Radion COJOCARU, doctor în drept, conferenţiar universitar,
şef al Facultăţii de drept a Academiei „Ştefan cel Mare"

ESCROCHERII INFORMAŢIONALE: FORME ŞI CLARIFICĂRI CONCEPTUALE ALE CADRULUI NORMATIV-PENAL DE INCRIMINARE

În condiţiile actuale de evoluţie a comunităţii umane, dezvoltarea diferitor domenii de activitate, inclusiv a celui economic, se bazează pe utilizarea la scară largă a tehnologiilor informaţionale şi a telecomunicaţiilor. Derularea operaţiilor economice prin sistemele şi reţelele computerizate a dus la apariţia business-ului „electronic" sau „virtual" ca alternativă eficientă de economisire a timpului în afaceri – element indispensabil în obţinerea rapidă a profiturilor şi beneficiilor.

În pofida numeroaselor aspecte pozitive pe care le oferă „businessul electronic", perpetuarea lui a generat săvârşirea unor fapte social-negative de fraudare a reţelelor şi sistemelor informatice. Tendinţele de răspândire a fraudelor de acest gen au atins cote alarmante, fiind puse la îndoială avantajele comerţului „virtual", declarate ca fiind prioritare faţă de cele ale comerţului „real" [1]. În acest sens, Organizaţia internaţională a poliţiei criminale Interpol apreciază Internetul ca fiind caracterizat prin cea mai acută creştere a criminalităţii, comparativ cu alte sectoare ale activităţii umane.

Din categoria infracţiunilor săvârşite tendenţios prin intermediul computerului fac parte „escrocheriile informaţionale", caracterizate prin mecanisme şi procedee proprii de fraudare a reţelelor informaţionale, cum ar fi:

– phishingul. Este recunoscut ca o formă modernă de inginerie financiară, ce constă în obţinerea frauduloasă a informaţiilor confidenţiale (numele de utilizator, parola şi detalii legate de cartea de credit) prin imitarea, aproape de perfecţiune, a paginii web a unei companii credibile cu utilizarea unei forme de comunicare electronică. Băncile care efectuează tranzacţii on-line sunt ţintele predilecte, phishingul realizându-se prin intermediul e-mail-ului sau al mesageriei instant şi, de obicei, redirecţionează utilizatorii spre o pagină identică cu cea a companiei credibile, unde utilizatorului i se cere să-şi introducă informaţiile personale;

– sustrageri cu carduri bancare false. În prezent, falsul de carduri şi punerea lor în circulaţie constituie un fenomen de proporţii la nivel global, aducând daune colosale sistemului financiar-bancar. Ingeniozitatea de care dau dovadă infractorii în ceea ce priveşte punerea în aplicare a metodelor de fals de multe ori depăşeşte experienţa organelor de resort în materia investigării acestor fap-

te. Cele mai răspândite moduri de operare sunt: instalarea în bancomate a unor dispozitive tehnice special adaptate de scanare a informaţiilor de pe carduri; accesarea şi interceptarea informaţiilor transmise băncii de către bancomat pentru verificarea sumelor de bani de care dispun deţinătorii; filmarea PIN-codurilor în timpul accesării bancomatului de către clienţi etc.;

– fraude pe piaţa valorilor mobiliare. Schemele de fraudare presupun obţinerea de beneficii din contul vânzării valorilor mobiliare al căror cost real este majorat în mod fictiv. Răspândind date eronate despre emiţător şi condiţia economică a acestuia, făptuitorul în mod fraudulos influenţează creşterea ofertei şi a preţurilor, după care încheie tranzacţii de vânzare a acţiunilor la un preţ majorat. Ulterior, preţurile pe piaţă se restabilesc la nivelul real, iar investitorii de rând suportă daune materiale [2];

– postarea licitaţiilor fictive sau vânzarea „produselor-momeală". Constă în ademenirea potenţialilor clienţi prin postarea de publicităţi fictive, oferindu-se spre vânzare produse costisitoare la preţuri avantajoase. În speţă, produsele fie că nu există în realitate, fie că sunt ulterior schimbate cu produse aparent similare, dar cu calităţi net inferioare. Caracteristic pentru această formă de fraudare este faptul că în nici un moment autorul nu are de gând să vândă „produsul-momeală" [3, p. 225];

