STUDIA UNIVERSITATIS MOLDAVIAE, 2016, nr.3(93)
Seria "Ştiinţe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.39-46

UNELE ASPECTE PRIVIND ANALIZA JURIDICO-PENALĂ COMPARATIVĂ A INFRACŢIUNILOR INFORMATICE ÎN LEGEA PENALĂ A REPUBLICII MOLDOVA ŞI ÎN CEA A ROMÂNIEI

Sergiu CRIJANOVSCHI
Universitatea de Stat din Moldova

Scopul propus în acest articol ştiinţific rezidă în soluţionarea unor aspecte discutabile legate de analiza juridico-penală a infracţiunilor săvârşite în domeniul informaticii. În el sunt elucidate anumite aspecte problematice, fiind înaintate soluţii relevante ale acestora şi formulate propuneri *de lege ferenda* cu scopul perfecţionării legislaţiei penale în vigoare. Pentru a atinge scopul trasat autorul a analizat doctrina din domeniul dreptului penal şi cibernetic, precum şi a efectuat analiza comparativă a legislaţiei penale interne a Republicii Moldova şi a celei a României, pe de o parte, a actelor internaţionale în sfera informaticii, pe de altă parte. Au fost aduse definiţii relevante ale infracţiunilor informatice. Autorul a clarificat natura unor termeni pur cibernetici, adaptându-i la realitatea juridică.

Cuvinte-cheie: *infracţiune informatică, atac fizic, schimb de informaţii, comandă a utilizatorului, interceptor de date, vulnerabilitate, acces superior, divulgare de informaţii, alterarea informaţiei, refuzul serviciului, furt de resurse.*

SOME ASPECTS CONCERNING THE COMPARATIVE ANALYSIS OF THE CYBER CRIMES IN THE CRIMINAL LAW OF THE REPUBLIC OF MOLDOVA AND ROMANIA

The main purpose of this scientific article consists in solving of some disputable aspects which are linked to the analysis of cyber crimes from the criminal law perspective. By means of this message there have been elucidated some questions which didn't found the relevant solution before the research, as well as there have been formulated some proposals for reform in order to improve criminal legislation in force. In order to obtain this purpose the author has analyzed the domain of the Substantive Criminal law and cybernetics, as well as has performed the comparative research of the criminal law provisions from the Republic of Moldova and Romania, on the one side, and international acts in the cybernetics, on the other. There have been formulated several definitions suitable for cyber crimes. The author has clarified the nature of some cybernetic terms, they being adapted to the juridical reality.

Keywords: *cyber crime, physical atack, information exchange, user command, data tap, vulnerability, increased access, disclosure of information, corruption of information, denial of service, theft of resources.*

Introducere

Scopul acestui articol ştiinţific este soluţionarea unor aspecte discutabile legate de analiza juridico-penală a infracţiunilor săvârşite în domeniul informaticii. Prin acest mesaj ştiinţific nu putem să epuizăm toate probleme ştiinţifice pe care le ridică încadrarea juridico-penală a infracţiunilor informatice; totodată, suntem motivaţi nu doar să elucidăm anumite puncte-problemă, dar şi să găsim soluţia promptă a acestora, să formulăm propuneri *de lege ferenda* cu scopul perfecţionării legislaţiei penale în vigoare şi, pe cale de consecinţă, cu scopul eliminării unor divergenţe pe care le provoacă aplicarea legii penale în materia infracţiunilor informatice.

Pentru a atinge scopul trasat vom purcede la analiza doctrinei din domeniul dreptului penal şi cibernetic, precum şi la analiza juridico-comparativă a legislaţiei penale interne a Republicii Moldova şi a celei a României, pe de o parte, şi a actelor internaţionale în sfera informaticii, pe de altă parte.

Totodată, în cadrul acestui studiu vor fi aduse definiţiile relevante ale infracţiunilor informatice, acestea fiind clasificate în funcţie de mai multe criterii.

Pentru a efectua o analiză juridico-penală aprofundată a infracţiunilor săvârşite în domeniul informaticii, urmează să precizăm anumite noţiuni pur cibernetice, cum ar fi categoriile de *„eveniment"*, *„ţintă"*, *„atac"*, *„acţiune"*, *„vulnerabilitate"* etc.

