CZU 343.9

CRIMINALITATEA INFORMATICĂ
COMPUTER CRIME

Anna NAGHERNEAC[1]

Abstract: *The article is devoted to the phenomenon of computer crime, of major magnitude in contemporary society. It is argued the need to use information technologies with great responsibility in institutions, including infodocumentation, as well as the importance of continuous training of employees, in order to obtain knowledge in the field of digital education, to ensure a high degree of cyber security.*
Keywords: *computer crime, information technologies, digital education, cybernetic security*

Pe parcursul ultimelor decenii, spaţiul cibernetic a avut un imens impact asupra tuturor componentelor societăţii umane. Evoluţia umanităţii şi activităţile societăţii moderne, apărarea drepturilor fundamentale, interacţiunile economice şi sociale depind tot mai mult de infrastructurile de comunicaţii şi tehnologia informaţiei.

Criminalitatea informatică reprezintă o noutate pentru mulţi dintre noi, aceasta diversificându-şi modurile de operare de la o perioadă la alta, şi obţinând performanţe" îngrijorătoare o dată cu dezvoltarea noilor tehnologii. *Criminalitatea informatică reprezintă totalitatea faptelor comise în zona noilor tehnologii, într-o anumită perioadă de timp şi pe un anumit teritoriu bine determinat* [1, p. 32]. În încercarea de a defini crima informatică, frecvent au fost folosiţi termenii de „utilizare improprie" şi „utilizare abuzivă" a calculatoarelor, deşi, prezintă incidente sensibil diferite [2, p. 97]. Este cunoscut faptul că, în cercetarea criminologică, criminalitatea ca fenomen social cuprinde: c*riminalitatea reală* care presupune totalitatea faptelor penale săvârşite pe un anumit teritoriu şi într-o anumită perioadă de timp; c*riminalitatea aparentă* care cuprinde întregul set de infracţiuni semnalate organelor abilitate ale statului şi înregistrate ca atare; c*riminalitatea legală* care reprezintă totalitatea faptelor de natură penală comise în spaţiul informatic şi pentru care s-au pronunţat hotărâri judecătoreşti definitive. Fiecare segment de criminalitate îşi are corespondenţa şi în criminalitatea informatică. Diferenţa dintre criminalitatea informatică reală şi criminalitatea informatică aparentă reprezintă *cifra neagră* a acestui nou gen de crimă şi cuprinde toate acele fapte sancţionate de legiuitor, dar, care din anumite motive rămân nedescoperite de către organele abilitate ale justiţiei penale [3, pp. 31-32].

Ca orice fenomen social, criminalitatea informatică reprezintă un sistem cu proprietăţi şi funcţii proprii, distincte calitativ de cele ale elementelor componente [4, p. 231]. Lumea criminalității informatice include, pe lângă actele infracţionale clasice (fraudă, contrafaceri, prostituţie, înşelăciune…) şi fapte proprii domeniului cibernetic (pirateria software, furtul de carduri sau falsificarea instrumentelor de plată electronice, virusarea reţelelor, terorismul electronic, hărţuirea prin e-mail etc.) Aceste fapte sunt de o ameninţare/pericol aparte, unele intrând pe terenul a ceea ce este denumit, potrivit amiralului J. Owens – *infowar* (*războiul informatic*) [5, p. 35]. Informatica a dat naştere unei multitudini de forme noi de deturnare şi abuz, care pot şi trebuie să fie considerate în egală măsură, drept acte criminale. Într-o societate care suportă repercusiunile economice şi sociale ale criminalităţii informatice, zilnic se face uz de calculatoare în aproape toate domeniile, de la controlul traficului aerian, feroviar, rutier, şi până la coordonarea serviciilor medicale şi securitatea naţională. Cea mai măruntă dificultate în funcţionarea acestor sisteme poate pune în pericol mii de vieţi omeneşti, fapt care ne demonstrează incidenţa noilor tehnologii asupra fiinţei umane, pe de o parte, şi, pe de altă parte, dependenţa societăţii faţă de noile sisteme informatizate [6, p. 19]. Accesul la bazele de date cât mai numeroase a sporit vulnerabilitatea acestor sisteme, iar ocaziile de a face uz în mod abuziv, sau de a le folosi în scopuri criminale, nu au întârziat să apară. Criminalitatea informatică poate să aibă un preţ foarte ridicat pe plan economic, dar şi în termenii securităţii umane. Marile reţele

[1] Bibliotecară principală, Biblioteca Ştiinţifică a USARB, ana.nagherneac@gmail.com, [ORDCI:0000-0002-8300-0748]

informatice au avut o ascensiune extrem de rapidă, atât în plan naţional, cât, mai ales, în plan internaţional, făcând posibilă accesarea a numeroase sisteme, atât prin legături telefonice (fixe) cât şi prin intermediul telefoniei (mobile). Cele mai răspândite infracţiuni care pot fi comise cu ajutorul computerului:

Folosirea neautorizată a computerului (pătrunderea în baza de date a computerelor, infractorii modifică sau distrug din informaţiile stocate, ori din programele de computer ale altei persoane. *Furtul de servicii.* În ultima perioadă de timp, tot mai multe servicii sunt plătite cu ajutorul cărţilor de credit sau debit. Într-un asemenea context, oricine încearcă să obţină un serviciu, sau să influenţeze, ori să încerce să convingă un furnizor de servicii să accepte plata acestora pe baza cărţilor de credit/ debit, având cunoştinţă că acestea sunt furate, comite o faptă care îl plasează în afara legii. *Accesarea neautorizată a sistemului de computer şi a serviciilor informatice*; *reproducerea neautorizată a programelor de soft conduce la* avarierea şi modificarea datelor computerilor şi a materialelor adiacente.