– escrocheriile săvârşite cu ajutorul telefoanelor mobile. Se cunosc diferite modalităţi faptice de manifestare a acestui tip de escrocherie, precum ar fi, de exemplu, expunerea spre comercializare a unor programe fictive, ce ar face posibilă efectuarea fără plată a convorbirilor telefonice. De regulă, schema de fraudare este deosebit de ingenioasă, presupunând lansarea pe pagina web a unor oferte atractive (este dată publicităţii lista operatorilor cu care asemenea programe pot fi puse în funcţiune; sunt afişate modelele telefoanelor mobile a căror utilizare permite funcţionarea programei respective etc.). O altă metodă de săvârşire a escrocheriilor informaţionale cu utilizarea telefoanelor mobile constă în scanarea Cod-pinurilor de pe cartelele telefonice, urmată de folosirea frauduloasă a timpului de convorbire, cu expunerea ulterioară a cartelelor în vânzare;

– propuneri de afaceri fictive. De regulă, pe pagina web este descrisă rentabilitatea afacerii, făcând-o să devină, astfel, atractivă pentru victimă. Participarea propriu-zisă la afacere sau oferirea unor date suplimentare pentru realizarea ei este condiţionată de transferarea pe un cont indicat de către făptuitor a unor mijloace băneşti, care, de regulă, poartă un caracter simbolic, fiind nesemnificative (de exemplu, victimei i se propune achitarea unei sume de bani pentru obţinerea unor mostre de contracte pe care urmează să le încheie cu viitori clienţi). După operarea transferului de bani, victima nu mai poate accesa pagina web, aceasta fiind distrusă de către făptuitor.

Cu referinţă la cadrul normativ aplicabil escrocheriilor informaţionale, este de menţionat că în sistemul reglementărilor penale ale Republicii Moldova expresia „escrocherie informaţională" nu şi-a găsit uzanţă legislativă, nefiind folosită la descrierea faptelor ilicite cu caracter penal. Din lipsa suportului normativ, sarcina

definirii conceptului de escrocherie informațională, precum şi stabilirea sferei de incidență a acesteia în normativul penal, revine, fără doar şi poate, doctrinei dreptului penal.

În legislațiile penale ale altor state, precum ar fi cea a Estoniei, escrocheria informațională şi-a găsit o incriminare distinctă la art.268 CP, cu următoarea exprimare legislativă: „Dobândirea averii străine, a avantajelor patrimoniale sau de altă natură prin introducerea programelor sau informațiilor, prin modificarea, distrugerea, blocarea sau printr-o altă intervenție realizată în procesul de prelucrare a informației, care influențează rezultatul acestuia şi care atrage după sine cauzarea unei daune materiale sau de altă natură proprietarului" [4].

O faptă similară celei amintite mai sus, cu denumirea marginală de „sustragere săvârşită cu utilizarea tehnicii informaționale" este stipulată în CP al Republicii Belarus, legiuitorul atribuindu-i calitatea de formă distinctă a sustragerii la art.212 CP: „Sustragerea averii săvârşită prin modificarea informației existentă în sistemul informațional, pe suporții materiali sau care este transmisă prin rețelele de transmitere a informației" [5].

Numerose demersuri dedicate definirii conceptului de escrocherie informațională au fost inițiate în doctrina dreptului penal.

Într-o primă opinie se consideră că escrocheriile informaționale reprezintă infracțiunile săvârşite cu scop cupidant, prin intermediul manipulării programelor, datelor sau anumitor părți componente ale computerului [6, p. 71].

Potrivit unul alt punct de vedere, se afirmă că escrocheria informațională reprezintă o infracțiune cu caracter informațional, care presupune denaturarea, modificarea sau ascunderea intenționată a datelor în scopul obținerii cu ajutorul sistemului computerizat a unor beneficii băneşti [7, p. 325].

Într-o altă accepțiune, escrocheria informațională presupune dobândirea averii străine pe calea înşelăciunii, abuzului de încredere, însuşirii sau înstrăinării bunurilor, precum şi prin cauzarea de pagube materiale săvârşite prin utilizarea calculatorului. După cum putem observa, în virtutea acestui ultim punct de vedere, este lărgită sfera de incidență a escrocheriei informaționale, cuprinzând trei manifestări infracționale incriminate distinct în legislația penală: escrocheria propriu-zisă; delapidarea averii străine; cauzarea de pagube materiale prin înşelăciune sau abuz de încredere [8].