Astfel, pătrunzând în esenţa acestora, putem obţine mai uşor răspunsuri la anumite probleme juridice complexe. Concluziile şi recomandările vor fi utile pentru perfecţionarea cadrului normativ în vigoare al Republicii Moldova în sfera luptei cu criminalitatea informatică.

Rezultate şi discuţii

Cum se arată în doctrină, consumatorii de informaţie electronică se confruntă nu doar cu avantajele sistemului informatic – *acces imediat la orice informaţie şi interacţiune prin intermediul internetului*, ci şi cu efectele nocive ale procesului informatic – *criminalitatea informatică* [1].

Infracţiunile informatice oferă posibilităţi sporite de comitere a unor crime tradiţionale. Infracţiunile informatice presupun realizarea unor acţiuni directe sau indirecte, fizice sau logice, premeditate sau nepremeditate, având în calitate de scop modificarea uneia sau mai multor stări (confidenţialitate, integritate, accesibilitate) ale unui sistem sau subsistem informaţional [1, p.86-92].

Infracţiunile informatice sunt fapte criminale pentru a căror executare, descoperire, represiune sunt necesare cunoştinţe în domeniul tehnologiei calculatoarelor. Fiind extrem de *„flexibile"*, ele sunt în plin proces de internaţionalizare. Procesarea electronică a datelor informatice este compatibilă cu domeniul telecomunicaţiilor. Or, infracţiunile informatice sunt comise tot mai frecvent prin intermediul reţelelor de telecomunicaţii [2].

Termenul *computer crymes* desemnează faptele ilicite comise prin intermediul informaticii. Astfel, jocurile de noroc şi pariurile, vânzările online de bunuri scoase de pe piaţă, frauda informatică, furtul de identitate, falsificările, accesul nepermis la baze de date secrete, răspândirea viruşilor informatici, pornografia, violarea corespondenţei sunt doar câteva din infracţiunile comise prin intermediul sistemului informatic. Prin urmare, s-a văzut necesară instituirea unor noi norme juridice prin care aceste fapte să fie incriminate, putând astfel atrage răspunderea penală a celor care le comiteau [3, p.87].

Faptele penale de natură informatică desemnează *orice comportament ilegal, neetic sau neautorizat ce priveşte un tratament automat al datelor şi/sau o transmitere de date.*

În literatura de specialitate se face o distincţie între infracţiuni *„eventual"* informatice şi infracţiuni informatice în sens restrâns.

Infracţiunile eventual informatice *(sau infracţiuni informatice în sens larg)* sunt acelea care pot fi săvârşite şi fără a se recurge la tehnologiile informatice. De exemplu, insulta prin intermediul Internetului. Cu alte cuvinte, prin infracţiune informatică în sens larg se înţelege *orice infracţiune în care un calculator sau o reţea de calculatoare este obiectul unei infracţiuni, sau în care un calculator sau o reţea de calculatoare este instrumentul sau mediul de săvârşire a unei infracţiuni.*

Infracţiunile informatice în sens restrâns sunt acelea care antrenează sisteme informatice sau telematice, fie ca obiect material, fie ca bun protejat. Astfel, accesul abuziv la un sistem informatic, frauda informatică, răspândirea viruşilor informatici constituie exemple de infracţiuni care într-o lume fără calculatoare nu ar putea exista [3, p.87]. Cu alte cuvinte. prin infracţiune informatică în sens restrâns se înţelege *orice infracţiune în care făptuitorul interferează, fără autorizare, cu procesele de prelucrare automată a datelor* [3, p.51].

Autorul român Ramona Mihaela Moldovan opinează: *„Cu privire la aceste infracţiuni se ridică problema locului săvârşirii faptei, care atrage şi legislaţia aplicabilă, şi competenţa judecătorească. Prin natura sa, Internetul este un instrument supranaţional în care utilizatorii devin administratorii informaţiilor fără a fi uneori conştienţi de aceasta. De aceea, se consideră necesar a se reveni la principiile anterioare principiului teritorialităţii, care este greu de aplicat în aceste cazuri"* [1, p.86-92].

