CRIMINALITATEA INFORMATICĂ ÎN ROMÂNIA

George **Zlati**[1)]

Rezumat: *Prin prezentul articol, autorul își propune să realizeze o analiză generală a criminalității informatice, pornind de la definirea acestui concept și continuând cu maniera în care instrumentele juridice internaționale ori europene au afectat legislația în materie penală. De asemenea, autorul analizează hotărâri obligatorii ale Înaltei Curți de Casație și Justiție cu privire la chestiuni, precum: montarea unui skimmer la bancomat; retragerea de numerar de la bancomat; crearea de conturi false pe rețelele de socializare; raportul înșelăciunea tradițională și frauda informatică.*

Summary: *Through this article the author provides a general analysis of cybercrime, starting from defining the concept and continuing with the way in which international or European legal instruments have affected the national criminal law legislation. The author also analyses binding rulings of the High Court of Cassation and Justice on issues such as: placing a skimmer at the ATM; cash withdrawal from ATM; creating fake accounts on social networks; the relationship between the traditional fraud and computer fraud.*

Cuvinte-cheie: *criminalitate informatică; infracțiuni informatice; acces ilegal la un sistem informatic; înșelăciune tradițională; fraudă informatică; fals informatic; sistem informatic; Directiva (UE) 2019/713; monede virtuale; instrument de plată fără numerar.*

Keywords: *cybercrime; illegal access to information system; traditional fraud; computer fraud; computer forgery; information system; Directive (EU) 2019/713; virtual currency; non-cash payment instrument.*

[1)] George Zlati este doctor în drept și avocat penalist specializat în infracțiuni informatice. Poate fi contactat la adresa de e-mail *contact@zlati.legal*

I. Conceptul de „criminalitate informatică”

Criminalitatea informatică reprezintă un „concept-umbrelă” ce ar putea fi calificat de către unii inclusiv ca fiind unul lipsit de previzibilitate[2]. În ciuda tuturor eforturilor doctrinare, nu avem în momentul de față o definiție legală la nivel internațional[3], cu toate că acest concept a fost recunoscut și adoptat inclusiv de către Consiliul Europei[4] și Organizația Națiunilor Unite[5]. Lipsa unei definiții general acceptate nu a reprezentat însă un impediment pentru ca acest concept să intre în vocabularul curent[6], criminalitatea informatică fiind identificată cu ușurință inclusiv în literatura de specialitate[7], jurisprudență[8], diverse date statistice[9] și uneori chiar în legislație[10].

Atunci când ne referim la „criminalitatea informatică”, ar trebui să avem în vedere, în primul rând, legislația penală prin intermediul căreia au fost aduse în sfera ilicitului penal o serie de conduite unde sistemul informatic ori datele informatice reprezintă un veritabil obiect al infracțiunii[11]. Tocmai de aceea, uneori se vorbește despre o criminalitate informatică în sens restrâns, atunci când conduita făptuitorului

[2] A se vedea o dezvoltare în *G. Zlati*, Tratat de criminalitate informatică, vol. 1, Ed. Solomon, București, 2020, pp. 5-15; a se vedea și *A. Chandra, M.J. Snowe*, A taxonomy of cybercrime: Theory and design, în International Journal of Accouting Information Systems, vol. 38, 2020, p. 1.

[3] A se vedea și *S. Broadhead*, The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, în Computer Law & Security Review, vol. 34, 2018, p. 1181.

[4] Cu referire evidentă la Convenția privind criminalitatea informatică.

[5] În acest sens, United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, 2013, material disponibil pe pagina *unodc.org* (ultima accesare la data de 4 iunie 2021).

[6] Spre exemplu, în Oxford English Dictionary, „criminalitatea informatică” este definită ca fiind o infracțiune comisă prin utilizarea unui computer ori a Internetului. De asemenea, potrivit Cambridge English Dictionary, criminalitatea informatică este o infracțiune sau o activitate ilegală săvârșită prin utilizarea Internetului. În mod evident, ambele definiții sunt deosebit de generoase din moment ce am ajunge să includem în sfera criminalității informatice inclusiv o determinare sau înlesnire a sinuciderii (art. 191 C.pen.) comisă pe Internet.

[7] Trebuie să recunoaștem că de multe ori apelăm și noi la acest concept pentru a evita o enumerare a tuturor infracțiunilor relevante.

[8] Extras C.A. Pitești, s. pen., dec. nr. 651/2008: „Ca atare, nu se poate ajunge, la împlinirea acestui scop a funcției sale preventive, în cazul acestor infracțiuni de criminalitate informatică organizată desfășurată în grup, cu lideri și roluri distribuite, de o deosebită periculozitate socială, cu rezonanțe atât de negative la nivelul comunităților locale și chiar la nivel național (...) dacă organele judiciare nu acționează suficient de ferm și exigent în astfel de cauze (...)”.

[9] În acest sens se poate vedea raportul de activitate al DIICOT pe anul 2020, material disponibil pe pagina *diicot.ro*. În cuprinsul acestui raport de activitate se face vorbire despre faptul că „tendințele de manifestare a formelor de criminalitate informatică la nivel național sunt similare cu cele înregistrate la nivel internațional, expuse de altfel și în raportul IOCTA (*Internet Organised Crime Threat Assessment*) 2020”, fiind oferite, de asemenea, date statistice pe diverse categorii de infracțiuni. În mod evident, criminalitatea informatică reprezintă o categorie relevantă în statisticile prezentate.

[10] A se vedea, cu titlu de exemplu, art. 97 alin. (1) pct. 11 din Legea nr. 302/2004 privind cooperarea judiciară internațională în materie penală, republicată în M. Of. nr. 411 din 27 mai 2019.

[11] Nu dorim cu această ocazie să dezvoltăm cu privire la posibilitatea calificării datelor informatice ca fiind obiect material al infracțiunii. Această problemă am analizat-o cu alte ocazii (a se vedea, cu titlu de exemplu, *G. Zlati*, Tratat..., vol. 1, op. cit., pp. 321-323; *idem*, Dematerializarea obiectului material al infracțiunii în contextul evoluției tehnologice și consecințele acesteia, în Dreptul nr. 9/2013, p. 163 și urm.). În ceea ce ne privește, teoria tradițională potrivit căreia „obiectul material” al infracțiunii – de altfel, o creație doctrinară – se poate raporta în mod exclusiv doar la o entitate materială (*e.g.,* un lucru sau o ființă) ar trebui reconsiderată. În realitate, nu discutăm despre un obiect material, ci despre un obiect al conduitei infracționale. Contează mai puțin faptul că acesta este corporal sau necorporal, relevant fiind faptul că lezarea sau punerea în pericol a valorii sociale protejate de textul de incriminare implică o conduită (comisivă ori omisivă) a făptuitorului îndreptată împotriva unei entități corporale sau necorporale. Astfel, cu toate că suntem de acord că o infracțiune precum cea de amenințare nu are un „obiect material”, infracțiunea de alterare a integrității datelor informatice (art. 362 C.pen.) implică o acțiune îndreptată împotriva unor date informatice. Acestea ajung să se interpună între conduita făptuitorului și valoarea socială protejată prin textul de incriminare, devenind un veritabil obiect al acțiunii (conduitei) infracționale.

lezează sau pune în pericol confidențialitatea, integritatea ori disponibilitatea sistemelor informatice ori a datelor informatice[12].

Raportarea la sistemele informatice și datele informatice ca fiind un obiect al infracțiunii nu este lipsită de consecințe. Dacă ne-am raporta la acestea inclusiv ca fiind un mijloc/instrument pentru comiterea de infracțiuni, ar exista riscul extinderii nejustificate a conceptului de „criminalitate informatică".

Astfel, dacă am include în sfera criminalității informatice și infracțiuni din Legea nr. 8/1996 privind dreptul de autor și drepturile conexe, republicată[13], sau infracțiuni tradiționale comise prin intermediul sistemelor informatice, în mod evident, conceptul de „criminalitate informatică" s-ar extinde în mod semnificativ. Spre exemplu, infracțiunea de pornografie infantilă prin sisteme informatice [art. 374 alin. (2)-(3) C.pen.] este general percepută ca intrând în sfera criminalității informatice. Cu toate acestea, pornografia infantilă a fost inițial incriminată în România[14] fără vreo trimitere la sistemele informatice. De asemenea, putem discuta despre o hărțuire în mediul online [art. 208 alin. (2) C.pen.], despre violarea vieții private prin intermediul unei supravegheri tehnice care să implice folosirea unor sisteme informatice ori a unor programe informatice [art. 226 alin. (1) C.pen.], o racolare de minori în mediul online (art. 222 C.pen.) etc.

Prin urmare, devine evident că, atunci când ne referim la conceptul de „criminalitate informatică", prezintă relevanță criteriul sau criteriile la care ne raportăm. În ceea ce ne privește, **criminalitatea informatică în sens restrâns** trebuie raportată la sistemele informatice și datele informatice ca fiind un obiect al infracțiunii. Cu alte cuvinte, sistemul informatic sau datele informatice nu reprezintă un mijloc/instrument de comitere a infracțiunii, ci o veritabilă țintă a conduitei făptuitorului. Vom discuta, așadar, despre criminalitate informatică în sens restrâns atunci când ne vom referi la infracțiuni, precum: frauda informatică[15] (art. 249 C.pen.), falsul informatic[16] (art. 325 C.pen.), accesul ilegal la un sistem informatic (art. 360 C.pen.), alterarea integrității datelor informatice (art. 362 C.pen.), perturbarea funcționării sistemelor informatice (art. 363 C.pen.) ori transferul neautorizat de date informatice (art. 364 C.pen.). De altfel, aceste infracțiuni nu se pot comite decât prin intermediul unui sistem informatic, al unei rețele informatice etc.[17].

[12] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, op. cit., p. XVII.

[13] Republicată în M. Of. nr. 489 din 14 iunie 2018. Ne referim aici îndeosebi la infracțiunea prevăzută la art. 195, ce pedepsește „reproducerea neautorizată pe sisteme de calcul a programelor pentru calculator în oricare dintre următoarele modalități: instalare, stocare, rulare sau executare, afișare ori transmitere în rețea internă".

[14] A se vedea, în acest sens, art. 11 din Legea nr. 196/2003 privind prevenirea și combaterea pornografiei, republicată în M. Of. nr. 87 din 4 februarie 2008, ce sancționa „distribuirea materialelor cu caracter obscen, care prezintă imagini cu minori având un comportament explicit sexual" [alin. (1)] și deținerea de materiale pornografice în vederea răspândirii lor [alin. (2)]. Înainte de republicarea Legii nr. 196/2003, textul de incriminare se regăsea în conținutul art. 12 din lege. Ulterior, prin art. 51 din Legea nr. 161/2003 a fost incriminată pornografia infantilă prin sisteme informatice. În prezent, art. 374 C.pen. grupează atât pornografia infantilă tradițională, cât și cea prin sisteme informatice în Legea nr. 196/2003, republicată în M. Of. nr. 198 din 20 martie 2014, rămânând incriminată doar „racolarea, determinarea sau folosirea unei persoane majore lipsite de discernământ la comiterea unor acte cu caracter obscen, în scopul producerii de materiale pornografice" (art. 9 din lege).

[15] Chiar dacă, în ceea ce privește infracțiunea de fraudă informatică (art. 249 C.pen.), este uneori dificil în a înțelege raportul cu infracțiunea tradițională de înșelăciune (art. 244 C.pen.), nu avem rezerve în a reține că nu am putea discuta despre o fraudă informatică fără să ne raportăm la sistemul informatic ori datele informatice stocate pe acesta ca fiind o veritabilă țintă a conduitei infracționale. Astfel, la o simplă analiză a laturii obiective a art. 249 C.pen., observăm că fiecare modalitate în parte vizează sistemul informatic ori datele informatice ca obiect al infracțiunii, și nu ca un simplu mijloc/instrument de comitere a acesteia.

[16] Apreciem că precizările făcute *supra* prezintă relevanță și pentru infracțiunea de fals informatic. În ciuda paralelismului deficitar existent între infracțiunea de fals informatic (art. 325 C.pen.) și infracțiunile tradiționale privind falsurile în înscrisuri (art. 320-322 C.pen.), sistemul informatic ori datele informatice devin o țintă a conduitei infracționale.

[17] A se vedea, în acest sens, și *J. Clough*, Principles of Cybercrime, second edition, Cambridge University Press, UK, 2015, p. 11.

În schimb, **criminalitatea informatică în sens larg** se raportează la sistemele informatice și datele informatice ca fiind un mijloc/instrument de comitere a infracțiunii. O asemenea raportare ne poate conduce înspre o pantă alunecoasă, deoarece aproape orice infracțiune se poate comite prin intermediul unor sisteme informatice ori a unor date informatice. Cu toate acestea, așa cum am menționat deja, există unele infracțiuni tradiționale care sunt acceptate ca intrând în sfera criminalității informatice atunci când sunt comise prin intermediul unor sisteme informatice ori a unor date informatice. Cel mai bun exemplu în acest sens este infracțiunea de pornografie infantilă (art. 374 C.pen.). De altfel, infracțiunea de pornografie infantilă prin sisteme informatice era reglementată, anterior intrării în vigoare a noului Cod penal, prin art. 51 din Legea nr. 161/2003 în cuprinsul Titlului cu denumirea marginală „Prevenirea și combaterea criminalității informatice".

