review, vol. 27, 2011, p. 162.

acoperă deja această conduită, nefiind necesară o intervenție viitoare a legiuitorului. Totuși, ar putea fi supus dezbaterii în ce măsură s-ar impune introducerea unei agravante cu acest conținut. Cu toate acestea, apreciem că o astfel de înșelăciune se comite de cele mai multe ori prin mijloace frauduloase (e-mail sau *caller ID spoofing*, *deepfake*, furt de identitate etc.), fiind, așadar, aplicabilă varianta agravată prevăzută de art. 244 alin. (2) C. pen. Ca propunere *de lege ferenda*, considerăm necesară doar modificarea limitelor de pedeapsă pentru a nu exista o diferență la nivelul regimului sancționator între art. 244 alin. (2) C. pen. și art. 249 C. pen.

Potrivit *FBI Internet Crime Report 2023*, fraudele investiționale online au generat în Statele Unite pierderi de aproximativ 3,31 miliarde USD în 2022, crescând la 4,57 miliarde USD în 2023 – o majorare de 38% într-un singur an[4]. Conform *FBI Internet Crime Report 2024*, această tendință ascendentă s-a menținut inclusiv în 2024, valoarea totală a pierderilor raportate în SUA din fraude comise prin mijloace informatice depășind 16 miliarde USD, dintre care peste 6,5 miliarde USD au reprezentat exclusiv prejudiciul cauzat prin fraude investiționale implicând criptoactive[5].

La nivel european și internațional, *EUROPOL Internet Organised Crime Threat Assessment (IOCTA) 2023* (actualizat în 2024)[6] și *INTERPOL Global Financial Fraud Assessment* (martie 2024)[7] evidențiază amenințarea majoră reprezentată de fraudele investiționale, escrocheriile romantice, fraudele de tip *Business Email Compromise* (BEC) sau *CEO fraud* etc. Raportul *Chainalysis Crypto Crime Trends 2024* estimează produsul infracțional rezultat din înșelăciunile cu criptoactive la cel puțin 9,9 miliarde USD în 2023, cu mențiunea că valoarea reală ar putea depăși 12 miliarde USD, odată ce toate adresele ilicite vor fi identificate[8].

Pe plan național, *Raportul de activitate al DIICOT pe anul 2024*[9] confirmă existența unor tendințe similare, indicând o creștere a numărului de cauze având ca obiect fraude de tip *Business Email Compromise*, *CEO fraud* și fraude investiționale cu criptoactive[10].

---

[4] Federal Bureau of Investigation, *Internet Crime Report 2023*, Internet Crime Complaint Center, U.S. Department of Justice, 2024, disponibil pe *www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf*, accesat la 13 august 2025.

[5] Federal Bureau of Investigation, *Internet Crime Report 2024*, Internet Crime Complaint Center, U.S. Department of Justice, 2025, disponibil pe *www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf*, accesat la data de 13 august 2025.

[6] Europol, *Online fraud schemes: a web of deceit (IOCTA 2023)*, European Union Agency for Law Enforcement Cooperation, 21 noiembrie 2024, disponibil pe *www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf*, accesat la 13 august 2025.

[7] Interpol, *Global Financial Fraud Assessment*, martie 2024, disponibil pe *www.interpol.int/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology*, accesat la 13 august 2025.

[8] Chainalysis, *The 2024 Crypto Crime Report*, februarie 2024, disponibil pe *https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf?pubDate=20250820*, accesat la 13 august 2025.

[9] DIICOT, *Raport de activitate 2024*, februarie 2025, București, disponibil pe *https://www.diicot.ro/images/documents/rapoarte_activitate/raport2024.pdf*, accesat la 13 august 2025.

[10] Observăm faptul că se folosește noțiunea de „criptomonedă" (în eng., *cryptocurrency*), deși aceasta nu se regăsește în legislația din România ori în Regulamentul MiCA.