Conţinutul noţiunii de faptă penală de natură informatică este deosebit de variat, fiind abordat din diferite perspective în cadrul lucrărilor de specialitate. În literatura de specialitate sunt întâlnite mai multe clasificări ale infracţiunilor informatice [4]. O variaţie a unei singure liste de termeni cu definiţii este o listă de categorii. Există o divizare în şapte categorii:

(1) *Furtul de parole* – metode de a obţine parolele altor utilizatori;
(2) *Inginerie socială* – convingerea persoanelor să divulge informaţii confidenţiale;
(3) *Greşeli de programare şi portiţe lăsate special în programe* – obţinerea de avantaje de la sistemele care nu respectă specificaţiile sau înlocuirea de software cu versiuni compromise;
(4) *Defecte ale autentificării* – înfrângerea mecanismelor utilizate pentru autentificare;
(5) *Defecte ale protocoalelor* – protocoalele sunt impropriu proiectate sau implementate;
(6) *Scurgere de informaţii* – utilizarea de sisteme ca DNS pentru a obţine informaţii care sunt necesare administratorilor şi bunei funcţionări a reţelei, dar care pot fi folosite şi de atacatori;
(7) *Refuzul serviciului* – încercarea de a opri utilizatorii de a utiliza sistemele lor [3].

În doctrină se susţine că un profil *„clasic"* al făptuitorilor acestor infracţiuni poate fi rezumat astfel: bărbat cu vârsta cuprinsă între 15 şi 45 de ani, având un statut social bun, fără antecedente penale, inteligent şi motivat. În multe cazuri, autorul este chiar salariat al întreprinderii atacate sau cunoaşte modul de funcţionare a sistemului atacat. Criteriile de delimitare a acestor tipologii sunt în principal două: primul – motivaţiile autorilor, precum şi consecinţele legale ale acestora; cel de-al doilea criteriu introduce o distincţie între acţiunile care au ca scop fie producerea de pagube, fie un folos necuvenit, şi acţiunile justificate de curiozitate sau explicate de motive pedagogice [3].

Conceptele de bază ale securității legate de oamenii care utilizează aceste informații sunt *autentificarea*, *autorizarea* şi *acceptarea*.

Trei ***concepte de bază ale securității***, importante în ceea ce priveşte informațiile de pe Internet, sunt *confidențialitatea, integritatea* şi *disponibilitatea*.

Când informația este citită şi copiată de cineva neautorizat, rezultatul este cunoscut ca pierderea ***confidențialității***. Pentru câteva tipuri de informații, confidențialitatea este un atribut foarte important. Exemplele includ date obținute din cercetare, înregistrări medicale şi de asigurări, specificații ale noilor produse şi strategii de investiții corporatiste. În unele locuri, s-ar putea să existe o obligație legală pentru protecția intimității persoanelor. Aceasta este adevărată pentru bănci şi companii de credit, spitale, cabinete medicale, laboratoare de testare medicală, cabinete psihologice şi agenții care colectează taxe.

Informația poate fi alterată când este disponibilă pe o rețea nesigură. Când informația este modificată în moduri neaşteptate, rezultatul e cunoscut drept pierderea ***integrității***. Aceasta înseamnă că datele suferă modificări neautorizate fie ca urmare a unei greşeli umane, fie prin modificare intenționată. Integritatea este importantă în mod particular pentru siguranța critică a datelor financiare utilizate în activități ca transferuri electronice de fonduri, în controlul traficului aerian şi în contabilitatea financiară.

Informația poate fi ştearsă sau poate deveni inaccesibilă, rezultând o *lipsă de* ***disponibilitate***. Aceasta înseamnă că persoanele care sunt autorizate să obțină informații nu pot obține ceea ce doresc. Disponibilitatea este deseori cel mai important atribut în afacerile orientate pe servicii care depind de informații (programări aeriene şi sisteme de inventar on-line). Disponibilitatea rețelei e importantă pentru orice persoană a cărei afacere sau educație depinde de o conectare la rețea. Când un utilizator nu poate accesa rețeaua sau un serviciu specific furnizat pe rețea, el experimentează un refuz al serviciului [3].

Operarea calculatoarelor şi a rețelelor se compune dintr-un şir de *evenimente*. Un eveniment reprezintă schimbarea stării unui sistem sau dispozitiv. Din punctul de vedere al securității informatice, aceste schimbări de stare apar ca urmare a unor *acțiuni* care sunt îndreptate asupra unor *ținte*. Un exemplu de acțiune este de a accesa un sistem de calcul. În acest caz, acțiunea este *autentificarea* de către programul de control a accesului utilizatorului, conform unei identități controlate de nume de utilizator şi parolă [3].