În încercarea de a concilia cele două abordări, am putea accepta că în conceptul-umbrelă de „criminalitate informatică" sunt înglobate, în primul rând, infracțiunile informatice îndreptate împotriva sistemelor informatice ori a datelor informatice (criminalitatea informatică în sens restrâns), iar pe urmă acele infracțiuni ce se pot comite prin intermediul unui sistem informatic ori al unor date informatice, în ipoteza în care acestea sunt prevăzute ca elemente constitutive ale infracțiunii. Astfel, infracțiunea de pornografie infantilă se raportează în mod explicit la sistemul informatic ori mijlocul de stocare a datelor informatice. În schimb, deși infracțiunea de omor se poate comite inclusiv prin intermediul unui sistem informatic, aceasta nu poate fi inclusă nici măcar în conceptul de „criminalitate informatică" în sens larg. De asemenea, spre deosebire de infracțiunea de hărțuire, care se raportează în mod explicit la efectuarea de comunicări prin mijloace de transmitere la distanță (deci inclusiv a unui sistem informatic[18]), infracțiunile de amenințare (art. 206 C.pen.) sau de șantaj (art. 207 C.pen.) rămân în afara sferei criminalității informatice.

Totuși, chiar și procedând de o asemenea manieră, această problemă a definirii conceptului de „criminalitate informatică" nu ar fi clarificată întru totul, deoarece ar exista în continuare unele texte de incriminare ce ar pune sub semnul întrebării această clasificare. Cu titlu de exemplu, infracțiunea de furt are o formă calificată ce sancționează furtul prin scoaterea din funcțiune a sistemului de alarmă ori de supraveghere [art. 229 alin. (1) lit. e) C.pen.].

Dincolo de faptul că nu este exclus ca un vehicul să fie sustras printr-o interacțiune logică de la distanță, relevantă din perspectiva reținerii infracțiunii de acces ilegal la un sistem informatic (art. 360 C.pen.), observăm faptul că legiuitorul s-a raportat, în conținutul art. 229 alin. (1) lit. e) C.pen., la sistemul informatic (dacă acesta este un sistem de alarmă ori de supraveghere) ca fiind chiar țintă a conduitei infracționale, adică reprezintă un veritabil obiect secundar al infracțiunii. Este însă infracțiunea de furt calificat o infracțiune informatică ce intră în sfera criminalității informatice în sens restrâns sau în sens larg? Credem că răspunsul la această întrebare ar trebui să fie mai degrabă unul negativ.

Suntem de părere, așadar, că orice criterii am folosi, definirea conceptului de „criminalitate informatică" rămâne problematică. Tocmai de aceea, este de preferat ca legiuitorul să evite folosirea acestui concept în legislație. Un exemplu negativ în acest sens este trimiterea făcută de legiuitor la „fapte legate de criminalitatea informatică" în cuprinsul art. 97 alin. (1) pct. 11 din Legea nr. 302/2004 privind cooperarea judiciară internațională în materie penală, republicată[19].

[18] Sintagma „mijloc de comunicare la distanță" include și noțiunea de „sistem informatic", fără a se reduce însă la aceasta. Astfel, chiar dacă un telefon fix analogic reprezintă un mijloc de comunicare la distanță, aceasta nu îl face automat și un sistem informatic.

[19] Republicată în M. Of. nr. 411 din 27 mai 2019.

II. Reglementarea criminalității informatice la nivel european și național

Convenția Consiliului Europei privind criminalitatea informatică[20] rămâne în continuare unul dintre cele mai reprezentative instrumente juridice în domeniul criminalității informatice la nivel internațional[21]. Ar trebui totuși menționat că acest instrument juridic se bazează într-o bună măsură pe Recomandarea Consiliului Europei din anul 1989[22]. Tocmai de aceea, nu credem că este eronat să afirmăm în legătură cu Convenția privind criminalitatea informatică faptul că discutăm despre un instrument juridic depășit de noile forme de criminalitate informatică.

Dincolo de acest instrument juridic, în ultimii 18 ani, legiuitorul european a fost deosebit de activ în a legifera în domeniul criminalității informatice. Printre instrumentele juridice relevante pentru dreptul penal substanțial, am putea enumera următoarele:

- Decizia-cadru 2001/413/JAI de combatere a fraudei și a falsificării mijloacelor de plată, altele decât numerarul;
- Decizia-cadru 2004/68/JAI privind combaterea exploatării sexuale a copiilor și a pornografiei infantile;
- Decizia-cadru 2005/222/JAI privind atacurile împotriva sistemelor informatice;
- Directiva 2011/93/UE privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile;
- Directiva 2013/222/JAI privind atacurile împotriva sistemelor informatice;
- Directiva (UE) 2019/713 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar.

A. Directiva 2013/222/JAI privind atacurile împotriva sistemelor informatice[23]

Această directivă a înlocuit Decizia-cadru 2005/222/JAI privind atacurile împotriva sistemelor informatice și a creat în sarcina legiuitorului obligația pozitivă de a incrimina anumite conduite ce intră în sfera criminalității informatice în sens restrâns, după cum urmează: accesarea ilegală a sistemelor informatice (art. 3)[24]; afectarea ilegală a integrității sistemului (art. 4)[25]; afectarea ilegală a integrității datelor (art. 5)[26];

[20] Ratificată prin Legea nr. 64/2004, publicată în M. Of. nr. 343 din 20 aprilie 2004.

[21] Pentru o analiză a prevederilor acestui instrument juridic, se poate vedea: *J. Clough*, A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation, în Monash University Law Review, vol. 40, 2014, p. 698 și urm.; *A.M. Weber*, The Council of Europe's Convention on Cybercrime, în Berkely Technology Law Journal, vol. 18, 2003, p. 425 și urm.; *M. Keyser*, The Council of Europe Convention on Cybercrime, în Journal of Transnational Law & Policy, vol. 12, 2002-2003, p. 287 și urm.

[22] Recomandarea nr. R(89)9 a Consiliului Europei. Aceasta ia forma unui raport întocmit de un comitet de experți ce conține o analiză juridică atât a unei liste minimale, cât și a unei liste opționale de infracțiuni informatice.

[23] Publicată în J. Of., seria L, nr. 218/8 din 14 august 2013.

[24] În prezent incriminată la art. 360 C.pen. Înainte de intrarea în vigoare a noului Cod penal, incriminarea se regăsea în cuprinsul art. 42 din Legea nr. 161/2003.

[25] În prezent incriminată la art. 363 C.pen. Înainte de intrarea în vigoare a noului Cod penal, incriminarea se regăsea în cuprinsul art. 45 din Legea nr. 161/2003.

[26] În prezent incriminată la art. 362 C.pen. Înainte de intrarea în vigoare a noului Cod penal, incriminarea se regăsea în cuprinsul art. 44 alin. (1) din Legea nr. 161/2003.

interceptarea ilegală (art. 6)[27] și conduite specifice legate de instrumentele care servesc la săvârșirea infracțiunilor informatice (art. 7)[28]. Toate aceste conduite sunt incriminate, *de lege lata*, prin intermediul art. 360-365 C.pen.

Similar cu Decizia-cadru 2005/222/JAI, Directiva 2013/222/JAI nu se referă la frauda informatică și falsul informatic. Impactul acestei directive a fost totuși nesemnificativ, având în vedere faptul că legiuitorul național incriminase deja prin Legea nr. 161/2003 toate aceste conduite la momentul transpunerii în dreptul intern a Convenției privind criminalitatea informatică. Astfel, frauda informatică era incriminată inițial prin intermediul art. 49 din Legea nr. 161/2003 (în prezent art. 249 C.pen.), iar falsul informatic prin intermediul art. 48 din aceeași lege (în prezent art. 325 C.pen.).

B. Directiva (UE) 2019/713 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar[29]

Această directivă a înlocuit Decizia-cadru 2001/413/JAI de combatere a fraudei și a falsificării mijloacelor de plată, altele decât numerarul. Decizia-cadru a determinat legiuitorul român să incrimineze, prin Legea nr. 365/2002 privind comerțul electronic[30], următoarele conduite: falsificarea instrumentelor de plată electronică (art. 24 din lege)[31], deținerea de echipamente în vedere falsificări instrumentelor de plată electronică (art. 25 din lege)[32], efectuarea de operațiuni financiare în mod fraudulos (art. 27 din lege)[33] și acceptarea operațiunilor financiare efectuate în mod fraudulos (art. 28 din lege)[34].

Directiva (UE) 2019/713 ridică totuși problema în ce măsură nu este necesară o nouă intervenție a legiuitorului pentru a pune în acord legislația națională cu dreptul european. În primul rând, spre deosebire de Decizia-cadru 2001/413/JAI, Directiva (UE) 2019/713 nu se raportează la instrumentele de plată (ce includeau și instrumentul de plată electronică)[35], ci la instrumentele de plată fără numerar. Rațiunea a fost aceea de a acoperi, prin definiția „instrumentului de plată fără numerar", și monedele virtuale (*e.g.*,

[27] În prezent incriminată la art. 361 C.pen. Înainte de intrarea în vigoare a noului Cod penal, incriminarea se regăsea în cuprinsul art. 43 din Legea nr. 161/2003.

[28] În prezent incriminată la art. 365 C.pen. Înainte de intrarea în vigoare a noului Cod penal, incriminarea se regăsea în cuprinsul art. 46 din Legea nr. 161/2003.

[29] Publicată în J. Of., seria L, nr. 123/18 din 10 mai 2019.

[30] Publicată în M. Of. nr. 483 din 5 iulie 2002. Legea a fost republicată în M. Of. nr. 959 din 29 noiembrie 2006, infracțiunile prevăzute la art. 24-28 din lege fiind transpuse în noul Cod penal. Tocmai de aceea, abrogarea art. 24-28 din Legea nr. 365/2002 prin art. 107 din Legea nr. 187/2012 nu echivalează cu o dezincriminare, conduitele avute în vedere fiind incriminate în continuare prin intermediul art. 311 alin. (2), art. 314 alin. (2), art. 250 și art. 251 C.pen.

[31] În prezent incriminată la art. 311 alin. (2) C.pen.

[32] În prezent incriminată la art. 314 alin. (2) C.pen.

[33] În prezent incriminată la art. 250 C.pen.

[34] În prezent incriminată la art. 251 C.pen.

[35] Potrivit art. 1 lit. (a) din Decizia-cadru 2001/413/JAI, „instrument de plată" înseamnă „un instrument corporal, altul decât moneda legală (bancnote sau monede), care, în funcție de natura lui specifică, singur sau împreună cu alt instrument (de plată), îi dă posibilitatea deținătorului sau utilizatorului să transfere bani sau o valoare bănească, ca, de exemplu, cărți de credit, carduri de tip eurocec, alte carduri emise de instituții financiare, cecuri de călătorie, eurocecuri, alte cecuri și cambii care sunt protejate împotriva imitației sau uzului fraudulos, de exemplu, prin intermediul modelului, codului sau semnăturii". Precizăm totuși că definițiile regăsite în Legea nr. 365/2002 (art. 1 pct. 11-13) nu au preluat *verbatim* definiția „instrumentului de plată" din Decizia-cadru 2001/413/JAI. Aceasta se datorează, în primul rând, faptului că instrumentul de plată la care face referire decizia-cadru nu se raporta în mod exclusiv la instrumentul de plată electronică.

bitcoin, ethereum, egld, zilliqa, ADA, DOT etc.), ce diferă în mod semnificativ de monedele electronice recunoscute ca mijloc de plată[36].

Astfel, în cuprinsul art. 2 lit. (d) din directivă este definită „moneda virtuală”[37], aceasta fiind inclusă, alături de monedele electronice, în accepțiunea noțiunii de „mijloc digital de schimb” la care se raportează definiția „instrumentului de plată fără numerar”[38]. Cu alte cuvinte, definiția „instrumentului de plată fără numerar” [art. 2 lit. (a) din directivă] are în vedere atât mijloacele de plată electronică tradiționale (cardul bancar, serviciul de Internet Banking etc.), cât și mijloacele digitale de schimb, ce includ atât monedele electronice, cât și monedele virtuale [art. 2 lit. (c) din directivă].

Precizarea este de o importanță deosebită, deoarece, *de lege lata*, definiția „instrumentului de plată electronică” de la art. 180 C.pen. este mai restrânsă decât definiția „instrumentului de plată fără numerar” de la art. 2 lit. (a) din directivă.