În viziunea noastră, extinderea conceptului de escrocherie informațională la alte fapte penale săvârşite prin intermediul rețelelor informaționale (cum ar fi, de exemplu, delapidarea averii străine, cauzarea de pagube materiale prin înşelăciune sau abuz de încredere, frauda informatică) poate fi acceptată doar în limitele unui studiu criminologic. Din perspectiva dreptului penal, o asemenea lărgire de concept nu poate fi acceptată, întrucât legiuitorul la art.190 CP al Republicii Molodva fixează un cadru legal bine definit al escrocheriei, care nu poate fi extins la alte conduite ilicite cu caracter penal. De fapt, din rațiuni de tehnică legislativă, în vederea asigurării unei interpretări uniforme a normativului penal, nu poate fi acceptată ideea atribuirii unor înțelesuri diferite

expresiilor şi termenilor folosiţi în legislaţia penală la descrierea componenţelor de infracţiune.

Dintr-o atare perspectivă, în vederea asigurării aplicării corecte a legii penale, în strictă consonanţă cu principiul legalităţii, este necesar de a stabili cu claritate normele cu caracter incriminator ce devin incidente în raport cu diferitele forme pe care le pot îmbrăca sustragerile din reţelele infromaţionale şi prin aceasta – limitele aplicării normei privitoare la escrocherie.

Punctul de reper în acest sens, fără doar şi poate, îl constituie norma prevăzută la art.190 CP al Republicii Moldova, care stabileşte extremităţile de incidenţă a legii penale în ceea ce priveşte posibilitatea încadrării unei fapte ca escrocherie.

În contextul abordărilor consemnate, considerăm că fapta incriminată la art.190 CP al Republicii Moldova devine aplicabilă când calculatorul şi informaţia computerizată sunt utilizate de către făptuitor pentru influenţarea voinţei victimei de a transmite benevol bunul sau dreptul asupra acestuia, sub dominaţia înşelăciunii sau abuzului de încredere. După cum susţine T. Tropina, la operarea schemelor de inducere în eroare, calculatorul este utilizat în calitate de element adiţional, prin care se asigură apropierea cu victima, iar mediul informaţional – mediu alternativ celui fizic ce permite contactarea acesteia [9].

Prin urmare, subscriem ideii după care sustragerea de bunuri prin metoda escrocheriei nu este o consecinţă a simplei manipulării a datelor şi informaţiilor computerizate. Actul sustragerii, în acest caz, este rezultatul inducerii în eroare a victimei cu ajutorul mijloacelor informaţionale, sub influenţa căreia are loc cedarea benevolă a bunului. Plecând de la aceste premise, doar în situaţiile semnalate poate deveni aplicabilă norma privitoare la escrocherie, în alte cazuri fiind necesară apelarea la alte dispoziţii prescrise de Codul penal.

O altă faptă, care exprimă un act de conduită bine conturat, în limitele căruia îşi poate găsi expresie sustragerea informaţională, o constituie infracţiunea incriminată art.237 CP, săvârşită prin modalitatea punerii în circulaţie a cardurilor sau a carnetelor de plată false.

Nu vom insista asupra tuturor variantelor posibile de comitere a infracţiunii vizate, ci doar asupra situaţiilor de folosire a cardurilor false, care în esenţă, după cum se menţionează în doctrina de specialitate, se referă la „...retragerea disponibilului sub formă de numerar de la ghişeul automat de bancă sau de la distribuitorul automat de numerar; achitarea mărfurilor sau a serviciilor comerciantului prin intermediul automatelor bancare, terminalelor pentru transferul electronic de fonduri la punctul de vânzare ..." [10, p. 424].

Reieşind din modul specific de comitere a faptei, precum şi din particularităţile obiectului material al infracţiunii, apare întrebarea: folosirea cardurilor false poate fi interpretată în calitate de formă specială a infracţiunii de escrocherie?

Deşi într-un demers făcut anterior, cu prilejul analizei componenţei descrise la art.237 CP al Republicii Moldova, nu s-au făcut precizările de rigoare, în

limitele prezentului studiu, punctăm ideea după care între folosirea cardurilor plăsmuite şi infracţiunea de escrocherie nu poate fi recunoscută o legătură de tipul special-general. Aceasta se face deoarece în cazul utilizării cardurilor false nu are loc influenţarea voinţei victimei de către făptuitor prin metodele frauduloase caracteristice escrocheriei, ci o manipulare a datelor informaţioanle, în urma căreia are loc trecerea bunurilor în posesia ilegală a victimei. Prin urmare, considerăm că uzul de carduri false poate fi catalogat la categoria fraudelor informaţionale, care, datorită obiectului juridic generic şi special de atentare, la moment şi-a găsit o incriminare distinctă în capitolul X Codul penal al Republicii Moldova.

O altă problemă de rezonanţă în materia vizată o constituie legătura corelativă dintre frauda informatică (art. 260^6 CP) şi infracţiunea de escrocherie (art. 190 CP).