Evenimentul, din punctul de vedere al unui calculator sau al unei rețele de calculatoare, constituie o acțiune realizată asupra unui sistem țintă prin care se intenționează schimbarea stării sistemului. *Acțiunea* (sondare; scanare; inundare; autentificare; evitare; simulare; citire; copiere; furt; modificare; ştergere) – un demers al unui utilizator sau program, cu scopul de a obține un rezultat. *Ținta* (cont; proces; dată; componentă; calculator; rețea; internet) – o entitate logică a unei rețele sau sistem de calcul (cont de utilizator, program sau date) sau o entitate fizică (PC, rețea) [5].

Uneori, un eveniment care are loc pe un computer sau o rețea este parte a unei serii de paşi ce intenționează să producă un eveniment neautorizat. Acest eveniment este apoi considerat parte a unui *atac*.

Un atac are mai multe elemente:

- În primul rând, e format din mai mulți paşi pe care atacatorul îi face. Printre aceşti paşi regăsim o *acțiune* îndreptată către o *țintă*, precum şi utilizarea unei *unelte* pentru a *exploata* o *vulnerabilitate*.
- În al doilea rând, un atac intenționează să obțină un *rezultat neautorizat*, privit din perspectiva utilizatorului sau administratorului sistemului în cauză.
- În final, un atac reprezintă o serie de etape voluntare pe care atacatorul le realizează, acest lucru diferențiind un atac de o secvență de acțiuni normale.

Conceptul de *autorizat* contra *neautorizat* este cheia pentru a înțelege ce diferențiază un atac de evenimente normale care au loc:

- ✓ *autorizat* – aprobate de utilizator sau administrator;
- ✓ *neautorizat* – care nu sunt aprobate de utilizator sau administrator.

Unealta este o modalitate de a exploata vulnerabilitatea unui computer sau a unei rețele. Categoriile de unelte folosite sunt următoarele: *Atac fizic* (*physical atack*); *Schimbul de informații* (*information exchange*); *Comandă a utilizatorului* (*user command*); *Script sau program* (*script or program*); *Agent independent* (*autonomous agent*); *Viruşii*; *Programe integrate* (*toolkit*); *Unelte distribuite* (*distributed tools*); *Interceptor de date* (*data tap*).

Pentru a obţine rezultatele pe care le doreşte, un atacator trebuie să se folosească de o ***vulnerabilitate*** a calculatorului sau a reţelei. *Vulnerabilitatea* (*vulnerability*) este o slăbiciune a sistemului care permite o acţiune neautorizată. Acestea sunt erori ce apar în diferite faze ale dezvoltării, respectiv folosirii sistemelor şi pot fi clasificate în următoarele categorii: *Vulnerabilitate de proiectare* (*design vulnerability*); *Vulnerabilitate de implementare* (*implementation vulnerability*); *Vulnerabilitate de configurare* (*configuration vulnerability*).

Rezultatul neautorizat este o consecinţă neautorizată a unui eveniment: *acces superior* (*increased access*); *divulgare de informaţii* (*disclosure of information*); *alterarea informaţiei* (*corruption of information*); *refuzul serviciului* (*denial of service*); *furt de resurse* (*theft of resources*).

În funcţie de rolul sistemelor informatice în comiterea infracţiunii, infracţiunile informatice se clasifică în:

- *infracţiuni săvârşite cu ajutorul sistemelor informatice*, în care sistemele informatice constituie un instrument de facilitare a comiterii unor infracţiuni. Este vorba despre infracţiuni „tradiţionale" perfecţionate prin utilizarea sistemelor informatice *şi*
- *infracţiuni săvârşite prin intermediul sistemelor informatice*, în care sistemele informatice, incluzând şi datele stocate în acestea, constituie ţinta infracţiunii. Aceste infracţiuni pot fi săvârşite doar prin intermediul sistemelor informatice. Ele au făcut obiect de reglementare în ultimii ani. Amintim aici şi un alt rol pe care îl au sistemele informatice.