Principala consecință este aceea că transferul neautorizat de monede virtuale nu poate intra, *de lege lata*, sub incidența art. 250 C.pen. (efectuarea de operațiuni financiare în mod fraudulos)[39]. Nu discutăm totuși despre un vid legislativ, deoarece un transfer neautorizat de monede virtuale se pliază întru totul pe elementele constitutive ale fraudei informatice (art. 249 C.pen.). Având totuși în vedere reticența legiuitorului de a renunța la incriminarea de la art. 250 C.pen., oferind astfel aplicabilitate art. 249 C.pen. ca normă generală[40], o intervenție legislativă prin care să se transpună art. 2 lit. (a) din directivă devine iminentă.

De altfel, am criticat recent *in extenso* un Proiect de Lege pentru modificarea și completarea Legii nr. 286/2009 privind Codul penal și pentru dispunerea altor măsuri de transpunere a Directivei (UE) 2019/713[41] ce a fost supus dezbaterii publice. Principala critică a fost aceea că, prin proiectul de act normativ, s-a urmărit modificarea art. 249 C.pen., în sensul introducerii unui nou alineat care să cuprindă o variantă de incriminare asimilată referitoare la „transferul de bani, valoare monetară sau monedă virtuală”. Or, o asemenea modificare era problematică, având în vedere că, prin aceeași propunere legislativă, se urmărea modificarea art. 180 C.pen. și a art. 250 C.pen. de o asemenea manieră încât să intre sub incidența textului de incriminare... transferul de valoare monetară sau monedă virtuală.

[36] Pentru clarificări, se poate vedea art. 2 din Directiva 2009/110/CE privind accesul la activitate, desfășurarea și supravegherea prudențială a activității instituțiilor emitente de monedă electronică (publicată în J. Of., seria L, nr. 267/7 din 10 octombrie 2009). De asemenea, se pot analiza prevederile Legii nr. 210/2019 privind activitatea de emitere de monedă electronică (publicată în M. Of. nr. 914 din 13 noiembrie 2019) ori Regulamentul B.N.R. nr. 5/2019 privind instituțiile emitente de monedă electronică (publicat în M. Of. nr. 1021 din 19 decembrie 2019).

[37] Potrivit art. 2 lit. (d) din directivă, „monedă virtuală” înseamnă o reprezentare digitală de valoare care nu este emisă sau garantată de o bancă centrală sau de o autoritate publică, nu este în mod obligatoriu legată de o monedă instituită legal și nu deține statutul legal de monedă sau de bani, dar este acceptată de către persoane fizice sau juridice ca mijloc de schimb și poate fi transferată, stocată și tranzacționată în mod electronic.

[38] Potrivit art. 2 lit. (a) din directivă, „instrument de plată fără numerar” înseamnă un dispozitiv, un obiect sau o înregistrare protejat(ă), nematerial(ă) sau material(ă) sau o combinație a acestora, altul (alta) decât monedele legale și care, singur(ă) sau împreună cu o procedură sau un set de proceduri, permite deținătorului sau utilizatorului să transfere bani sau valoare monetară, inclusiv prin mijloace digitale de schimb.

[39] A se vedea o analiză, în acest sens, în *G. Zlati*, Tratat..., vol. 1, op. cit., pp. 340-344.

[40] Credem că art. 250 alin. (1)-(2) C.pen. nu este nimic altceva decât o normă specială în raport cu frauda informatică (art. 249 C.pen.). Doar art. 250 alin. (3) C.pen. incriminează în mod autonom un act pregătitor (transmiterea de date necesare în vederea efectuării unei operațiuni financiare) ce ar rămâne nesancționat în măsura în care transmiterea datelor respective nu ar lua forma unei complicități materiale.

[41] A se vedea, în acest sens, *G. Zlati*, Critici punctuale cu privire la Proiectul de Lege pentru modificarea și completarea Legii nr. 286/2009 privind Codul penal și pentru dispunerea altor măsuri de transpunere a Directivei (UE) 2019/713, *passim*, material disponibil pe *juridice.ro* (ultima accesare la data de 3 iunie 2021).

Există, din acest punct de vedere, o suprapunere nu doar între sfera de aplicabilitate a art. 249 C.pen. și a art. 250 C.pen., ci inclusiv între art. 249 alin. (1) (varianta actuală de incriminare) și alin. (2) C.pen. (varianta de incriminare ce se dorea a fi introdusă). Toate aceste suprapuneri la nivelul sferei de aplicabilitate a textelor ori a variantelor de incriminare nu ar fi condus decât la apariția unor concursuri de calificări dificil de soluționat la nivelul practicii judiciare.

În cele din urmă, în proiectul de act normativ[42] transmis Parlamentului nu s-a mai regăsit modificarea art. 249 C.pen. în sensul introducerii unei variante de incriminare distincte. Din contră, în Expunerea de motive a PL-x nr. 162/2021[43] se precizează faptul că „transferul neautorizat de monede virtuale (care nu fac parte din categoria instrumentelor de plată electronică) va fi încadrat la art. 249 C.pen. (frauda informatică), prevedere generală care a fost apreciată ca fiind suficientă pentru acoperirea acestei ipoteze din Directiva non-cash, precum și pentru a nu determina dificultăți în practica organelor judiciare".

O asemenea abordare ne dă totuși de gândit. Aceasta, întrucât pare să se susțină faptul că transferul de monede virtuale[44] se situează oricum sub incidența fraudei informatice, ceea ce este corect, din punctul nostru de vedere. De asemenea, se susține că transpunerea art. 6 din directivă printr-un text de incriminare distinct nu este necesară, având în vedere sfera de aplicabilitate generală a art. 249 C.pen., afirmație pe care o apreciem, de asemenea, ca fiind corectă. Ceea ce nu înțelegem este cum se va putea reține art. 249 C.pen. ulterior adoptării acestui proiect de lege, având în vedere modificarea art. 180 și a art. 250 alin. (1) C.pen. de o asemenea manieră încât să vizeze inclusiv monedele virtuale, nu doar pe cele electronice.

Luând în considerare posibilitatea reală ca acest proiect de act normativ să fie însușit de către legiuitor, apreciem necesar să facem o analiză punctuală la nivel de conținut. Precizăm în acest sens că **ne vom raporta în continuare la forma adoptată de către Senat**, la data redactării acestui material, proiectul de act normativ aflându-se în dezbatere la Camera Deputaților.

1. Observații referitoare la modificarea art. 180 C.pen. – mijlocul de plată fără numerar

Prin proiectul de act normativ se dorește modificarea art. 180 C.pen., acesta urmând a avea următorul conținut:

„Art. 180. Mijloace de plată fără numerar

(1) Prin «instrument de plată fără numerar» se înțelege un dispozitiv, un obiect sau o înregistrare, protejat, respectiv protejată, material ori nematerial, respectiv materială ori nematerială, sau o combinație a acestora, altul, respectiv alta, decât o monedă cu valoare circulatorie și care, singur, respectiv singură, sau împreună cu o procedură sau un set de proceduri, permite deținătorului sau utilizatorului transferul de bani sau valoare monetară, inclusiv prin monedă electronică sau monedă virtuală.

(2) Prin «instrument de plată electronică» se înțelege un instrument care permite efectuarea de retrageri de numerar, încărcarea și descărcarea unui instrument de monedă electronică, precum și transferuri de fonduri, altele decât cele ordonate și executate de către instituții financiare.

---

[42] A se vedea PL-x nr. 162/2021 pentru modificarea și completarea Legii nr. 286/2009 privind Codul penal, precum și pentru dispunerea unor 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. La data redactării acestui material, Proiectul de Lege a fost adoptat de către Senat și a fost transmis pentru raport comisiilor permanente ale Camerei Deputaților.

[43] A se vedea, în acest sens, *http://www.cdep.ro/proiecte/2021/100/60/2/em188.pdf.*

[44] Monedele virtuale nu sunt niciodată instrumente de plată electronică, ci doar un instrument de plată fără numerar, potrivit art. 180 alin. (1) raportat la alin. (4) C.pen., în varianta propusă spre modificare prin Proiectul de Lege.

(3) Prin «monedă electronică» se înțelege valoarea monetară stocată electronic, inclusiv magnetic, reprezentând o creanță asupra emitentului, emisă la primirea fondurilor în scopul efectuării de operațiuni de plată și care este acceptată de o persoană, alta decât emitentul de monedă electronică.

(4) «Moneda virtuală» înseamnă o reprezentare digitală a valorii care nu este emisă sau garantată de o bancă centrală sau de o autoritate publică, nu este în mod obligatoriu legată de o monedă instituită legal și nu deține statutul legal de monedă sau de bani, dar este acceptată de către persoane fizice sau juridice ca mijloc de schimb și poate fi transferată, stocată și tranzacționată electronic".

Din modificarea propusă pentru art. 180 C.pen. rezultă faptul că urmează să ne raportăm, *de lege ferenda*, la patru noțiuni distincte, fiecare dintre acestea beneficiind de o definiție proprie: „instrumentul de plată fără numerar" [art. 180 alin. (1) C.pen.], „instrumentul de plată electronică" [art. 180 alin. (2) C.pen.], „moneda electronică" [art. 180 alin. (3) C.pen.] și „moneda virtuală" [art. 180 alin. (4) C.pen.]. De asemenea, am mai preciza faptul că moneda electronică este avută în vedere atât în definiția „instrumentului de plată fără numerar", cât și în definiția „instrumentului de plată electronică". În schimb, moneda virtuală este menționată – în mod corect – doar în cuprinsul definiției „instrumentului de plată fără numerar".

În primul rând, este lesne de observat faptul că propunerea pentru modificarea art. 180 C.pen. preia, într-o bună măsură, conținutul din cuprinsul art. 2 din Directiva (UE) 2019/713. O diferență – importantă – ar fi aceea că, în art. 2 lit. (a) din directivă, „instrumentul de plată fără numerar" este definit ca fiind un mijloc prin intermediul căruia deținătorul sau utilizatorul poate transfera bani sau valoare monetară, fiind incluse aici și mijloacele digitale de schimb. Mijloacele digitale de schimb sunt, la rândul lor, definite în cuprinsul art. 2 lit. (c) din directivă, incluzând atât moneda electronică, cât și moneda virtuală.

Observăm, așadar, că în proiectul de act normativ nu se face trimitere la mijloacele digitale de schimb, ci se realizează o trimitere directă la moneda electronică și moneda virtuală în cuprinsul definiției „instrumentului de plată fără numerar". Sub acest aspect, nu vedem neapărat o problemă, această abordare rezultând mai degrabă dintr-o simplificare a definiției, fiind evitată o trimitere în cascadă. În măsura în care moneda electronică și moneda virtuală reprezintă mijloace digitale de schimb, apreciem că se poate face trimitere directă la acestea fără a se introduce o noțiune distinctă ce trebuia, la rândul ei, să beneficieze de o definiție legală.

De asemenea, lipsa unei trimiteri la noțiunea de „mijloc digital de schimb" este o alegere potrivită, având în vedere diferența care există între moneda electronică și moneda virtuală. Astfel, fie că ne raportăm la definițiile din Directiva (UE) 2019/713 și Directiva 2009/110/CE, fie la definițiile propuse prin proiectul de act normativ supus analizei, rezultă că moneda electronică poate fi acceptată pentru operațiuni de plată, în vreme ce moneda virtuală este folosită ca mijloc de schimb. Diferența nu este una lipsită de consecințe juridice, din moment ce moneda virtuală nu poate reprezenta prețul într-un contract de vânzare, aceasta putând face doar obiectul unui contract de schimb. Rămâne de văzut care vor fi consecințele juridice ale acestei distincții prin raportare la prevederile art. 239 alin. (2) C.pen. (abuzul de încredere prin fraudarea creditorilor), potrivit cărora constituie infracțiune fapta persoanei care achiziționează bunuri ori servicii știind că nu va putea plăti[45)].

Criticabil, din punctul nostru de vedere, este faptul că în conținutul art. 180 C.pen. a fost inclusă în definiția „mijlocului de plată fără numerar" (denumirea marginală a art. 180 C.pen.) atât instrumentul

[45)] Ipoteza problematică ar fi următoarea: X „achiziționează" un produs de la un comerciant folosind un card prin intermediul căruia poate transfera monedă virtuală. În realitate, X nu deține cuantumul necesar de monedă virtuală pentru „achiziționarea" produsului respectiv, dar, până la procesarea tranzacției, este necesar să treacă un interval de timp ce îi permite lui X să părăsească locația respectivă. Dincolo de faptul că, într-o asemenea ipoteză, s-ar putea pune inclusiv problema reținerii infracțiunii de înșelăciune, putându-se susține că există o conduită comisivă de inducere în eroare a comerciantului, este discutabil în ce măsură ar putea fi reținute elementele constitutive ale art. 239 alin. (2) C.pen.

de plată fără numerar [alin. (1)], cât și instrumentul de plată electronică [alin. (2)]. Această abordare nu o regăsim în Directiva (UE) 2019/713 și este discutabilă, în contextul în care scopul acestei intervenții legislative ar fi trebuit să fie, în principal, înlocuirea instrumentului de plată electronică cu instrumentul de plată fără numerar, adică un concept mai larg care să includă atât instrumentul de plată electronică, cât și monedele virtuale. Nu credem că s-ar putea susține că menținerea instrumentului de plată electronică în cuprinsul art. 180 C.pen.se datorează faptului că doar așa s-ar fi transpus în mod adecvat prevederile art. 2 lit. (c) din directivă în dreptul intern. Art. 2 lit. (c) din directivă nu se referă la instrumentele de plată electronică în general, ci la mijloacele digitale de schimb, care includ doar moneda electronică (doar acestea având legătură cu instrumentul de plată electronică) și moneda virtuală. În realitate, instrumentul de plată electronică este absorbit în definiția „instrumentului de plată fără numerar" de la art. 2 lit. (a) din directivă.