Conform Dreptului penal o faptă infracţională trebuie să îndeplinească cumulativ trei condiţii: 1) *fapta să fie comisă cu vinovăţie*; 2) *să prezinte pericol social*; 3) *să fie prevăzută de legea penală* [7]. Lipsa unuia dintre cele trei elemente esenţiale ale infracţiunii, face ca aceasta să nu fie considerată faptă de natură penală, să nu fie infracţiune. Ca atare, întreaga legislaţie penală referitoare la criminalitatea informatică va trebui să stabilească o distincţie între utilizarea improprie, accidentală, a unui sistem informatic, utilizarea improprie prin imprudenţă şi accesul intenţionat sau neautorizat, ori o utilizare abuzivă.

Plecând de la aceste considerente, apreciem că *infracţiunea informatică reprezintă o faptă comisă cu ajutorul noilor tehnologii, care trebuie să prezinte pericol social, să fie comisă cu vinovăţie şi să fie sancţionată de legea penală* [8, p. 285]. Este evident că faptele comise în câmpul virtual trebuie să fie sancţionate prin lege, ele prezentând caracteristici care evidenţiază particularitatea fiecăreia, însă, dacă se înlătură caracteristicile proprii, rămân drept caracteristici esenţiale şi comune tuturor faptelor: pericol social, vinovăţia şi incriminarea, cu corolarul său – sancţiunea. Aceste trei elemente esenţiale nu trebuie să lipsească nici în cazul infracţiunilor informatice, de aceea ele dau – prin reunirea lor – noţiunea generală de infracţiune şi, implicit de infracţiune informatică.

Este evident, că astăzi trăim într-o lume tehnologizată, în care revoluţia digitală este tot mai evidentă în multe domenii. Tehnologiile informaţionale, inteligenţa artificială, precum şi sfera roboticii nu pot fi ignorate având în vedere impactul acestor domenii în societate.

Dacă tehnologiile ar putea fi folosite doar în scopuri benefice şi nu distructive pentru omenire, evoluţia inteligenţei umane ar fi de bun augur. Prin urmare evoluţia accelerată a tehnologiei generează multe oportunităţi, dar şi multe provocări pentru societatea informaţională. Având în vedere amploarea fenomenului criminalității informatice considerăm că şi instituţiile infodocumentare pot cădea pradă fenomenului în cauză. În această ordine de idei este necesar și util să ne informăm asupra pericolelor la care ne expunem şi să fim pregătiţi pentru a le evita. Internetul trebuie protejat continuu de intervenţii criminale, abuzuri şi incidente. Pentru a face faţă provocărilor actuale este nevoie de o dezvoltarea rapidă a unor noi aptitudini, acumulare de noi cunoştinţe, de o schimbare a culturii cibernetice din partea fiecăruia, de o nouă abordare educaţională în domeniu (formele şi metodele pot fi diferite), deoarece *libertatea online necesită siguranţă şi securitate* [9]. Reglementarea spaţiului virtual trebuie să ofere soluţii problemelor legate de anonimitate, de disponibilitate în timp real la solicitările organelor de drept, de activitare a mecanismelor de blocare ale atacurilor maliţioase etc. [10]. A nu educa tinerii în ceea ce priveşte utilizarea responsabilă a noilor tehnologii, înseamnă a le limita oportunităţile şi a-i supune unor serii de riscuri. Împreună însă, familia, instituţiile de învăţământ, bibliotecile pot reduce aceste riscuri şi modela cetăţeni responsabili ai lumii digitale de mâine.

Referinţe bibliografice

1. AMZA, Tudor. *Criminologie*. *Tratat de teorie şi politică criminologică*. Bucureşti: Ed. Lumina Lex, 2002, p. 32. ISBN 973-588-492-5.
2. AMZA, Tudor, Cosmin-Petronel AMZA. *Criminalitatea informatică*. Bucureşti: Ed. LUMINA LEX, 2003, p. 97.

3. AMZA, Tudor. *Criminologie*. Bucureşti: Ed. Lumina Lex, 1998, pp. 31-32. ISBN 973-9186-33-5.
4. NISTOREANU, Gheorghe, Costică PĂUN. *Criminologie*. Bucureşti: Ed. Europoa Nova, 1996. 318 p. ISBN 973-9183-26-3.
5. OWENS, William A. Infowar. In: *Planeta internet*. 1997, nr. 2, p. 35. ISSN 1224-8274.
6. VOICU, C., I. DASCĂLU, Em. STAN. *Investigarea infracţiunilor digitale*. Bucureşti: Ed. Argument, 2002, p. 78.
7. Codul penal al Republicii Moldova: Nr. 985 din 18.04. 2002. In: *Monitorul Oficial al Republicii Moldova*. 2002, nr. 128-129 [online] [citat 13 ferbr. 2019]. Disponibil: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=286230
8. DIACONESCU, Gheorghe, Constantin DUVAC. *Tratat de drept penal*. *Partea specială*. Bucureşti: Ed. C.H. BECK, 2009, p. 285.
9. VARĂ, Octavian. *Criminalitatea informatică* [online] [citat 13 ferbr. 2019]. Disponibil: https://www.juridice.ro/wp-content/uploads/2014/11/REZUMAT-TEZA-DE-DOCTORAT-VARA-OCTAVIAN.pdf
10. ŞCHEAU, Mirce-Constantin. Educaţia în faţa provocărilor cibernetice. In: *Securitatea cibernetică: provocări şi perspective în educaţie.* Craiova: Sitech, 2020, p. 201. ISBN 978-606-11-7675-5.