În conformitate cu art.1 al Convenţiei Consiliului Europei privind criminalitatea informatică, nr.185 *(ulterior în text – Convenţie),* expresia *sistem informatic* desemnează orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură, care asigură ori dintre care unul sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor; expresia *date informatice* desemnează orice reprezentare de fapte, informaţii sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcţii de către un sistem informatic; expresia *furnizor de servicii* desemnează: orice entitate publică sau privată care oferă utilizatorilor serviciilor sale posibilitatea de a comunica prin intermediul unui sistem informatic şi orice altă entitate care prelucrează sau stochează date informatice pentru acest serviciu de comunicaţii sau pentru utilizatorii săi; iar *datele referitoare la trafic* desemnează orice date având legătură cu o comunicare transmisă printr-un sistem informatic, produse de acest sistem în calitate de element al lanţului de comunicare, indicând originea, destinaţia, itinerarul, ora, data, mărimea, durata sau tipul de serviciu subiacent.

Convenţia clasifică infracţiunile săvârşite în domeniul informaticii în următoarele patru categorii:

(1) Infracţiuni împotriva confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice (accesarea ilegală; interceptarea ilegală; afectarea integrităţii datelor; afectarea integrităţii sistemului; abuzurile asupra dispozitivelor);
(2) Infracţiuni informatice (falsificarea informatică; frauda informatică);
(3) Infracţiuni referitoare la conţinut (infracţiuni referitoare la pornografia infantilă);
(4) Infracţiuni referitoare la atingerile aduse proprietăţii intelectuale şi drepturilor conexe.

Codul penal al Republicii Moldova incriminează infracţiunile informatice şi infracţiunile în domeniul telecomunicaţiilor în Capitolul IX al Părţii Speciale:

(1) Accesul ilegal la informaţia computerizată (art.259 CP RM) – corespunde faptei de *„acesare ilegală"* incriminate de Convenţie;
(2) Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau produselor program (art.260 CP RM) – corespunde faptei de *„abuzuri asupra dispozitivelor"* incriminate de Convenţie;
(3) Interceptarea ilegală a unei transmisii de date informatice (art.260^1 CP RM) – corespunde faptei de *„interceptare ilegală"* incriminate de Convenţie;
(4) Alterarea integrităţii datelor informatice ţinute într-un sistem informatic (art.260^2 CP RM) – corespunde faptei de *„afectare a integrităţii datelor"* incriminate de Convenţie;
(5) Perturbarea funcţionării sistemului informatic (art.260^3 CP RM) – corespunde faptei de *„afectare a integrităţii sistemului"* incriminate de Convenţie;
(6) Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a parolelor, codurilor de acces sau a datelor similare (art.260^4 CP RM) – corespunde faptei de *„atingeri aduse proprietăţii intelectuale şi drepturilor conexe"* incriminate de Convenţie;

(7) Falsul informatic (art.260[5] CP RM) – corespunde faptei de *„falsificare informatică"* incriminate de Convenție;
(8) Frauda informatică (art.260[6] CP RM) – corespunde faptei de *„fraudă informatică"* incriminate de Convenție;
(9) Încălcarea regulilor de securitate a sistemului informatic (art.261 CP RM) – corespunde faptei de *„afectare a integrității sistemului"* incriminate de Convenție;
(10) Pornografia infantilă (art.208[1] CP RM) este incriminată separat în cadrul Capitolului VII al Părții Speciale (Infracțiuni contra familiei şi minorilor) şi corespunde *infracțiunilor referitoare la conținut* prevăzute de Convenție.

Codul penal al României (aprobat prin Legea nr.286/2009) prevede următoarele fapte penale comise în domeniul informaticii:

(1) *Fraude comise prin sisteme informatice şi mijloace de plată electronice* (frauda informatică (art.249 C.pen.Rom.); efectuarea de operațiuni financiare în mod fraudulos (art.250 C.pen.Rom.); acceptarea operațiunilor financiare efectuate în mod fraudulos (art.251 C.pen.Rom.));
(2) *Infracțiuni contra siguranței şi integrității sistemelor şi datelor informatice* (accesul ilegal la un sistem informatic (art.360 C.pen.Rom.); interceptarea ilegală a unei transmisii de date informatice (art.361 C.pen.Rom.); alterarea integrității datelor informatice (art.362 C.pen.Rom.); perturbarea funcționării sistemelor informatice (art.363 C.pen.Rom.); transferul neautorizat de date informatice (art.364 C.pen.Rom.); operațiunii ilegale cu dispozitive sau programe informatice (art.365 C.pen.Rom.));
(3) *Infracțiuni de fals* (falsul informatic (art.325 C.pen.Rom));
(4) *Alte infracțiuni care sunt săvârşite în domeniul informaticii* (pornografia infantilă (art.374 C.pen.Rom.); falsificarea documentelor şi evidențelor electorale (art.391 C.pen.Rom.)).