Având în vedere că moneda electronică o regăsim atât în definiția „instrumentului de plată fără numerar", cât și în definiția „instrumentului de plată electronică", avem rezerve că, la nivelul practicii judiciare, se va putea face distincția dintre cele două mijloace (nu instrumente) de plată fără numerar. Se pune, așadar, problema de a stabili în ce măsură discutăm despre o dihotomie sau doar despre o tehnică legislativă deficitară. Apreciem ca fiind mult prea complicat să ne raportăm la un mijloc de plată fără numerar (denumirea marginală a art. 180 C.pen.), care include instrumentul de plată fără numerar (distincția dintre „mijloc" și „instrument" fiind de o subtilitate deosebită), instrumentul de plată electronică, moneda electronică și moneda virtuală. Iar pentru a complica lucrurile și mai mult, moneda electronică este menționată atât în definiția „instrumentului de plată fără numerar", cât și în definiția „instrumentului de plată electronică", fără să fie însă evident în ce măsură instrumentul de plată fără numerar include instrumentul de plată electronică (*sic!*).

De altfel, maniera de reglementare a art. 180 C.pen. pare să fi generat confuzie la momentul elaborării proiectului de act normativ, din moment ce în cuprinsul art. 250 C.pen. nu se face trimitere la instrumentul de plată electronică [definit în cuprinsul art. 180 alin. (2) C.pen.], ci doar la instrumentul de plată fără numerar [definit în cuprinsul art. 180 alin. (1) C.pen.][46]. O asemenea trimitere ar putea ridica probleme, în contextul în care în art. II din Proiectul de Lege se precizează faptul că, ori de câte ori în Codul de procedură penală se utilizează sintagma „instrument de plată electronică", referirea se consideră făcută la „mijloc [nu instrument – n.n.] de plată fără numerar" (*sic!*).

2. Observații referitoare la modificarea art. 250 alin. (1) C.pen. – efectuarea de operațiuni financiare în mod fraudulos

Art. 250 alin. (1) C.pen. – forma actuală	Art. 250 alin. (1) C.pen. – forma din Proiectul de Lege
Efectuarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utilizarea, fără consimțământul titularului, **a unui instrument de plată electronică** sau a datelor de identificare care permit utilizarea acestuia, se pedepsește cu închisoarea de la 2 la 7 ani.	Efectuarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, valoare monetară sau monedă virtuală, prin utilizarea, fără consimțământul titularului, **a unui instrument de plată fără numerar** sau a datelor de identificare care permit utilizarea acestuia, se pedepsește cu închisoarea de la 2 la 7 ani.

[46] Aceasta dacă nu cumva legiuitorul național a dorit să se raporteze la denumirea marginală a art. 180 C.pen., dar, din eroare, a făcut trimitere la instrumentul de plată fără numerar, și nu la mijlocul de plată fără numerar, care include atât instrumentul de plată fără numerar, cât și instrumentul de plată electronică.

În primul rând, modificarea art. 180 C.pen. conduce *per se* la necesitatea modificării art. 250 C.pen. în vederea unei corelări din punct de vedere terminologic. Totuși, așa cum am precizat *supra* (la pct. 2), din definiția de la art. 180 C.pen. rezultă că legiuitorul a făcut o distincție între instrumentul de plată fără numerar și instrumentul de plată electronică.

Dacă o asemenea distincție este una reală, fără să rezulte în mod artificial din maniera defectuoasă de redactare a art. 180 C.pen., atunci înlocuirea instrumentului de plată electronică cu instrumentul de plată fără numerar în cuprinsul art. 250 alin. (1) C.pen. devine problematică. Eventual, modificarea art. 250 alin. (1) C.pen. trebuie să fie în sensul de a se face trimitere atât la instrumentul de plată fără numerar, cât și la instrumentul de plată electronică ori de a se raporta la denumirea marginală a art. 180 C.pen., și anume „Mijloace de plată fără numerar".

Pe de altă parte, credem că textul de incriminare ar fi fost mult mai ușor de înțeles în măsura în care acesta s-ar fi rezumat la „utilizarea, fără drept, a unui instrument de plată electronică ori a unui instrument de plată fără numerar (sau, generic, a unui mijloc de plată fără numerar) sau a datelor de identificare care permit utilizarea acestora (acestuia)". Susținem acest lucru, deoarece actul material incriminat generic (utilizarea) ar fi putut să fie interpretat prin prisma definițiilor regăsite în cuprinsul art. 180 C.pen.

Apreciem, așadar, că **ar fi suficientă incriminarea generică a utilizării fără drept a acestor mijloace de plată fără numerar**[47]. Nu putem ignora faptul că în cuprinsul art. 250[1] C.pen. se face vorbire în mod repetat despre scopul special al „utilizării frauduloase a unui instrument de plată fără numerar", fiind omisă enumerarea modalităților alternative prevăzute la art. 250 alin. (1) C.pen. Or, în măsura în care s-a apreciat că sintagma „utilizarea frauduloasă a instrumentului de plată fără numerar" respectă întru totul exigențele principiului legalității incriminării, nu vedem de ce nu s-a procedat în mod similar și în ceea ce privește art. 250 alin. (1) C.pen. în vederea simplificării laturii obiective.

De altfel, faptul că această utilizare a instrumentului de plată fără numerar poate implica o retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori a unui transfer de fonduri, a unei valori monetare sau a unei monede virtuale rezultă cu evidență din cuprinsul art. 180 C.pen. De asemenea, observăm că prin art. 3 din Directiva (UE) 2019/713 se creează în sarcina legiuitorului național obligația pozitivă de a incrimina două tipuri de conduite: „utilizarea frauduloasă a unui instrument de plată fără numerar care a fost fie furat, fie însușit sau obținut pe alte căi ilegale" [lit. (a)] și „utilizarea frauduloasă a unui instrument de plată fără numerar contrafăcut sau falsificat" [lit. (b)]. Prin urmare, inclusiv legiuitorul a avut în vedere conduita generică de a „utiliza în mod fraudulos" un instrument de plată fără numerar, evitând să recurgă la enumerarea unor modalități alternative care să fie subsumate acestei utilizări.

Nu în ultimul rând, apreciem că teza finală a art. 250 alin. (1) C.pen. [„utilizarea (...) datelor de identificare care permit utilizarea acestuia"] nu ține cont de specificul monedelor virtuale. Avem serioase rezerve că, în ceea ce privește moneda virtuală, putem discuta despre date de identificare care permit utilizarea acesteia în mod fraudulos. Această teză de incriminare are în vedere utilizarea datelor de identificare a unui instrument de plată electronică (în concret, datele unui card bancar) în vederea efectuării unor plăți pe Internet. Nu vedem însă cum am putea extinde această teză la utilizarea monedelor virtuale. Cunoașterea adresei publice din *blockchain* (adică echivalentul datelor de identificare a unui instrument de plată electronică), unde sunt stocate monedele virtuale, devine irelevantă din perspectiva utilizării instrumentului de plată fără numerar în vederea efectuării unei tranzacții.

[47] Observăm că se oscilează în cuprinsul textelor de incriminare între sintagmele „utilizarea frauduloasă" și „utilizare fără consimțământul (titularului)". Aceasta este o eroare de tehnică legislativă, fiind imperios necesar ca legiuitorul să se raporteze în mod unitar la utilizarea fără drept, utilizarea frauduloasă sau utilizarea fără consimțământul titularului mijlocului de plată fără numerar.

3. Observații referitoare la introducerea art. 250[1] C.pen. – operațiuni ilegale cu instrumente de plată fără numerar

Prin Proiectul de Lege se urmărește introducerea unui nou text de incriminare, acesta urmând a avea următorul conținut:

„Art. 250[1]. Operațiuni ilegale cu instrumente de plată fără numerar

(1) Deținerea în vederea utilizării frauduloase a unui instrument de plată fără numerar însușit prin săvârșirea uneia dintre faptele prevăzute la art. 228, art. 229, art. 233-236, art. 238, art. 239 și art. 295 se pedepsește cu închisoarea de la 2 la 7 ani.

(2) Dobândirea pentru sine sau pentru altul, inclusiv prin primire, însușire[48)] cumpărare sau ca urmare unei operațiuni precum transferul, importul, exportul, vânzarea, transportul, distribuirea sau punerea la dispoziție în vederea utilizării frauduloase a unui instrument de plată fără numerar obținut prin săvârșirea uneia dintre faptele prevăzute la art. 228, art. 229, art. 233-236, art. 238, art. 239 și art. 295 se pedepsește cu închisoarea de la 2 la 7 ani.

(3) Fabricarea, producerea, primirea, deținerea, transmiterea sau punerea la dispoziție a unui dispozitiv, instrument, date informatice, echipamente, inclusiv hardware sau software, ori a oricăror alte mijloace, cu scopul de a servi la însușirea unui instrument de plată fără numerar prin săvârșirea uneia dintre faptele prevăzute la art. 228, art. 229, art. 233-236, art. 238, art. 239 si art. 295, se pedepsește cu închisoarea de la 2 la 7 ani.

(4) Cu pedeapsa prevăzută la alin. (3) se sancționează și dobândirea pentru sine sau pentru altul, inclusiv prin importul, exportul, vânzarea, transportul sau distribuția unui dispozitiv, instrument, date informatice, echipamente, inclusiv hardware ori software, sau a oricăror alte mijloace cu scopul de a servi la însușirea unui instrument de plată fără numerar prin săvârșirea uneia dintre faptele prevăzute la art. 228, art. 229, art. 233-236, art. 238, art. 239 și art. 295”.

În primul rând, propunerea de a incrimina aceste conduite, care, din punct de vedere conceptual, reprezintă acte de pregătire realizate în scopul comiterii altor infracțiuni în legătură cu instrumentul de plată fără numerar, se datorează prevederilor art. 4[49)], art. 5 și art. 7 din Directiva (UE) 2019/713. Având în vedere că unele dintre aceste conduite nu sunt incriminate *de lege lata*, o intervenție a legiuitorului național era necesară.

Avem totuși unele rezerve cu privire la conținutul art. 250[1] C.pen., în forma adoptată de către Senat. Dincolo de faptul că trimiterea exclusivă la instrumentul de plată fără numerar evidențiază aceleași critici precum cele învederate *supra* (la pct. 3), acest text de incriminare autonom prezintă inclusiv alte neajunsuri.

***i.* Referitor la conținutul art. 250[1] alin. (1) C.pen.** Potrivit art. 4 lit. (c) din directivă, ar trebui să constituie infracțiune „posesia în vederea utilizării frauduloase a unui instrument de plată fără numerar material, furat sau însușit pe alte căi ilegale, sau contrafăcut sau falsificat”. Discutăm, așadar, despre incriminarea posesiei (deținerii) atunci când este identificat un scop special (în vederea utilizării frauduloase) și situația premisă constă în obținerea instrumentului de plată fără numerar prin mijloace ilegale ori prin falsificare/contrafacere.

48) Aici ar fi fost necesară introducerea unei virgule (*sic!*).

49) Art. 4 din Directiva (UE) 2019/713 era parțial transpus în dreptul național. Astfel, furtul sau însușirea în alt mod ilegal a unui instrument de plată fără numerar material [lit. (a)] se află și *de lege lata* sub incidența a numeroase texte de incriminare. Lipsa unei mențiuni cu privire la instrumentul de plată fără numerar în cuprinsul art. 228, art. 229, art. 233, art. 234, art. 295 C.pen. etc. nu vedem ca fiind problematică din perspectiva transpunerii adecvate a acestei directive. De asemenea, contrafacerea sau falsificarea frauduloasă a unui instrument de plată fără numerar material [lit. (b)] se află deja sub incidența art. 311 alin. (2) C.pen., atunci când ne raportăm la un instrument de plată electronică.