În viziunea noastră, frauda informatică nu poate fi asimilată escrocheriei, date fiind deosebirile de conţinut existente între aceste două fapte infracţionale. Deosebirea esenţială dintre frauda informatică şi escrocherie poate fi făcută prin prisma obiectului material al infracţiunii. În cazul escrocheriei, obiectul material este reprezentat de bunurile mobile aflate în posesia persoanei, asupra cărora este fixat dreptul de proprietate, pe când în cazul fraudei informatice obiectul material îl formează beneficiile ce urmează să fie obţinute de către persoană.

Prin beneficiu se înţelege câştig, profit sau folos pe care cineva îl are din ceva; profit financiar al unei întreprinderi, reprezentând diferenţa dintre veniturile realizate şi cheltuielile ocazionate din acesta.

În cazul fraudei informaţionale, înşelăciunea poate fi realizată prin metode similare sau identice escrocheriei, însă făptuitorul nu urmăreşte deposedarea ilegală a victimei de un bun, ci obţinerea unor beneficii ilegale, sub formă de profit nerealizat ce putea rezulta dintr-un anumit bun sau din afacerile practicate de antreprenor. Prin urmare, între fapta de fraudă informatică şi escrocherie poate exista o legătură de tip escrocherie – cauzarea de pagube materiale prin înşelăciune sau abuz de încredere.

Problema calificării juridice a faptelor de schimbare sau de manipulare a datelor informaţionale, urmate de obţinerea ilegală a bunurilor, deocamdată nu şi-au găsit o rezolvare unitară în doctrina dreptului penal (cum ar fi, de pildă, transferul de bani de pe un cont pe alt cont, urmat de sustragerea lor – cazul Levin care, prin spargerea măsurilor de protecţie, a transferat de pe conturile băncii City Bank of America pe diferite conturi circa 11 milioane de dolari SUA).

O. Borunov susţine că în speţă poate fi identificată infracţiunea de furt dacă persoana, după ce a transferat mijloacele băneşti, le scoate de pe cont, adică intră în posesia lor putând dispune de ele după propria-i voinţă; posibilitatea de dispunere intervine şi atunci când făptuitorul le pune în circulaţie într-o altă formă, de exemplu, le depozitează pe un alt cont pentru obţinerea dobânzii [11, p. 26].

În contrast, pe bună dreptate, în doctrina de specialitate se susţine că săvârşirea sustragerii pe calea furtului cu utilizarea mijloacelor informaţionale se face imposibilă, întrucât în calculator nu sunt păstrate bunurile sau mijloacele băneşti, ci informaţiile despre drepturile asupra bunurilor, păstrarea sau circulaţia lor [9]. Se mai afirmă că în asemenea situaţii nu se poate identifica sustragerea de bunuri, ci dobândirea dreptului asupra bunurilor, legiuitorul făcând pe plan normativ distincţie dintre aceste două categorii juridice [9].

În finalul prezentărilor relatate, considerăm că problema sustragerilor informaţionale îşi va putea găsi o rezolvare corespunzătoare doar în perspectiva operării unor modificări de *lege ferenda*. Dintr-o atare perspectivă, pledăm în favoarea ideii de introducere a unei norme penale distincte ce ar încorpora toate formele de sustragere a bunurilor săvârşite prin intermediul utilizării tehnologiilor informaţionale.

Referinţe bibliografice:

1. В. Сабадаш, Современное состояние проблемы распространения мошенничества в Интернете // http://www.crime-research.ru/articles.
2. С.С. Карабаналов, Компьютерное мошенничество при торговле ценными бумагами с использованием сети Интернет в США // http://skyglobe.ru.
3. M. Dobrinoiu, *Infracţiuni în domeniul informaticii*, Ed. C.H. Beck, Bucureşti, 2006, p. 225.
4. http://www.crime.vl.ru.
5. http://pravo.kulichki.com.
6. А.В. Черных, „Некоторые вопросы уголовно-правовой квалификации компьютерных мошенничеств" în *Советское государство и право*, 1989, №6, с. 71.
7. Д. Айков, *Компьютерные преступления*, Москва, Мир, 1999, с. 325.
8. Д. Зыков, Понятие компьютерного мошенничества // www.crime-research.org.
9. Т. Тропина, Компьютерное мошенничество»: вопросы квалификации и законодательной техники // www.connect.ru/article.
10. Stati în *Drept penal, Partea specială*, vol. II, Ed. Cartier Juridic, Chişinău, p. 424.
11. О. Борунов, „Проблемы квалификации хищения денежных средств со счетов банк с использованием средств компьютерной техники" în *Российский судья*, 2004 г., № 6, стр. 26.