Dacă vom corobora prevederile Convenției cu incriminările din Codul penal al României, observăm următoarele:

(1) Frauda informatică (art.249 C.pen.Rom.) corespunde faptei de *„fraudă informatică"* incriminate de Convenție;
(2) Efectuarea de operațiuni financiare în mod fraudulos (art.250 C.pen.Rom.) corespunde faptei de *„fraudă informatică"* incriminate de Convenție;
(3) Acceptarea operațiunilor financiare efectuate în mod fraudulos (art.251 C.pen.Rom.) corespunde faptei de *„fraudă informatică"* incriminate de Convenție;
(4) Accesul ilegal la un sistem informatic (art.360 C.pen.Rom.) – corespunde faptei de *„acesare ilegală"* incriminate de Convenție;
(5) Interceptarea ilegală a unei transmisii de date informatice (art.361 C.pen.Rom.) corespunde faptei de *„interceptare ilegală"* incriminate de Convenție;
(6) Alterarea integrității datelor informatice (art.362 C.pen.Rom.) corespunde faptei de *„afectare a integrității datelor"* incriminate de Convenție;
(7) Perturbarea funcționării sistemelor informatice (art.363 C.pen.Rom.) corespunde faptei de *„afectare a integrității sistemului"* incriminate de Convenție;
(8) Transferul neautorizat de date informatice (art.364 C.pen.Rom.) corespunde faptei de *„atingeri aduse proprietății intelectuale şi drepturilor conexe"* incriminate de Convenție;
(9) Operațiunii ilegale cu dispozitive sau programe informatice (art.365 C.pen.Rom.) corespunde faptei de *„abuzuri asupra dispozitivelor"* incriminate de Convenție;
(10) Falsul informatic (art.325 C.pen.Rom) corespunde faptei de *„falsificare informatică"* incriminate de Convenție;
(11) Pornografia infantilă (art.374 C.pen.Rom.) – corespunde *infracțiunilor referitoare la conținut* prevăzute de Convenție;
(12) Falsificarea documentelor şi evidențelor electorale (art.391 C.pen.Rom.) corespunde faptei de *„falsificare informatică"* incriminate de Convenție.

STUDIA UNIVERSITATIS MOLDAVIAE, 2016, nr.3(93)
Seria "Ştiinţe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.39-46

Tabel

Analiza comparativă a normelor ce incriminează faptele infracţionale săvârşite în domeniul informaticii la nivel intern (Republica Moldova, România) şi internaţional (Convenţia privind criminalitatea informatică)

	Convenţia privind criminalitatea informatică	***Codul penal al Republicii Moldova din 18 aprilie 2002***	***Codul penal al României, aprobat prin Legea nr.286/2009***
1.	Infracţiuni împotriva confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice		
a.	*accesarea ilegală;*	Accesul ilegal la informaţia computerizată *(art.259 CP RM)*	Accesul ilegal la un sistem informatic *(art.360 C.pen.Rom.)*
b.	*interceptarea ilegală;*	Interceptarea ilegală a unei transmisii de date informatice *(art.260[1] CP RM)*	Interceptarea ilegală a unei transmisii de date informatice *(art.361 C.pen.Rom.)*
c.	*afectarea integrităţii datelor;*	Alterarea integrităţii datelor informatice ţinute într-un sistem informatic *(art.260[2] CP RM)*	Alterarea integrităţii datelor informatice *(art.362 C.pen.Rom.)*
d.	*afectarea integrităţii sistemului;*	Perturbarea funcţionării sistemului informatic *(art.260[3] CP RM)* Încălcarea regulilor de securitate a sistemului informatic *(art.261 CP RM)*	Perturbarea funcţionării sistemelor informatice *(art.363 C.pen.Rom.)*
e.	*abuzurile asupra dispozitivelor*	Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau produselor program *(art.260 CP RM)*	Operaţiunii ilegale cu dispozitive sau programe informatice *(art.365 C.pen.Rom.)*
2.	Infracţiuni informatice		
a.	*falsificarea informatică;*	Falsul informatic *(art.260[5] CP RM)*	Falsul informatic *(art.325 C.pen.Rom)* Falsificarea documentelor şi evidenţelor electorale *(art.391 C.pen.Rom.)*
b.	*frauda informatică*	Frauda informatică *(art.260[6] CP RM)*	Frauda informatică *(art.249 C.pen.Rom.);* Efectuarea de operaţiuni financiare în mod fraudulos *(art.250 C.pen.Rom.);* Acceptarea operaţiunilor financiare efectuate în mod fraudulos *(art.251 C.pen.Rom.)*
3.	Infracţiuni referitoare la conţinut		
a.	*infracţiuni referitoare la pornografia infantilă*	Pornografia infantilă *(art.208[1] CP RM)*	Pornografia infantilă *(art.374 C.pen.Rom.)*
4.	Atingeri aduse proprietăţii intelectuale şi drepturilor conexe	Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a parolelor, codurilor de acces sau a datelor similare *(art.260[4] CP RM)*	Transferul neautorizat de date informatice *(art.364 C.pen.Rom.)*