Observăm, în primul rând, faptul că prin art. 250[1] alin. (1) C.pen. se acoperă doar prima teză avută în vedere de art. 4 lit. (c) din directivă. Astfel, **nu este acoperită de această variantă de incriminare deținerea de instrumente de plată fără numerar contrafăcute ori falsificate**. Cu toate că s-ar putea argumenta că o asemenea conduită intră sub incidența art. 313 alin. (1) C.pen., trebuie remarcat că acest din urmă text de incriminare acoperă doar deținerea valorilor falsificate prevăzute în art. 310-312 C.pen. în scopul punerii în circulație a acestora.

Sub acest aspect, necesită a fi clarificate două chestiuni:

- în primul rând, necesită lămurit în ce măsură „valorile falsificate" la care se referă art. 313 C.pen. acoperă și instrumentele de plată fără numerar. Având în vedere că, prin modificarea art. 313 C.pen., denumirea marginală a acestei infracțiuni urmează să fie „Punerea în circulație de valori falsificate sau dobândirea de instrumente de plată fără numerar falsificate", s-ar putea argumenta că trimiterea generică la art. 310-312 C.pen., făcută în cuprinsul art. 313 alin. (1) C.pen., vizează, în realitate, doar valorile menționate la art. 311 alin. (1) C.pen., fără a avea în vedere și instrumentele de plată fără numerar;

- în al doilea rând, necesită lămurit în ce măsură utilizarea unui instrument de plată fără numerar în oricare dintre modalitățile prevăzute la art. 250 alin. (1) C.pen. echivalează cu o punere în circulație.

Nu poate fi ignorat nici faptul că, în baza unei interpretări *per a contrario* a art. 313 alin. (2) C.pen., autorul ori participantul la infracțiunea prevăzută la art. 311 alin. (2) C.pen. nu va răspunde pentru infracțiunea de punere în circulație de valori falsificate în modalitatea deținerii[50)].

De asemenea, nu credem că deținerea instrumentului de plată fără numerar în scopul utilizării frauduloase a acestuia va intra sub incidența art. 313 alin. (4) C.pen. (în varianta modificată). Art. 313 alin. (4) C.pen. se referă doar la dobândirea în diverse modalități a instrumentului de plată fără numerar, fără a acoperi deținerea acestuia. Este adevărat faptul că, ulterior dobândirii instrumentului de plată fără numerar, putem discuta despre o deținere, aceasta putând fi o consecință naturală a dobândirii. Nu este totuși exclus ca deținerea să aibă ca situație premisă inclusiv o altă ipoteză decât cea avută în vedere la art. 313 alin. (4) C.pen. Un exemplu în acest sens ar fi deținerea unui instrument de plată electronică găsit pe stradă.

Cu privire la prima teză a art. 250[1] alin. (1) C.pen., este discutabil în ce măsură enumerarea exhaustivă a infracțiunilor prin intermediul cărora se realizează însușirea instrumentului de plată fără numerar nu va conduce la o restrângere nedorită a sferei de aplicabilitate a textului de incriminare. Este lesne de observat faptul că legiuitorul a dorit un plus de previzibilitate, sintagma „furat sau însușit pe alte căi ilegale" din cuprinsul art. 4 lit. (c) din directivă fiind probabil apreciată ca fiind una necorespunzătoare.

Cu toate acestea, credem că un instrument de plată fără numerar poate să fie obținut inclusiv pe alte căi ilegale decât cele avute în vedere de infracțiunile la care se face trimitere în cuprinsul art. 250[1] alin. (1) C.pen. Ne referim aici la însușirea bunului găsit sau ajuns din eroare la făptuitor (art. 243 C.pen.) sau la o eventuală înșelăciune (art. 244 C.pen.). Ne scapă motivele pentru care aceste infracțiuni nu au fost apreciate de către legiuitor ca fiind o modalitate ilegală de obținere a unui instrument de plată fără numerar.

De asemenea, observăm că, în cuprinsul art. 250[1] alin. (1) C.pen., legiuitorul se raportează doar la noțiunea de „însușire"[51)], fără să fie foarte clar în ce măsură aceasta are un înțeles autonom în raport cu alte texte de incriminare. Spre exemplu, art. 295 C.pen. (delapidarea) prevede modalități alternative precum însușirea, folosirea sau traficarea. De asemenea, art. 238 C.pen. (abuzul de încredere) acoperă conduite precum însușirea, dispunerea, folosirea sau refuzul de restituire. Intră, așadar, sub incidența art. 250[1] alin. (1)

[50)] A se vedea, în acest sens, *C. Rotaru*, Comentariu, în C. Rotaru, A.-R. Trandafir, V. Cioclei, Drept penal. Partea specială II, ed. 4, Ed. C.H. Beck, București, 2020, pp. 347-348.

[51)] Cu toate că la art. 250[1] alin. (2) C.pen. se face trimitere la noțiunea de „obținere", și nu la cea de „însușire".

C.pen. conduita făptuitorului de a deține un instrument de plată fără numerar obținut prin comiterea unei infracțiuni de abuz de încredere în modalitatea refuzului de restituire, și nu în cea de însușire? Apreciem că răspunsul este unul incert.

Nu în ultimul rând, așa cum am precizat *supra* (la pct. 2), găsim ca fiind interesantă trimiterea făcută în mod repetat în cuprinsul art. 250[1] C.pen. la scopul „utilizării frauduloase a unui instrument de plată fără numerar". Astfel, nu s-a recurs la o normă de trimitere, în sensul menționării în cuprinsul art. 250[1] C.pen. că scopul special este cel de a săvârși faptele prevăzute la art. 250 alin. (1) C.pen.[52)]. Din contră, s-a apreciat că sintagma „utilizarea frauduloasă a unui instrument de plată fără numerar" înglobează conduitele incriminate la art. 250 alin. (1) C.pen. Or, o asemenea abordare nu denotă decât faptul că inclusiv conținutul art. 250 alin. (1) C.pen. putea să fie simplificat prin utilizarea aceleiași sintagme.

***ii.* Referitor la conținutul art. 250[1] alin. (2) C.pen.** Potrivit art. 4 lit. (d) din directivă, ar trebui să constituie infracțiune „achiziția în folosul propriu sau al unei alte persoane, inclusiv primirea, însușirea, cumpărarea, transferul, importul, exportul, vânzarea, transportul sau distribuirea în vederea utilizării frauduloase a unui instrument de plată fără numerar material, furat, contrafăcut sau falsificat".

În primul rând, art. 250[1] alin. (2) C.pen. acoperă doar prima teză avută în vedere de art. 4 lit. (d) din directivă. Se mențin, sub acest aspect, observațiile făcute *supra* (la pct. *i*) referitoare la aplicabilitatea art. 313 C.pen. De asemenea, se mențin observațiile făcute *supra* referitoare la lista exhaustivă de infracțiuni. Observăm totuși o diferență de abordare, deoarece în cuprinsul art. 250[1] alin. (2) C.pen. nu se mai face trimitere la „însușirea" instrumentului de plată electronică, ci la „obținerea" acestuia prin săvârșirea uneia dintre infracțiunile enumerate în mod exhaustiv. Credem că această lipsă de corelare terminologică ar putea reprezenta un argument suplimentar în susținerea unei interpretări restrictive a art. 250[1] alin. (1) C.pen.[53)].

Nu în ultimul rând, apreciem că s-a exagerat prin enumerarea tuturor modalităților prevăzute la art. 250[1] alin. (2) C.pen., o parte dintre aceste modalități fiind redundante. Aceasta, dincolo de faptul că, lecturând conținutul textului de incriminare, am ajuns să descoperim că dobândirea poate avea loc prin cumpărare sau printr-o operațiune de... vânzare (*sic!*). Poate ar fi totuși momentul ca, atunci când se apelează la enumerarea modalităților alternative de comitere a unei infracțiuni, să se verifice în ce măsură există o corelare cu alte texte de incriminare.

Sub acest aspect, observăm că în cuprinsul art. 250[1] alin. (2) C.pen. se face vorbire despre primire și cumpărare, în vreme ce, în cuprinsul art. 374 alin. (1) C.pen. (pornografia infantilă), legiuitorul a considerat suficient să se raporteze la modalitatea procurării. Folosirea unor noțiuni diferite – pentru a exprima același lucru – în cadrul aceluiași text de incriminare ori în texte de incriminare diferite denotă fie o nesiguranță a legiuitorului, fie o neglijență crasă a acestuia în procesul de legiferare.

***iii.* Referitor la conținutul art. 250[1] alin. (3)-(4) C.pen.** Potrivit art. 7 din directivă, ar trebui să constituie infracțiune „producerea, achiziționarea în folos propriu sau al unei alte persoane, inclusiv importul, exportul, vânzarea, transportul sau distribuția, sau punerea la dispoziție a unui dispozitiv sau a unui instrument, a unor date informatice sau a oricăror alte mijloace concepute în principal sau adaptate special în scopul săvârșirii uneia dintre infracțiunile menționate la articolul 4 literele (a) și (b), la articolul 5 literele (a) și (b) sau la articolul 6, cel puțin atunci când sunt săvârșite cu intenția ca aceste mijloace să fie folosite".

[52)] Potrivit art. 16 alin. (1) din Legea nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative (republicată în M. Of. nr. 260 din 21 aprilie 2010), pentru sublinierea unor conexiuni legislative se utilizează norma de trimitere.

[53)] Potrivit art. 37 alin. (1) din Legea nr. 24/2000, republicată, „în limbajul normativ aceleași noțiuni se exprimă numai prin aceiași termeni".

În mod evident, legiuitorul european s-a raportat inclusiv la conduite care vizează instrumentele de plată fără numerar nemateriale ce ar putea fi obținute prin comiterea unor infracțiuni informatice prevăzute la art. 3-6 din Directiva 2013/40/UE. Legiuitorul român a restrâns însă sfera de aplicabilitate a art. 250[1] alin. (3)-(4) C.pen. doar la instrumentele de plată fără numerar materiale, din moment ce se raportează doar la conduite realizate cu scopul de a însuși un instrument de plată fără numerar prin săvârșirea unei fapte prevăzute la art. 228, art. 229, art. 233-236, art. 238, art. 239 și art. 295 C.pen.

O asemenea restrângere ar putea fi apreciată ca fiind justificată, având în vedere prevederile art. 365 C.pen., care se raportează la scopul comiterii unei infracțiuni prevăzute la art. 360-364 C.pen. Credem totuși că discutăm din nou despre o lipsă de corelare legislativă, observațiile făcute *supra* (la pct. *ii*) referitoare la lista exhaustivă de infracțiuni fiind valabile inclusiv în ceea ce privește art. 250[1] alin. (3)-(4) C.pen.

De asemenea, rămân valabile criticile făcute *supra* cu privire la redundanța unora dintre modalitățile alternative enumerate în cuprinsul normei de incriminare. De ce era oare necesar să se facă trimitere în cuprinsul art. 250[1] alin. (3) C.pen. atât la modalitatea fabricării, cât și la modalitatea producerii, în contextul în care în cuprinsul art. 365 alin. (1) C.pen. se face trimitere doar la modalitatea producerii? De asemenea, de ce era necesar să se facă trimitere în cuprinsul art. 250[1] alin. (3)-(4) C.pen. la dispozitive, instrumente, date informatice și echipamente, inclusiv hardware și software, în contextul în care art. 365 C.pen. se raportează doar la dispozitive (ce includ atât instrumentele materiale, cât și echipamentele hardware) și date informatice (ce includ atât instrumentele nemateriale, cât și echipamentele software)? Faptul că legiuitorul european recurge la enumerarea unor noțiuni care au același înțeles nu implică faptul că legiuitorul național trebuie să procedeze de aceeași manieră. Rațiunea pentru care legiuitorul european recurge la o asemenea tehnică legislativă este pentru a oferi statelor membre posibilitatea de a transpune în dreptul intern acea terminologie care se corelează și este compatibilă cu restul dispozițiilor legale.

4. Observații referitoare la modificarea art. 249 C.pen. – frauda informatică

Prin modificarea propusă urmează să fie introdusă o modalitate alternativă suplimentară de comitere a fraudei informatice, și anume transmiterea de date informatice. În Expunerea de motive a acestui proiect de act normativ s-a precizat faptul că: „întrucât prevederile art. 249 C.pen. nu conțin modalitatea de săvârșire a faptei sub forma transmiterii de date informatice, deși strict tehnic, transmiterea poate fi inclusă în modalitatea introducerii de date informatice, pentru evitarea unei interpretări neunitare a art. 249 C.pen., prin raportare la toate variantele elementului material al infracțiunii, detaliate în art. 6 din Directiva non-cash, s-a apreciat că norma de incriminare din dreptul național trebuie completată în mod corespunzător”[54].

În ceea ce ne privește, ne menținem punctul de vedere potrivit căruia „o transmitere de date informatice într-un sistem informatic poate lua forma unei introduceri de date informatice. Astfel, atunci când discutăm despre transferarea datelor informatice din sursa A în sursa B, discutăm implicit despre o introducere a respectivelor date informatice în sursa B. Sub acest aspect, trimiterea la această modalitate poate fi apreciată ca fiind redundantă”[55].