LIBRIS | We know books

Înșelăciunea comisă prin mijloace informatice nu este nimic altceva decât o înșelăciune tradițională (art. 244 C. pen.) ce folosește tehnologia pentru înlesnirea conduitei infracționale[11]. Această infracțiune poate intra într-un raport mijloc-scop cu alte infracțiuni, inclusiv din sfera criminalității informatice în sens restrâns. Astfel, făptuitorii pot utiliza tehnologia *deepfake* pentru uzurparea identității unei persoane publice[12], exploatând notorietatea acesteia în promovarea unor scheme frauduloase. De asemenea, simularea poștei electronice (în eng., *email spoofing*) ori a numărului de telefon (în eng., *caller ID spoofing*), împreună cu contrafacerea de facturi electronice, reprezintă un mod de operare frecvent întâlnit în fraude investiționale ori în scheme de inginerii sociale precum *business email compromise*. În aceste cazuri, înșelăciunea se va reține într-un concurs de infracțiuni cu conexitate etiologică[13] cu falsul informatic (art. 325 C. pen.[14]).

În ultimii ani au fost identificate inclusiv cazuri de uzurpare a conturilor de WhatsApp prin atacuri de tip *SIM swapping*[15], scopul conduitei infracționale fiind acela de a utiliza identitatea victimei în vederea inducerii în eroare a persoanelor apropiate. În asemenea situații, infracțiunile mijloc care înlesnesc înșelăciunea comisă prin mijloace informatice sunt accesul ilegal la un sistem informatic (art. 360 C. pen.)[16] și alterarea integrității datelor informatice, în modalitatea restricționării accesului la datele informatice (art. 362 C. pen.)[17].

În acest context, prezintă relevanță inclusiv decizia nr. 4/2021 a Înaltei Curți de Casație și Justiție referitoare la crearea de conturi false pe rețelele de

---

[11] A se vedea și M.-G. Maras, E.R. Ives, *op. cit.*, p. 2. De altfel, ICCJ, Completul pentru dezlegarea unor chestiuni de drept, prin decizia nr. 37/2021, publicată în M. Of. nr. 707 din 16 iulie 2021, a tranșat tocmai acest aspect.

[12] Pentru analiza relației dintre folosirea tehnologiei *deepfake* și infracțiunile de înșelăciune și fals informatice, a se vedea N.C. Bularda, *Manipularea conținutului prin tehnologia deepfake. Răspunderea penală și relația cu infracțiunile de fals informatic, violarea vieții private și înșelăciune*, în Penalmente Relevant nr. 1/2023, p. 68-76.

[13] Pentru analiza acestei forme a concursului real caracterizat, a se vedea F. Streteanu, D. Nițu, *Drept penal. Partea generală*, vol. II, Ed. Universul Juridic, București, 2018, p. 110-112.

[14] Pentru analiza posibilității reținerii infracțiunii de fals informatic în cazul simulării poștei electronice și a numărului de telefon sau al contrafacerii de facturi electronice, a se vedea G. Zlati, *Tratat de criminalitate informatică*, vol. I, Ed. Solomon, București, 2020, p. 523-526, 551-552 și 583-584.

[15] Despre acestea se face vorbire inclusiv în Raportul de activitate al DIICOT pe anul 2024. Observăm însă că în conținutul raportului se face confuzie între atacul *SIM swapping* și *SIM cloning*, între acestea existând o diferență majoră sub aspectul modului de operare: *SIM swapping* presupune transferul fraudulos al numărului de telefon al victimei pe un SIM controlat de făptuitor, de regulă prin inginerie socială asupra operatorului de telefonie, în timp ce *SIM cloning* constă în copierea conținutului tehnic al cartelei SIM (inclusiv a cheilor de autentificare) pe o altă cartelă fizică. Cea de-a doua conduită se distanțează de ingineria socială, având la bază un atac cu un grad mult mai ridicat de complexitate tehnică.

[16] Constând în accesarea contului WhatsApp. Nu prezintă relevanță faptul că făptuitorul folosește propriul telefon mobil inteligent, atât timp cât accesarea aplicației prin uzurparea contului este similară cu accesarea fără drept a contului de Facebook, Gmail etc. pe propriul dispozitiv.

[17] Restricționarea accesului la date informatice intervine atunci când accesarea contului WhatsApp determină deconectarea victimei. În opinia noastră, nu prezintă relevanță faptul că victima își poate ulterior recupera accesul la cont, atâta vreme cât infracțiunea prevăzută de art. 362 C. pen. s-a consumat deja la un moment anterior.