Concluzii

În opinia noastră, infracţiunile informatice pot fi clasificate în funcţie de obiectul atentării formând următoarele categorii:

- infracţiuni informatice ce aduc atingeri dreptului la viaţă privată (încălcarea inviolabilităţii vieţii private; persecutarea electronică a victimei; încălcarea dreptului la corespondenţă etc.);
- infracţiuni informatice frauduloase cu caracter economico-financiar ce atentează la proprietatea financiară a victimei (efectuarea operaţiunilor financiare frauduloase prin intermediul programelor şi uneltelor electronice etc.);
- infracţiuni informatice ce aduc atingere intereselor statului şi securităţii acestuia (spionajul informatic etc.);
- infracţiuni informatice ce aduc atingere drepturilor de autor şi altor drepturi conexe (pirateria programelor pentru calculator etc.);
- infracţiuni informatice ce aduc atingere securităţii publice (sabotajul informatic etc.);
- infracţiuni informatice ce aduc atingere conviețuirii paşnice şi moravurilor sociale (propagandă rasistă, extremistă, difuzare de materiale pornografice, cu idei suicidare etc.).

Atragem atenţia că, spre deosebire de legea penală a Republicii Moldova care a asimilat definiţia utilizată în Convenţie, frauda informatică în accepţiunea legiuitorului român cuprinde trei norme juridico-penale de sine stătătoare: frauda informatică *(art.249 C.pen.Rom.);* efectuarea de operaţiuni financiare în mod fraudulos *(art.250 C.pen.Rom.);* acceptarea operaţiunilor financiare efectuate în mod fraudulos *(art.251 C.pen.Rom.)*. Astfel, legiuitorul român incriminează:

- **Frauda informatică (art.249 C.pen.Rom.)**: Introducerea, modificarea sau ştergerea de date informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, daca s-a cauzat o pagubă unei persoane.
- **Efectuarea de operaţiuni financiare în mod fraudulos (art.250 C.pen.Rom.)**:
  - Efectuarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utilizarea, fără consimţământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia *(alin.(1));*
  - Efectuarea uneia dintre operaţiunile prevăzute în alin.(1), prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive *(alin.(2));*
  - Transmiterea neautorizată către altă persoană a oricăror date de identificare, în vederea efectuării uneia dintre operaţiunile prevăzute în alin.(1) *(alin.(3))*.
- **Acceptarea operaţiunilor financiare efectuate în mod fraudulos (art.251 C.pen.Rom.)**:
  - Acceptarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând ca este efectuată prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimţământul titularului său *(alin.(1));*
  - Acceptarea uneia dintre operaţiunile prevăzute în alin.(1), cunoscând că este efectuată prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive *(alin.(2))*.

Observăm că două din ele atentează la relaţiile sociale care protejează patrimoniul financiar al unei persoane, atunci când prezenţa respectivei persoane în spaţiul cibernetic se cuantifică într-un anumit volum de date stocate într-un sistem informatic sau vehiculate într-o reţea. Mai mult, efectuând o comparare simplă a legii penale autohtone şi a legii penale române, se scoate în evidenţa un domeniu cibernetic suficient de larg, care rămâne a fi neacoperit de legea penală a Republicii Moldova, şi anume – domeniul efectuării operaţiunilor financiare frauduloase *„prin utilizarea, fără consimţământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia"*, sau *„prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimţământul titularului său"*, sau *„prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive"*.