Riscul este acela de a se interpreta, la nivelul practicii judiciare, că introducerea acestei modalități suplimentare de comitere a fraudei informatice conduce la o extindere a sferei de aplicabilitate a acesteia, cu efecte doar pentru viitor. Or, o asemenea concluzie ar însemna că transferul de date informatice efectuat anterior intervenției legislative nu poate intra sub incidența fraudei informatice.

[54] A se vedea, în acest sens, Expunerea de motive, disponibilă pe pagina *http://www.cdep.ro/proiecte/2021/100/60/2/em188.pdf* (ultima accesare la data de 2 iunie 2021).

[55] A se vedea, în acest sens, *G. Zlati*, Critici punctuale..., cit. *supra*, *passim*. A se vedea și analiza făcută în *idem*, Tratat..., vol. 1, op. cit., p. 376.

C. Directiva 2011/93/UE privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile[56)]

Această directivă a înlocuit Decizia-cadru 2004/68/JAI privind combaterea exploatării sexuale a copiilor și a pornografiei infantile[57)]. Este important de precizat faptul că, din punct de vedere cronologic, textele de incriminare aferente pornografiei infantile prin sisteme informatice s-au raportat inițial la prevederile din Convenția privind criminalitatea informatică (art. 9), iar ulterior la Decizia-cadru 2004/68/JAI (art. 3) și Directiva 2011/93/UE (art. 5).

Sfera de aplicabilitate a infracțiunii de pornografie infantilă prin sisteme informatice a suferit în timp următoarele modificări[58)]:

***i.* Infracțiunea de pornografie infantilă în Legea nr. 161/2003.** Inițial, prin art. 51 din Legea nr. 161/2003 era incriminată „producerea în vederea răspândirii, oferirea sau punerea la dispoziție, răspândirea sau transmiterea, procurarea pentru sine sau pentru altul de materiale pornografice cu minori prin sisteme informatice ori deținerea, fără drept, de materiale pornografice cu minori într-un sistem informatic sau un mijloc de stocare a datelor informatice".

De asemenea, „materialele pornografie cu minori" erau definite, în cuprinsul art. 35 alin. (1) lit. i) din Legea nr. 161/2003, ca fiind „orice material care prezintă un minor având un comportament sexual explicit sau o persoană majoră care este prezentată ca un minor având un comportament sexual explicit ori imagini care, deși nu prezintă o persoană reală, simulează, în mod credibil, un minor având un comportament sexual explicit".

Înainte de intrarea în vigoare a noului Cod penal, art. 51 din Legea nr. 161/2003 nu era singurul text de incriminare cu privire la pornografia infantilă. În legislația specială se putea identifica, de asemenea, o incriminare a pornografiei infantile în art. 18 din Legea nr. 678/2001 privind prevenirea și combaterea traficului de persoane[59)] și în art. 11 din Legea nr. 196/2003 privind prevenirea și combaterea pornografiei[60)].

***ii.* Infracțiunea de pornografie infantilă în noul Cod penal.** Ulterior, la intrarea în vigoare a noului Cod penal, infracțiunile de pornografie infantilă au fost preluate și grupate în cuprinsul art. 374 C.pen.

Inițial, faptele incriminate de art. 374 C.pen. erau: „producerea, deținerea în vederea expunerii sau distribuirii, achiziționarea, stocarea, expunerea, promovarea, distribuirea, precum și punerea la dispoziție, în orice mod, de materiale pornografice cu minori". De asemenea, potrivit art. 374 alin. (3) C.pen., constituie infracțiune inclusiv „accesarea, fără drept, de materiale pornografice cu minori, prin intermediul sistemelor informatice sau altor mijloace de comunicații electronice".

[56)] Publicată în J. Of., seria L, nr. 335/1 din 17 decembrie 2011.

[57)] Publicată în J. Of., seria L, nr. 013/44 din 20 ianuarie 2004.

[58)] Pentru o analiză comparativă între art. 51 din Legea nr. 161/2003 și art. 374 C.pen., se poate vedea și *S. Bogdan, D.A. Șerban, G. Zlati*, Noul Cod penal. Partea specială. Perspectiva clujeană, Ed. Universul Juridic, București, 2014, pp. 723-727. De asemenea, pentru o analiză a infracțiunii de pornografie infantilă, se poate vedea: *O. Bugnar*, Pornografia infantilă. Legiuitorul european *versus* legiuitorul național, în Caiete de drept penal nr. 3/2014, p. 40 și urm.; *I.-A. Măhălean*, Transpunerea Directivei 2011/93/UE a Parlamentului și a Consiliului privind combaterea abuzului sexual a copiilor, a exploatării sexuale a copiilor și a pornografiei infantile în legislația națională, în Caiete de drept penal nr. 3/2014, p. 61 și urm.; *R.B. Teslovan*, Pornografia infantilă. O perspectivă asupra incriminării faptei în modalitățile deținerii și accesării corelate cu pseudopornografia și pornografia virtuală, în Caiete de drept penal nr. 2/2015, p. 122 și urm.; *A. Mărgineanu*, Combaterea exploatării sexuale a copiilor și a pornografiei infantile, în Caiete de drept penal nr. 3/2013, p. 63 și urm.; *M.-K. Guiu*, Pornografia infantilă, în Dreptul nr. 7/2016, p. 77 și urm.

[59)] Publicată în M. Of. nr. 783 din 11 decembrie 2001.

[60)] Republicată în M. Of. nr. 87 din 4 februarie 2008. Ulterior intrării în vigoare a noului Cod penal, această lege a fost din nou republicată în M. Of. nr. 198 din 20 martie 2014.

Comparând conținutul art. 51 din Legea nr. 161/2003 cu forma inițială a art. 374 C.pen., se pot observa următoarele diferențe:

- spre deosebire de art. 51 din Legea nr. 161/2003, art. 374 C.pen. sancționa simpla producere de materiale pornografice cu minori fără să fie necesară probarea unui scop special, și anume răspândirea acestor materiale. Discutăm, sub acest aspect, despre o extindere a sferei de aplicabilitate a textului de incriminare;

- pe de altă parte, potrivit art. 374 C.pen., deținerea de materiale pornografice cu minori era incriminată doar dacă aceasta se realiza în scopul expunerii sau distribuirii materialelor. Având în vedere că art. 51 din Legea nr. 161/2003 nu raporta modalitatea deținerii la un anumit scop special[61], nu este exclusă posibilitatea de a discuta despre o dezincriminare parțială la momentul intrării în vigoare a noului Cod penal;

- accesarea materialelor pornografice cu minori prin intermediul sistemelor informatice a fost incriminată abia ulterior intrării în vigoare a noului Cod penal, ca o consecință a transpunerii în dreptul intern a prevederilor art. 5 din Directiva 2011/93/UE. Sub acest aspect, discutăm din nou despre o extindere a sferei de aplicabilitate a textului de incriminare.

De asemenea, definiția „materialelor pornografice cu minori" din cuprinsul art. 374 alin. (4) C.pen. (în forma existentă la data intrării în vigoare a noului Cod penal) prezenta o deosebire relevantă în raport cu definiția „materialelor pornografice cu minori" din cuprinsul art. 35 alin. (1) lit. i) din Legea nr. 161/2003.

Definiția „materialelor pornografice cu minori" din Legea nr. 161/2003	**Definiția „materialelor pornografice cu minori" din noul Cod penal**
Orice material care prezintă un minor având un comportament sexual explicit sau **o persoană majoră care este prezentată ca un minor** având un comportament sexual explicit ori imagini care, deși nu prezintă o persoană reală, simulează, în mod credibil, un minor având un comportament sexual explicit.	Orice material care prezintă un minor având un comportament sexual explicit sau care, deși nu prezintă o persoană reală, simulează, în mod credibil, un minor având un astfel de comportament.

După cum rezultă din tabelul comparativ, la data intrării în vigoare a noului Cod penal, prezentarea unei persoane majore drept un minor având un comportament sexual explicit nu mai intra în accepțiunea materialelor pornografice cu minori. Cu alte cuvinte, modificarea definiției „materialelor pornografice cu minori" a avut drept consecință o dezincriminare parțială. Această alegere a legiuitorului român s-a datorat prevederilor art. 5 alin. (7) din Directiva 2011/93/UE, potrivit cărora „statele membre decid dacă dispozițiile prezentului articol se aplică cazurilor care implică pornografie infantilă, astfel cum sunt menționate la articolul 2 litera (c) punctul (iii), în care o persoană care pare a fi un copil are în realitate 18 ani sau mai mult la data reprezentării sale pe materialele respective".

***iii.* Infracțiunea de pornografie infantilă în noul Cod penal, ulterior modificării acesteia prin O.U.G. nr. 18/2016[62]**

Art. 374 C.pen. a suferit unele modificări de la data intrării în vigoare a noului Cod penal, modificări ce necesită a fi avute în vedere atunci când se analizează aplicarea în timp a legii penale. Printre modificările aduse de O.U.G. nr. 18/2016, se regăsesc următoarele:

[61] Precizăm totuși că deținerea de materiale pornografice în vederea răspândirii acestora putea intra inclusiv sub incidența art. 18 din Legea nr. 678/2001 privind prevenirea și combaterea traficului de persoane, abrogat în prezent.

[62] Publicată în M. Of. nr. 389 din 23 mai 2016.

- s-a renunțat la scopul special în ceea ce privește modalitatea deținerii. Prin urmare, de la data publicării în Monitorul Oficial a O.U.G. nr. 18/2016 (23 mai 2016), simpla deținere de materiale pornografice (inclusiv pentru uz personal) constituie infracțiune;

- s-a incriminat inclusiv vizionarea de spectacole pornografice în cadrul cărora participă un minor [art. 374 alin. (1^2) C.pen.]. Potrivit art. 374 alin. (4^1) C.pen., prin „spectacol pornografic" se înțelege „expunerea în direct adresată unui public, inclusiv prin tehnologia informațiilor și comunicațiilor, a unui copil implicat într-un comportament sexual explicit ori a organelor genitale ale unui copil, cu scop sexual". Prin urmare, chiar fără a discuta despre conduita prevăzută la art. 374 alin. (3) C.pen. (accesarea, fără drept, de materiale pornografice cu minori), simpla vizualizare a unui spectacol pornografic prin intermediul unui sistem informatic constituie infracțiune. Un exemplu relevant în acest sens ar fi vizualizarea unui *live stream* cu caracter pornografic, fără ca acesta să fie inițiat de către făptuitor;

- definiția „materialelor pornografice cu minori" a fost, de asemenea, extinsă, fiind inclusă atât teza prezentării unui major ca fiind un minor (teză de incriminare la care s-a renunțat la data intrării în vigoare a noului Cod penal), cât și teza reprezentării organelor genitale ale unui copil, cu scop sexual (nu doar prezentarea unui comportament sexual explicit).

Discutăm în context despre o extindere semnificativă a textului de incriminare, atât din perspectiva modalităților de comitere a pornografiei infantile, cât și în ceea ce privește definiția „materialelor pornografice cu minori".

III. Dezlegări de drept și recursuri în interesul legii

În ciuda existenței unei practici judiciare neunitare cu privire la multiple infracțiuni ce intră în sfera criminalității informatice, până recent, puteam discuta despre o singură hotărâre pentru unificarea practicii judiciare. Ne referim aici la Decizia nr. 15/2013[63] a ICCJ, prin care a fost soluționat un recurs în interesul legii cu privire la interpretarea dispozițiilor art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003 [*de lege lata*, art. 360 C.pen.].

Recent însă, Înalta Curte de Casație și Justiție s-a pronunțat prin Decizia nr. 4/2021[64] cu privire la dezlegarea unei chestiuni de drept referitoare la raportul dintre crearea de conturi false pe rețelele de socializare și reținerea infracțiunii de fals informatic [a se vedea *infra*, la pct. B]. De asemenea, Înalta Curte de Casație și Justiție a fost sesizată de către Curtea de Apel Alba Iulia în vederea dezlegării unei chestiuni de drept cu privire la raportul dintre infracțiunea de înșelăciune și frauda informatică [a se vedea *infra*, la pct. C].

A. Recursul în interesul legii soluționat prin Decizia ICCJ nr. 15/2013

În esență, recursul în interesul legii a urmărit interpretarea unitară a noțiunii de „acces fără drept la un sistem informatic", determinat de diferențierea practică dintre următoarele două ipoteze:

[63] ICCJ, Completul competent să judece recursul în interesul legii, dec. nr. 15/2013, publicată în M. Of. nr. 760 din 6 decembrie 2013.

[64] ICCJ, Completul pentru dezlegarea unor chestiuni de drept în materie penală, dec. nr. 4/2021, publicată în M. Of. nr. 171 din 19 februarie 2021.

i. accesul prin intermediul montării la ATM a dispozitivelor de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia sau

ii. accesul produs prin folosirea la bancomat a cardului falsificat ori chiar a celui autentic, fără acordul titularului său.