LIBRIS We know books

socializare[18]. Astfel, dacă făptuitorul uzurpă identitatea unei persoane prin crearea unui cont fals pe o rețea de socializare, în scopul inducerii în eroare a unor persoane, se va putea reține un concurs de infracțiuni cu conexitate etiologică între fals informatic (art. 325 C. pen.) și înșelăciune comisă prin mijloace frauduloase [art. 244 alin. (2) C. pen.].

2. Raportul dintre infracțiunea de înșelăciune și alte infracțiuni informatice

Înșelăciunea poate intra atât într-un concurs de infracțiuni, cât și într-un concurs de calificări (de norme penale)[19] cu numeroase alte infracțiuni informatice, precum accesul ilegal la un sistem informatic (art. 360 C. pen.)[20], alterarea integrității datelor informatice (art. 362 C. pen.)[21], falsul informatic (art. 325 C. pen.)[22] sau efectuarea de operațiuni financiare în mod fraudulos (art. 250 C. pen.)[23]. Totuși, prezintă o relevanță deosebită clarificarea raportului juridic dintre înșelăciune, fraudă informatică (a se vedea *infra*, pct. 2.1) și *phishing* (a se vedea *infra*, pct. 2.2).

2.1. Raportul dintre înșelăciune și frauda informatică

Delimitarea dintre înșelăciunea comisă prin mijloace informatice și frauda informatică prezintă o importanță deosebită nu doar din perspectiva corectei încadrări juridice, ci inclusiv pentru corecta evaluare a fenomenului criminalității informatice în sens restrâns. Deși decizia nr. 37/2021 a Înaltei Curți de Casație și Justiție[24] ar fi trebuit să tranșeze raportul juridic dintre cele două infracțiuni, observăm că practica judiciară continuă să întâmpine unele dificultăți în a le

---

[18] ICCJ, Completul pentru dezlegarea unor chestiuni de drept, decizia nr. 4/2021, publicată în M. Of. nr. 171 din 19 februarie 2021. Pentru o analiză succintă a acestei dezlegări de drept, a se vedea G. Zlati, *Recursuri în interesul legii și hotărâri prealabile pentru dezlegarea unor chestiuni de drept relevante în domeniul criminalității informatice*, în Curierul Judiciar nr. 11/2021, p. 684-686.

[19] În legătură cu concursul de calificări (de norme penale), a se vedea F. Streteanu, D. Nițu, *Drept penal. Partea generală*, vol. I, Ed. Universul Juridic, București, 2014, p. 161-165.

[20] De regulă, atunci când făptuitorul accesează conturi pentru a înlesni comiterea înșelăciunii.

[21] În ipoteza în care se uzurpează contul de WhatsApp, iar una dintre consecințe este deconectarea (restricționarea accesului la datele informatice) titularului de cont.

[22] În ipotezele în care discutăm despre o formă de uzurpare de identitate – crearea de conturi false pe rețele de socializare, *email spoofing*, *caller ID spoofing*, *web spoofing*, *deepfake* etc.

[23] Discutând despre două infracțiuni contra patrimoniului, un concurs ideal cu privire la același subiect pasiv ar trebui exclus de *plano*. De altfel, din perspectiva laturii obiective, apreciem că raportul dintre aceste două infracțiuni este similar cu raportul dintre înșelăciune și fraudă informatică. Astfel, în cazul art. 250 C. pen. nu discutăm despre o conduită autoprejudiciantă din partea victimei, făptuitorul fiind cel care procedează în mod nemijlocit la inițierea operațiunii.

[24] ICCJ, Completul pentru dezlegarea unor chestiuni de drept, decizia nr. 37/2021, publicată în M. Of. nr. 707 din 16 iulie 2021. Pentru o analiză succintă a acestei dezlegări de drept, a se vedea G. Zlati, *Recursuri...*, *precit.*, p. 686-687; G. Zlati, *Comentariu*, în G. Bodoroncea *et al.*, *Codul penal. Comentariu pe articole*, ed. a 3-a, Ed. C.H. Beck, București, 2020, p. 919-920; I.-M. Ursache, *Încadrarea juridică a fraudelor săvârșite prin intermediul platformelor de vânzări online – fraudă informatică sau înșelăciune?*, în Revista Pro Lege nr. 4/2021, p. 60-62. Pentru o analiză *in extenso*, a se vedea G. Zlati, *Tratat...*, *op. cit.*, p. 453-461.