Astfel, în conformitate cu rezumatul Deciziei nr.3574 din 13 octombrie 2011 ***(Arhiva Înaltei Curţi de Casaţie şi Justiţie a României. Secţia penală. Decizia nr.3574 din 13 octombrie 2011),*** *transmiterea neautorizată, la diferite intervale de timp, dar în realizarea aceleiaşi rezoluţii infracţionale, prin intermediul unui sistem informatic, către mai multe persoane, a datelor de identificare care permit utilizarea unor cărţi de*

credit, fără consimţământul titularilor acestora, în vederea retragerii de numerar din conturile titularilor, întruneşte elementele constitutive ale infracţiunii de efectuare de operaţiuni financiare în mod fraudulos. Fapta de a crea, la diferite intervale de timp, dar în realizarea aceleiaşi rezoluţii infracţionale, pagini web după modelul unor website-uri financiare, prin care se solicită clienţilor unor bănci furnizarea unor date confidenţiale de identificare care permit utilizarea cardurilor, pagini postate, fără drept, pe serverele unor firme cu bună reputaţie şi trimise la mai multe adrese de e-mail, urmând ca datele cardurilor dezvăluite de către clienţi să fie folosite fără drept, constituie infracţiunea de acces, fără drept, la un sistem informatic [6].

În opinia noastră, introducerea în legea penală a normelor speciale care ar sancţiona efectuarea de operaţiuni financiare în mod fraudulos prin metode enumerate *supra* ar contribui la asigurarea consecutivităţii legii penale, pe de o parte, şi la îmbunătăţirea practicii judiciare de aplicare a normelor ce sancţionează frauda informatică, contracarând aplicarea legii penale prin analogie (interzisă expres de Codul penal al Republicii Moldova), când astfel de fapte sunt calificate ca escrocherie, ce ni se impune a fi inadmisibil. Considerăm că norma juridico-penală prevăzută la art.260^6 CP RM, fiind una generală şi lăsând neacoperită o gamă largă de fapte prejudiciabile, nu rezistă realităţii juridice şi economico-financiare.

Totodată, Codul penal al României prevede şi anumite expresii care, în opinia noastră, sunt binevenite şi în legea penală a Republicii Moldova în cadrul Părţii Generale a acesteia. Astfel, în art.181 C.pen.Rom. legiuitorul defineşte două noţiuni – *sistem informatic* şi *date informatice*. Ţinând cont de aceste novele, propunem introducerea definiţiilor identice şi în legea penală autohtonă, după cum urmează:

- *Prin sistem informatic* se înţelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic.
- *Prin date informatice* se înţelege orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic.

Referinţe:

1. MOLDOVAN, R.M. Traficul de persoane în spaţiul virtual. În: *Curentul Juridic*, p.86-92. http://www.scipio.ro/documents/204712/a85b336c-e019-474c-b441-c34a3b6797dd
2. CIOPEC, F., ROIBU, M. *Infracţiunile informatice – crime invizibile*. http://drept.uvt.ro/documents/Anale_UVT_Drept_1-2.2008_final-Infractiunile-informatice---crime-invizibile.pdf
3. *Ghid introductiv pentru aplicarea dispoziţiilor legale referitoare la criminalitatea informatică*. Bucureşti, 2004, p.86 http://andrei.clubcisco.ro/cursuri/f/f-sym/5master/aac-msi/Ghid%20cybercrime%20-%20vers%20finala.pdf
4. POONIA, A.S. Cyber Crime: Challenges and its Classification. In: *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, Volume 3, Issue 6, November-December 2014. (ISSN 2278-6856) http://www.ijettcs.org/Volume3Issue6/IJETTCS-2014-12-08-96.pdf
5. MCGUIRE, M., DOWLING, S. *Cyber crime: A review of the evidence Research Report 75 Chapter 1: Cyber-dependent crimes.* October 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf
6. Arhiva Înaltei Curţi de Casaţie şi Justiţie a României. Secţia penală. Decizia nr.3574 din 13 octombrie 2011.

Prezentat la 10.05.2016