În soluționarea acestui recurs în interesul legii, Înalta Curte de Casație și Justiție a statuat următoarele:

1. Montarea la bancomat a dispozitivelor autonome de citire a benzii magnetice a cardului autentic și a codului PIN aferent acestuia (skimmere, minivideocamere sau dispozitive tip tastatură falsă) constituie infracțiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003 [*de lege lata*, art. 365 C.pen.].

Concluzionând astfel, Înalta Curte de Casație și Justiție a respins teza potrivit căreia montarea la bancomat a unor dispozitive autonome de citire a benzii magnetice echivalează *per se* cu accesarea unui sistem informatic. Am apreciat dintotdeauna ca fiind de ordinul evidenței faptul că, într-o asemenea ipoteză, nu se poate reține infracțiunea de acces ilegal la un sistem informatic[65].

Construcția în plan juridic este una elementară – pentru a putea discuta despre un acces, este necesar să existe o interacțiune logică cu sistemul informatic de natură să-i confere făptuitorului posibilitatea de a exercita un control asupra funcțiilor ori/și resurselor respectivului sistem. Or, prin montarea unui skimmer la bancomat nu discutăm despre crearea premisei pentru existența unei interacțiuni logice cu bancomat. În realitate, între skimmer și bancomat nu există niciun fel de interacțiune la nivel logic, datele stocate pe instrumentul de plată electronică fiind citite și copiate prin intermediul skimmer-ului fără a fi utilizate în vreun fel funcțiile bancomatului.

Pe de altă parte, avem serioase rezerve că reținerea *de plano* a art. 365 C.pen. este corectă atunci când se montează un skimmer la bancomat, cu scopul citirii și copierii datelor stocate pe instrumentul de plată electronică. În măsura în care făptuitorul a urmărit falsificarea instrumentului de plată electronică (clonarea acestuia) și utilizarea ulterioară a acestuia în vederea retragerii de numerar de la bancomat, reținerea art. 365 C.pen. își poate găsi justificarea. Aceasta, întrucât, potrivit art. 365 C.pen., deținerea unor dispozitive în scopul săvârșirii uneia dintre faptele prevăzute la art. 360-364 C.pen. constituie infracțiune. Condiția scopului special ar fi îndeplinită în această ipoteză, având în vedere că retragerea de numerar de la bancomat utilizând un instrument de plată electronică falsificat implică un acces la un sistem informatic (a se vedea și *infra*, la pct. 2).

În schimb, în măsura în care scopul făptuitorului se limitează la obținerea datelor de identificare a instrumentului de plată electronică sau la falsificarea unui instrument de plată electronică în vederea comercializării acestuia pe piața neagră, nu credem că este îndeplinită condiția scopului special prevăzută la art. 365 C.pen. Astfel, dincolo de faptul că, *de lega lata*, nu constituie infracțiune comercializarea datelor de identificare a instrumentului de plată electronică în vederea falsificării acestuia[66], este lesne de observat că art. 365 C.pen. nu se raportează la art. 311 alin. (2) C.pen. sau la art. 250 C.pen.

2. Folosirea la bancomat a unui card bancar autentic, fără acordul titularului său, în scopul efectuării unor retrageri de numerar, constituie infracțiunea de efectuare de operațiuni financiare în mod fraudulos prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia, prevăzută de art. 27 alin. (1) din Legea nr. 365/2002 [*de lege lata*, art. 250

[65] A se vedea, în acest sens, *G. Zlati*, Tratat..., vol. 1, op. cit., p. 132; *idem*, Unele aspecte în legătură cu infracțiunile informatice din perspectiva legislației în vigoare, precum și a noului Cod penal, în Dreptul nr. 10/2012, pp. 218-221; *idem*, Greșita interpretare a accesului la un sistem informatic. Consecințe practice, *passim*, material disponibil pe pagina *juridice.ro*.

[66] Exceptând situația în care putem discuta despre o participație penală în raport cu art. 311 alin. (2) C.pen. În rest, potrivit art. 250 alin. (3) C.pen., constituie infracțiune transmiterea datelor de identificare a unui instrument de plată electronică în scopul comiterii faptelor prevăzute la alin. (1).

alin. (1) C.pen.], în concurs ideal cu infracțiunea de acces, fără drept, la un sistem informatic, comisă în scopul obținerii de date informatice prin încălcarea măsurilor de securitate, prevăzută de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003 (*de lege lata*, art. 360 C.pen.).

Încadrarea juridică în această ipoteză este corectă, rezervele noastre vizând în mod exclusiv reținerea unui concurs ideal, și nu a unui concurs real de infracțiuni[67]. În rest, suntem întru totul de acord că utilizarea unui card bancar autentic, fără acordul titularului său, în scopul efectuării unor retrageri de numerar de la bancomat se află sub incidența art. 360 C.pen. Instrumentul de plată electronică este, în acest context, o veritabilă cheie de acces necesară pentru autentificarea la bancomat. De asemenea, utilizarea instrumentului de plată electronică și introducerea corectă a codului PIN permite făptuitorului să efectueze o serie de operațiuni, precum: retragerea de numerar, interogarea soldului disponibil, schimbarea codului PIN etc. Toate aceste interacțiuni logice cu bancomatul se transpun în exercitarea unui control efectiv asupra funcțiilor acestuia.

Credem totuși că această concluzie a Înaltei Curți de Casație și Justiție referitoare la reținerea art. 360 C.pen. nu poate fi extinsă cu privire la alte ipoteze în care se efectuează operațiuni financiare în mod fraudulos. Astfel, efectuarea unor plăți pe Internet folosind datele de identificare a unui instrument de plată electronică ori la un terminal POS nu implică un acces la un sistem informatic. În ciuda existenței unei interacțiuni la nivel logic cu un server web sau cu un terminal POS[68], discutăm despre o simplă transmitere de date informatice care nu prezintă relevanță pentru reținerea art. 360 C.pen. Prin urmare, în aceste ipoteze, apreciem că ar trebui reținută doar infracțiunea prevăzută la art. 250 alin. (1) C.pen.[69].

3. Folosirea la bancomat a unui card bancar falsificat, pentru retrageri de numerar, constituie infracțiunea de efectuare de operațiuni financiare în mod fraudulos prin utilizarea unui instrument de plată electronică, inclusiv a datelor de identificare care permit utilizarea acestuia, prevăzută de art. 27 alin. (1) din Legea nr. 365/2002 [*de lege lata*, art. 250 alin. (1) C.pen.], în concurs ideal cu infracțiunea de acces, fără drept, la un sistem informatic, comisă în scopul obținerii de date informatice prin încălcarea măsurilor de securitate, prevăzută de art. 42 alin. (1), (2) și (3) din Legea nr. 161/2003 (*de lege lata*, art. 360 C.pen.), și cu infracțiunea de falsificare a instrumentelor de plată electronică, prevăzută de art. 24 alin. (2) din Legea nr. 365/2002 [*de lege lata*, art. 311 alin. (2) C.pen.].

Diferența față de pct. 2 analizat *supra* este aceea că, în acest caz, discutăm despre un card bancar falsificat. Tocmai de aceea, în concursul de infracțiuni va intra și infracțiunea prevăzută de art. 311 alin. (2) C.pen.

Recent, Curtea de Apel București a sesizat Înalta Curte de Casație și Justiție în vederea pronunțării unei hotărâri prealabile cu privire la următoarea problemă de drept: „dacă retragerea de numerar cu carduri falsificate, folosind datele cardurilor copiate, întrunește elementele constitutive ale infracțiunii de efectuare de operațiuni financiare în mod fraudulos prevăzute de art. 250 alin. (1) și (2) C.pen. în concurs ideal cu infracțiunea de acces ilegal la un sistem informatic, prevăzută de art. 360 C.pen., sau doar infracțiunea de efectuare de operațiuni financiare în mod fraudulos, prevăzută de art. 250 alin. (1) și (2) C.pen.”[70].

[67] A se vedea, în acest sens, și *G. Zlati*, Tratat..., vol. 1, op. cit., p. 129. Credem, de asemenea, că agravanta prevăzută la alin. (2) nu poate fi reținută *de plano*. O simplă retragere de numerar, fără interogarea soldului ori tipărirea unei chitanțe, nu poate proba scopul obținerii de date informatice.

[68] Ori chiar cu serverul bancar prin intermediul terminalului POS.

[69] A se vedea, în acest sens, și *G. Zlati*, Tratat..., vol. 1, op. cit., pp. 207-210.

[70] Pentru o analiză critică a acestei sesizări, se poate vedea *idem*, Accesarea unui sistem informatic și retragerea de numerar de la bancomat. Dezlegarea unei chestiuni de drept. Inadmisibilitate?, *passim*, material disponibil pe *juridice.ro* (ultima accesare la data de 2 iunie 2021).

Această sesizare a fost respinsă pe bună dreptate de către Înalta Curte de Casație și Justiție ca fiind inadmisibilă prin Decizia nr. 2/2021[71]. În motivarea soluției de inadmisibilitate, Curtea a statuat faptul că „se constată că obiectul sesizării îl constituie interpretarea, din aceeași perspectivă, a dispozițiilor legale în vigoare care au preluat reglementările anterioare, astfel încât se impune concluzia că intervenția instanței supreme nu se impune, întrucât dezlegarea ce se solicită a se da problemelor de drept se regăsește într-o decizie anterioară dată în interesul legii, ale cărei considerente se aplică, *mutatis mutandis*, și în cauza aflată pe rolul Curții de Apel București – Secția a II-a penală".

B. Dezlegarea unei chestiuni de drept prin Decizia ICCJ nr. 4/2021. Crearea de conturi false pe rețelele de socializare și falsul informatic

Prin Decizia nr. 4/2021[72], Înalta Curte de Casație și Justiție a statuat următoarele: „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 prevăzute 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".

Necesitatea dezlegării acestei chestiuni de drept[73] s-a datorat unei practici judiciare neunitare cu privire la interpretarea elementelor constitutive ale art. 325 C.pen. în ipoteze în care făptuitorul creează conturi false pe rețele de socializare ori pe site-uri de escorte.

În esență, atât opinia majoritară la nivelul practicii judiciare, cât și a unor autori de drept penal[74] era în sensul că nu se poate reține infracțiunea de fals informatic. Argumentele în susținerea acestei teze au fost următoarele:

1. conduita făptuitorului nu este realizată fără drept, nefiind incidentă vreo ipoteză dintre cele enumerate în cuprinsul art. 35 alin. (2) din Legea nr. 161/2003;

În primul rând, credem că o asemenea opinie ignoră faptul că, în ceea ce privește clonarea de pagini web (ca parte integrantă a unei conduite tip *phishing*), practica judiciară este unanimă în ceea ce privește reținerea infracțiunii de fals informatic. Or, din perspectiva analizei elementului „fără drept", nu vedem să existe vreo diferență între conduita de a crea un cont fals pe o rețea de socializare și clonarea unei pagini web.

Ceea ce s-a omis este faptul că sistemul informatic cu care se interacționează în vederea creării contului fals, fie că discutăm aici despre serverul web unde este găzduit un site de escorte, fie serverul Facebook prin intermediul căruia rețeaua de socializare devine operațională, reprezintă doar instrumentul folosit la comiterea falsului informatic. Prin urmare, existența sau inexistența unui drept cu privire la utilizarea instrumentului folosit la falsificare nu ar trebui să aibă o relevanță deosebită. Atunci când discutăm despre clonarea unei pagini web, făptuitorul poate contraface interfața vizuală folosind propriul sistem informatic

[71] ICCJ, Completul pentru dezlegarea unor chestiuni de drept în materie penală, dec. nr. 2/2021, publicată în M. Of. nr. 293 din 24 martie 2021.

[72] ICCJ, Completul pentru dezlegarea unor chestiuni de drept în materie penală, dec. nr. 4/2021, publicată în M. Of. nr. 171 din 19 februarie 2021.

[73] Pentru o analiză a acesteia, se poate vedea *G. Zlati*, Punct de vedere referitor la problema conturilor „false" pe rețelele de socializare. Dezlegarea unei dezlegări de drept, *passim*, material disponibil pe *penalmente.ro* (ultima accesare la data de 3 iunie 2021).

[74] A se vedea, în acest sens, *D. Pârgaru*, Despre limitele falsului informatic în cazul rețelelor de socializare. Opinie cu privire la dezlegarea unei chestiuni de drept în materie penală, *passim*, material disponibil pe *juridice.ro* (ultima accesare la data de 1 iunie 2021). În ceea ce ne privește, am susținut, încă din anul 2014, faptul că o asemenea conduită intră sub incidența falsului informatic – a se vedea, în acest sens, *S. Bogdan, D.A. Șerban, G. Zlati*, Noul Cod penal..., op. cit., p. 560.