LIBRIS We know books

distinge[25] – sub acest aspect prezintă relevanță solicitările frauduloase de rambursare tip *fast refund*[26]. Astfel, dincolo de asemănările evidente[27], la fel de evidente ar trebui să fie și deosebirile.

În primul rând, doar la frauda informatică ținta conduitei infracționale este reprezentată de un sistem informatic (de exemplu, un bancomat[28]), un program informatic (de exemplu, un contract inteligent[29]) sau alte date informatice (de exemplu, o bază de date). În schimb, înșelăciunea comisă prin mijloace informatice folosește tehnologia ca pe un simplu instrument pentru înlesnirea inducerii în eroare.

De asemenea, de esența fraudei informatice nu este existența unei conduite de inducere în eroare, ci manipularea unui sistem sau program informatic, prin una dintre modalitățile alternative prevăzute de art. 249 C. pen.[30]. Drept urmare, în cazul înșelăciunii comise prin mijloace informatice conduita autopăgubitoare aparține persoanei induse în eroare, în vreme ce în cazul fraudei informatice paguba este cauzată de modul în care sunt procesate în mod automat datele informatice ca urmare a acțiunii nemijlocite a făptuitorului. Acest aspect se

---

[25] Până la intervenția Înaltei Curți de Casație și Justiție, atât doctrina (M. Dobrinoiu, *Comentariu*, în M.A. Hotca, M. Dobrinoiu, *Infracțiuni prevăzute în legi speciale*, ed. 2, Ed. C.H. Beck, București, 2010, p. 609; M. Dobrinoiu, *Comentariu*, în I. Pascu *et al.*, *Noul Cod penal comentat. Partea specială*, ed. a II-a, Ed. Universul Juridic, București, 2014, p. 315-317; N. Neagu, *Fraude comise prin sisteme informatice și mijloace de plată electronice – variante speciale ale infracțiunii de înșelăciune?*, în Revista română de drept penal al afacerilor nr. 3/2019, p. 89; P.-M. Marcoci, *Some Considerations Regarding Fraud Investigation in E-Commerce*, în International Journal of Information Security and Cybercrime nr. 1/2016, p. 58-59), cât și jurisprudența erau majoritate în a reține eronat infracțiunea de fraudă informatică în ipotezele în care făptuitorul inducea în eroare victimele pe diverse platforme de comerț electronic (în eng., *e-commerce*).

[26] Astfel, făptuitorii utilizează codurile de retur furnizate de comerciant pentru a restitui produse fără valoare ori cu valoare mult diminuată. Deși în aceste cazuri elementul esențial de diferențiere constă în interpunerea unei persoane fizice în procesul de rambursare a plății, putem observa faptul că la nivelul practicii judiciare există trimiteri în judecată atât pentru înșelăciune (C. Ap. Constanța, secția penală și pentru cauze cu minori și de familie, decizia nr. 1260/2024, *www.rejust.ro*), cât și pentru fraudă informatică (C. Ap. Brașov, secția penală, decizia nr. 895/2024, *www.rejust.ro*). În ceea ce ne privește, atât timp cât rambursarea sumelor achitate pentru produsul aparent restituit se realizează de către sistemul de plăți, fără intervenția unui prepus sau reprezentant al persoanei prejudiciate, fapta constituie o frauda informatică. În esență, făptuitorul transmite o instrucțiune sistemului informatic (modalitatea introducerii de date informatice), determinându-l să inițieze procedura de rambursare.

[27] Pentru asemănări, a se vedea inclusiv C. Duvac, *Asemănări și deosebiri între înșelăciune și alte incriminări din noul Cod penal*, în Dreptul nr. 2/2012, p. 76. Autorul concluzionează în mod corect că în cazul ambelor infracțiuni putem discuta despre un *animus fraudandi*.

[28] Nu este exclus ca făptuitorul să manipuleze bancomatul în vederea remiterii de numerar, fără a utiliza un instrument de plată electronică. Procedând astfel, nu se va putea reține efectuarea de operațiuni financiare în mod fraudulos (art. 250 C. pen.), urmând a fi reținută norma generală – frauda informatică (art. 249 C. pen.).

[29] Un contract inteligent poate implementa funcția de schimb între două tokenuri (de exemplu, USDC/ETH, USDT/BTC). În cazul în care codul sursă conține o vulnerabilitate, făptuitorul ar putea transmite o tranzacție susceptibilă să exploateze această eroare, determinând contractul inteligent să inițieze o tranzacție fără să existe o contraprestație – a se vedea, în acest sens, și: G. Zlati, *Blockchain and criminal law; the fundamentals*, ERA Forum, vol. 24, nr. 2/2023, p. 309-310; N. Furneaux, *There's no such thing as crypto crime. An investigative handbook*, Ed. Wiley, 2024, p. 93-94.

[30] De cele mai multe ori discutăm despre o fraudă informatică comisă printr-o introducere de date informatice.

LIBRIS We know books

răsfrânge implicit asupra analizei raportului de cauzalitate dintre acțiunea făptuitorului și paguba produsă.

2.2. Raportul dintre înșelăciune și phishing

Uneori, în doctrină[31], se pune semnul echivalenței între înșelăciunea prin mijloace informatice și *phishing*, ceea ce, din punctul nostru de vedere, este vădit eronat. Cu toate că între cele două poate exista o relație mijloc-scop, în realitate discutăm despre două fapte cu totul diferite. Astfel, o conduită tip *phishing* poate înlesni săvârșirea ulterioară a infracțiunii de înșelăciune sau a unei alte infracțiuni[32], dar nu rezultă *per se* în cauzarea unei pagube.

De altfel, în vreme ce înșelăciunea este o infracțiune contra patrimoniului, modul de operare tip *phishing* ar putea fi încadrat din punct de vedere juridic ca fiind un fals informatic (art. 325 C. pen.). Eventuala pagubă rezultă însă din exploatarea subsecventă a datelor obținute prin *phishing*, ca urmare a inducerii în eroare a unei persoane, ceea ce implică un act de executare distinct[33].

În concluzie, atunci când analizăm din punct de vedere juridic modul de operare tip *phishing* putem avea în vedere eventual o infracțiune de fals informatic (art. 325 C. pen.), între aceasta și orice altă infracțiune scop (art. 244, art. 249, art. 250 etc.) trebuind a fi reținut un concurs real cu conexitate etiologică.

Deși inclusiv conduita tip *phishing* presupune o inducere în eroare ca formă de inginerie socială, paguba nu se produce decât ca urmare a unei conduite ulterioare. Simplul fapt al obținerii unor date care înlesnesc comiterea unei infracțiuni scop nu prezintă relevanță sub aspectul reținerii unei infracțiuni contra patrimoniului. Astfel, dincolo de faptul că date precum conturi de utilizator, parole de acces, coduri PIN, date de identificare ale instrumentelor de plată electronică, seturi de cuvinte-cheie (*seed phrase*) nu au o valoare economică intrinsecă, obținerea unui beneficiu material din comercializarea acestora pe *dark web* nu se transpune *per se* într-o pagubă pentru titularul acestor date. Doar exploatarea acestor informații este susceptibilă de a cauza o pagubă, însă în aceste cazuri discutăm despre o conduită distinctă ce va atrage aplicabilitatea unui alt text de incriminare – acces ilegal la un sistem informatic (art. 360 C. pen.), înșelăciune (art. 244 C. pen.), fraudă informatică (art. 249 C. pen.), efectuare de operațiuni financiare în mod fraudulos (art. 250 C. pen.) etc.

---

[31] A se vedea, în acest sens, J.-J. Oerlmans, A. de Hingh, W. van der Wagen, *op. cit.*, p. 116.

[32] De regulă, prin *phishing* se urmărește obținerea următoarelor date: credențiale de acces, în scopul înlesnirii unui acces la un sistemul informatic (art. 360 C. pen.); date de identificare ale unui instrument de plată electronică (card bancar), în scopul înlesnirii efectuării unei operațiuni financiare în mod fraudulos (art. 250 C. pen.); seturi de cuvinte-cheie (în eng., *seed phrase* sau *mnemonic phrase*), în scopul înlesnirii unor tranzacții frauduloase având ca obiect monede virtuale (art. 250 C. pen.) sau alte criptoactive (art. 249 C. pen.); date personale, în scopul înlesnirii unui furt de identitate (posibil art. 325 C. pen.), distribuirii sau punerii acestora la dispoziție altor persoane (art. 365 C. pen.) etc.