și poate găzdui pagina web rezultată fie pe un server web propriu, fie poate proceda la achiziționarea unui serviciu de găzduire web de la o terță persoană. Aceasta nu înseamnă totuși că făptuitorul a acționat cu drept la momentul contrafacerii respectivei pagini web.

Tocmai de aceea am susținut faptul că esențială, din perspectiva reținerii infracțiunii de fals informatic, este încălcarea manifestării de voință a titularului identității uzurpate la momentul creării unui cont fals. Justețea acestei construcții juridice este cu atât mai evidentă dacă ne raportăm la simularea poștei electronice (în engleză, *e-mail spoofing*), conduită acceptată, de asemenea, ca intrând sub incidența falsului informatic[75]. În această ipoteză, făptuitorul poate interacționa cu propriul său server (*mail server*) și propriul său cont de poștă electronică pentru a modifica adresa expeditorului. Singura posibilitate de a reține că acesta acționează fără drept este de a ne raporta la manifestarea de voință a persoanei a cărei identitate o uzurpă, căci, altfel, el interacționează la nivel logic cu propriul său sistem informatic și propriul cont de poștă electronică.

2. conduita făptuitorului de a introduce date informatice la momentul creării unui cont fals nu rezultă în date necorespunzătoarele adevărului.

Construcția juridică era aceea că, prin folosirea datelor de identificare reale aparținând unei alte persoane, fie nu putem discuta despre rezultarea unor date necorespunzătoare adevărului, fie aceste date necorespunzătoare adevărului nu sunt susceptibile de a produce consecințe juridice.

O asemenea construcție este eronată, deoarece, prin raportare la teoria intelectuală a falsului, nu ne interesează corespondența dintre datele folosite la crearea contului și datele rezultate, ci corespondența dintre introducerea acestor date de identificare și manifestarea de voință a titularului identității uzurpate. Apreciem că discutăm în această ipoteză despre date necorespunzătoare adevărului, așa cum discutăm și în ipoteza contrafacerii unei cărți de identitate. De asemenea, crearea unui cont fals cu scopul de a uzurpa identitatea unei persoane este de natură să producă consecințe juridice.

În soluționarea acestei probleme de drept, Înalta Curtea de Casație și Justiție a statuat – printre altele – următoarele:

„Verificarea existenței sau nu a dreptului de a introduce, modifica sau șterge date informatice se impune a fi făcută prin raportare la persoana care are dreptul de dispoziție asupra acestor date, respectiv la existența sau nu a manifestării de voință a acesteia.

(...) Făptuitorul care creează un cont/profil într-o rețea de socializare deschisă publicului, introducând numele și datele cu caracter personal reale ale altei persoane și care permit identificarea acesteia (informații, fotografii, imagini video etc.), ca fiind date referitoare la propria persoană, acționează prin încălcarea manifestării de voință a persoanei a cărei identitate și-a uzurpat-o.

(...) Făptuitorul nu este autorizat în temeiul legii, pentru că nu există nicio dispoziție legală care să permită unei persoane să introducă într-o rețea de socializare deschisă publicului date informatice privind o altă persoană (date de identificare și alte date cu caracter personal reale), ca fiind date privind propria persoană. Dimpotrivă, legea protejează dreptul la propria imagine (art. 73 din Codul civil), iar utilizarea, cu rea-credință, a numelui, imaginii sau vocii unei persoane constituie, potrivit art. 74 lit. h) din Codul civil, o atingere adusă vieții private.

(...) În cazul contrafacerii, trebuie studiat dacă manifestarea de voință conținută în înscrisul contrafăcut are sau nu un corespondent în realitatea materială.

(...) Crearea unui cont fără drept, uzurpând identitatea unei persoane, prin introducerea de date reale și care permit identificarea respectivei persoane, presupune o falsificare a manifestării de voință a acesteia și creează o percepție contrară realității în privința titularului respectivului cont.

[75] A se vedea, în acest sens, *G. Zlati*, Tratat..., vol. 1, op. cit., pp. 523-526.

(...) 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).

(...) Pentru reținerea infracțiunii, pe lângă cele două cerințe esențiale ce fac obiectul analizei în prezenta sesizare, este necesar ca 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, acesta urmând a fi verificat în funcție de circumstanțele concrete ale fiecărei cauze".

În ceea ce ne privește, nu putem decât să achiesăm acestor considerente care se pliază într-o bună măsură pe viziunea noastră asupra sferei de aplicabilitate a infracțiunii de fraudă informatică. Având ca premisă această dezlegare de drept, credem că se impun următoarele concluzii:

- falsul informatic (art. 325 C.pen.) incriminează inclusiv o etapă a furtului de identitate[76];
- prin această dezlegare de drept nu s-a concluzionat că orice utilizare fără drept a datelor de identificare a unei persoane constituie infracțiunea de fals informatic. Un element constitutiv care nu a fost analizat de către Curte este scopul special al producerii de consecințe juridice. Având în vedere că trebuie să raportăm contextual această producere de consecințe juridice la uzurparea de identitate, vom exclude din sfera de aplicabilitate a art. 325 C.pen. acele conduite care nu reflectă o uzurpare de identitate;
- apreciem că trebuie făcută o distincție între crearea de profile false și crearea de profile fictive. Dacă, în primul caz, putem discuta despre o uzurpare de identitate tipică art. 325 C.pen., în cel de-al doilea caz, discutăm despre o formă de anonimitate în mediul online[77]. Este irelevant faptul că scopul creării unui profil fictiv a fost ascunderea identității reale și, implicit, împiedicarea identificării făptuitorului. Crearea unui cont fictiv în vederea ascunderii identității nu constituie infracțiune, așa cum nu constituie infracțiune nici utilizarea unui serviciu VPN (*Virtual Private Network*) sau *Onion routing* (de exemplu, prin intermediul unui browser TOR);
- având în vedere faptul că, *de lege lata*, nu este incriminat uzul de fals informatic (spre deosebire de falsul tradițional, unde este incident art. 323 C.pen.), se pune problema în ce măsură utilizarea profilului fals prin publicarea de conținut în numele titularului identității uzurpate echivalează cu un uz de fals informatic (conduită neincriminată) sau cu un fals informatic;
- de asemenea, se pune problema în ce măsură accesarea fără drept a unui cont de Facebook și publicarea de conținut în numele titularului de cont echivalează cu un fals informatic în modalitatea introducerii de date informatice.

În concluzie, nu putem decât să observăm că, prin această dezlegare de drept, Înalta Curte de Casație și Justiție a răsturnat un trend la nivelul practicii judiciare, aducând în sfera ilicitului penal o conduită care, în opinia multora, nu constituia infracțiune. Cu toate acestea, dezbaterile nu iau sfârșit odată cu această dezlegare de drept. Așa cum am arătat *supra*, există în continuare o serie de aspecte ce necesită o analiză laborioasă pentru identificarea unei soluții corecte din punct de vedere juridic.

[76] Pentru o analiză mai în detaliu, se poate vedea *G. Zlati*, Tratat..., vol. 1, op. cit., p. 592 și urm.

[77] A se vedea, în acest sens, *ibidem*, pp. 530-536; *S. Bogdan, D.A. Șerban, G. Zlati*, Noul Cod penal..., op. cit., p. 560.

C. Dezlegarea unei chestiuni de drept prin Decizia ICCJ nr. 37/2021. Raportul dintre infracțiunea de înșelăciune și frauda informatică

Prin Decizia nr. 37/2021[78], Înalta Curte de Casație și Justiție a statuat următoarele: „publicarea de anunțuri fictive online care a avut drept consecință producerea unei pagube, fără ca prin această activitate să se intervină asupra sistemului informatic sau asupra datelor informatice prelucrate de acesta, realizează condițiile de tipicitate ale infracțiunii de înșelăciune prevăzute de art. 244 din Codul penal".

Așa cum a susținut și reprezentanta Ministerului Public în momentul în care aceasta a formulat concluzii cu privire la sesizarea Înaltei Curți de Casație și Justiție, „practica judiciară este constantă în a considera că fapta de a publica anunțuri fictive pe Internet, urmată de producerea unei pagube, întrunește elementele constitutive ale infracțiunii de fraudă informatică"[79].

O asemenea practică judiciară majoritară, existentă încă dinainte de intrarea în vigoare a noului Cod penal, era una eronată și avea la bază o confuzie regretabilă între înșelăciunea tradițională comisă prin mijloace informatice (art. 244 C.pen.) și frauda informatică (art. 249 C.pen.)[80]. Nu orice introducere de date informatice urmată de producerea unei pagube atrage aplicabilitatea infracțiunii de fraudă informatică. Pentru a discuta despre o fraudă informatică, este necesar ca paguba să fie rezultatul introducerii de date informatice (ori o altă modalitate prevăzută la art. 249 C.pen.), fără a discuta despre o conduită autopăgubitoare a victimei. Existența unei asemenea conduite autopăgubitoare, chiar și în măsura în care este determinată de datele informatice introduse de către făptuitor[81], este de esența infracțiunii de înșelăciune.

În încercarea de a simplifica raportul dintre cele două infracțiuni, susținem faptul că discutăm despre o fraudă informatică în acele situații în care, prin modalitățile prevăzute la art. 249 C.pen., este manipulat un sistem informatic. În măsura în care manipularea sistemului informatic este înlocuită cu inducerea în eroare a unei persoane fizice sau juridice, chiar prin intermediul unei introduceri de date informatice, vom discuta despre o înșelăciune tradițională prin mijloace informatice. Se observă, așadar, că, pentru reținerea fraudei informatice, conduita victimei este irelevantă pentru producerea pagubei, iar atunci când paguba este produsă de conduita autopăgubitoare a victimei, vom discuta despre o infracțiune de înșelăciune.

Această analiză se poate transpune și în sfera raportului de cauzalitate. Astfel, observăm că, în ipoteza anunțurilor fictive/frauduloase, nu există un raport de cauzalitate direct între introducerea de date informatice și producerea unei pagube. Dacă victima nu s-ar autoprejudicia ca urmare a unei induceri în eroare, introducerea de date informatice nu ar fi niciodată aptă să producă o pagubă. Discutăm, așadar, chiar despre o tentativă neidonee.

[78] ICCJ, Completul pentru soluționarea unor chestiuni de drept în materie penală, dec. nr. 37/2021 (nemotivată).

[79] Exemple relevante în acest sens sunt: ICCJ, s. pen., dec. nr. 2106/2013; C.A. Bacău, s. pen. min. și fam., dec. nr. 128/2011; C.A. Pitești, s. pen., dec. nr. 496/2014; C.A. Pitești, s. pen., dec. nr. 672/2013; C.A. Craiova, s. pen., dec. nr. 1113/2015; C.A. București, s. a II-a pen., dec. nr. 637/2017; C.A. Alba Iulia, s. pen., dec. nr. 171/2015; C.A. Bacău, s. pen. min. și fam., dec. nr. 128/2011; C.A. Cluj, s. pen. și de minori, dec. nr. 1801/2011; C.A. București, s. I pen., dec. nr. 938/2016; C.A. București, s. I pen., dec. nr. 1189/2016; C.A. București, s. a II-a pen., dec. nr. 1472/2017; C.A. Craiova, s. pen., dec. nr. 279/2017 etc.

[80] Pentru o analiză amplă cu privire la raportul dintre infracțiunea de înșelăciune și infracțiunea de fraudă informatică, se poate vedea: *G. Zlati*, Tratat..., vol. 1, op. cit., pp. 453-461; *idem*, Comentariu, în G. Bodoroncea, V. Cioclei, I. Kuglay și colab., Codul penal. Comentariu pe articole, ed. 3, Ed. C.H. Beck, București, 2020, pp. 919-920.

[81] În încheierea de sesizare am observat că uneori se insistă prea mult pe ideea că, în cazul licitațiilor/anunțurilor online fictive/frauduloase, esențial este faptul că, ulterior introducerii de date de informatice (a anunțului), există o comunicare între făptuitor și victimă. Nu acesta este elementul esențial, deoarece, chiar în lipsa unei asemenea comunicări ulterioare, tot nu credem că s-ar putea reține infracțiunea de fraudă informatică. Esențial este faptul că nu introducerea de date informatice cauzează *per se* paguba, ci conduita autoprejudiciantă a victimei.

De altfel, dacă s-ar accepta teza reținerii infracțiunii de fraudă informatică, ar însemna că simpla introducere de date informatice se situează în sfera tentativei. Or, nu putem decât să ne întrebăm retoric: care sunt subiecții pasivi la care trebuie să raportăm această tentativă de fraudă informatică? Răspunsul nu ar putea să fie decât că subiecți pasivi sunt toți utilizatorii care pot vizualiza sau au vizualizat conținutul anunțului fictiv/fraudulos. În mod evident, o asemenea concluzie este de neacceptat.

Având în vedere toate aceste aspecte, apreciem că Înalta Curte de Casație și Justiție a tranșat în mod corect această problemă de drept, fapt ce va conduce la un veritabil reviriment al practicii judiciare pe acest subiect.