[33] A se vedea și S. Bogdan, D.A. Șerban, *Drept penal. Partea specială. Infracțiuni contra patrimoniului, contra autorității, de corupție, de serviciu, de fals și contra ordinii și liniștii publice*, ed. a II-a, Ed. Universul Juridic, București, 2023, p. 154. Autorii susțin faptul că în cazul înșelăciunii conduita autopăgubitoare trebuie să producă în mod direct paguba, fără să fie necesară o conduită subsecventă a făptuitorului.

LIBRIS | We know books

II. Analiza înșelăciunii comise prin mijloace informatice

În cele ce urmează vom analiza conduite infracționale unde obiectul infracțiunii sau produsul acesteia constă în monedă fiduciară, monedă virtuală sau alte criptoactive (de exemplu, NFT-uri). Având în vedere că art. 244 C. pen. face vorbire despre scopul obținerii unui folos patrimonial, se pune problema în ce măsură obținerea frauduloasă de criptoactive se pliază pe un asemenea scop special. Sub acest aspect, n-ar trebui să existe vreo controversă – obținerea de criptoactive se transpune într-un veritabil folos (beneficiu) patrimonial (material)[34]. De altfel, din perspectiva dreptului penal, criptoactivele sunt văzute ca bunuri mobile incorporale.

Dacă în privința unor conduite infracționale (de exemplu, fraudele investiționale) natura juridică a obiectului sau produsului infracțiunii nu prezintă relevanță[35], unele dintre acestea (de exemplu, o înșelăciune prin simularea adresei publice[36] sau prin utilizarea unor tokeni creați în scop de testare) exploatează chiar modul în care funcționează atât tehnologia registrelor distribuite (inclusiv blockchain)[37], cât și aplicațiile dezvoltate pe aceasta.

Având în vedere că prezentul articol se concentrează pe analiza infracțiunii de înșelăciune în raport cu diverse conduite infracționale, vom evita o analiză *in extenso* în legătură cu aspectele de ordin terminologic și tehnic deosebit de relevante pentru înțelegerea raportului dintre tehnologia registrelor distribuite (inclusiv blockchain) și dreptul penal[38].

În esență, atragem atenția asupra modificărilor aduse de Legea nr. 207/2021 pentru modificarea și completarea Codului penal[39] ca urmare a transpunerii Directivei (UE) 2019/713[40] în dreptul național. Discutăm în acest caz despre reformarea definiției legale cuprinse în art. 180 C. pen.[41] prin modificarea denumirii marginale și introducerea monedei virtuale alături de cea electronică, modificarea unor texte de incriminare prin înlocuirea noțiunii de „instrument de plată electronică" cu cea de „instrument de plată fără numerar" sau introducerea

---

[34] A se vedea și G. Zlati, *Tehnologia blockchain, monedele virtuale și dreptul penal*, în Penalmente Relevant nr. 1/2021, p. 56.

[35] În acest caz, monedele virtuale sau alte criptoactive sunt preferate de către făptuitori deoarece înlesnesc procesul de spălare a banilor prin folosirea unor servicii de obfuscare a tranzacțiilor (în eng., *mixers* sau *tumblers*). Pentru o analiză în acest sens, a se vedea N. Furneaux, *op. cit.*, p. 336-346.

[36] În engleză, *public address poisoning*.

[37] În continuare ne vom raporta la noțiunea „blockchain".

[38] Pentru o analiză aprofundată în acest sens, a se vedea: G. Zlati, *Tehnologia blockchain...*, *precit.*, p. 10 și urm.; G. Zlati, *Blockchain...*, *precit.*, p. 295 și urm.; A.-R. Trandafir, G. Zlati, *Monedele virtuale: între obținerea datelor privind tranzacțiile financiare și luarea măsurilor asiguratorii în procesul penal*, AUBD – Forum Juridic, nr. 1/2022, p. 56 și urm.; G. Zlati, *Securitatea cibernetică – de la blockchain la monede virtuale și criptoactive*, în Curierul Judiciar nr. 11/2021, p. 661 și urm.; D. Herinean, *Înțelesul unor termeni și expresii din dreptul penal în cyberspațiu*, în AUBD – Forum Juridic, nr. 2/2024, p. 180-182.

[39] Publicată în M. Of. nr. 720 din 22 iulie 2021.

[40] Directiva (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.

[41] Extinderea instrumentului de plată electronică.