Adrian Cristian MOISE

METODOLOGIA INVESTIGĂRII CRIMINALISTICE A INFRACȚIUNILOR INFORMATICE

Universul Juridic
București
-2011-

Editat de **S.C. Universul Juridic S.R.L.**

Descrierea CIP a Bibliotecii Naționale a României
MOISE, ADRIAN CRISTIAN
Metodologia investigării criminalistice a infracțiunilor informatice / Adrian Cristian Moise. - Bucureşti : Universul Juridic, 2011
Bibliogr.
ISBN 978-973-127-556-7

343:004

REDACȚIE: tel./fax: **021.314.93.13**
tel.: **0732.320.666**
e-mail: **redactie@universuljuridic.ro**

DEPARTAMENTUL DISTRIBUȚIE: telefon: **021.314.93.15; 0726.990.184**
tel./fax: **021.314.93.16**
e-mail: **distributie@universuljuridic.ro**

www.universuljuridic.ro

COMENZI ON-LINE,
CU REDUCERI DE PÂNĂ LA 15%

PREFAȚĂ

Apariția şi dezvoltarea tehnologiei informației şi comunicațiilor a determinat transformarea societății omeneşti într-o societate informațională şi, de asemenea, a creat un cadru favorabil pentru activitățile infracționale, determinând apariția unei noi forme de manifestare a criminalității, criminalitatea informatică, aceasta fiind într-o continuă dezvoltare.

Lucrarea elaborată, abordează o problemă de actualitate şi de importanță deosebită în contextul creşterii fenomenului infracțional din ultimii ani, respectiv cea a investigării criminalistice a infracțiunilor informatice.

Lucrarea intitulată ***Metodologia investigării criminalistice a infracțiunilor informatice*** poate fi considerată o lucrare bine documentată, care încearcă să clarifice un fenomen infracțional aflat în creştere nu numai pe plan internațional, dar şi în țara noastră, oferind totodată un punct de reper teoretic şi practic asupra unui domeniu relativ nou pentru țara noastră.

Caracterul de originalitate al lucrării rezultă din studiul aprofundat şi analiza sub diferite aspecte asupra fenomenului criminalității informatice şi a legislației din domeniu, precum şi din modul în care sunt prezentate în mod unitar metodologiile şi tehnicile de investigare criminalistică a infracțiunilor informatice.

Complexitatea temei a necesitat o abordare interdisciplinară, criminalitatea informatică fiind analizată din punct de vedere al dreptului penal, al dreptului procesual penal şi în mod special sub aspect criminalistic.

Prezentarea şi analiza metodologiilor şi tehnicilor de investigare criminalistică a infracțiunilor informatice în cadrul acestei lucrări reprezintă un demers ştiințific important pentru literatura română de specialitate, această lucrare remarcându-se prin noutatea problemelor tratate.

Se evidențiază numărul mare de surse bibliografice, române şi străine, care i-a permis autorului să realizeze o lucrare valoroasă din punct de vedere ştiințific, de mare utilitate teoretică şi practică.

Privită în ansamblul său, lucrarea aduce o contribuție remarcabilă în domeniul investigării criminalistice a infracțiunilor informatice şi se constituie într-o pledoarie pentru pregătirea pluridisciplinară a celor implicați în lupta împotriva acestui gen de fapte, motiv pentru care recomand cu toată căldura ca cititorul să parcurgă cu atenție bogăția de informații din această lucrare.

Prof. univ. dr. Emilian Stancu

ABREVIERI

A.C.P.O.	Association of Chief Police Officers
A.N.I.	Automatic Number Identification
A.R.P.	Address Resolution Protocol
A.T.M.	Automatted Teller Machine
A.S.C.I.I.	American Standard Code for Information Interchange
B.I.O.S.	Basic Input/Output System
C.F.A.A.	Computer Fraud and Abuse Act
C.M.O.S.	Complementary Metal Oxide Semiconductor
C.P.	Codul Penal
C.P.P.	Codul de Procedură Penală
C.V.V.	Card Verification Value
D.F.R.W.S.	Digital Forensic Research Workshop
D.H.C.P.	Dynamic Host Configuration Protocol Servers
D.I.I.C.O.T.	Direcția de Investigare a Infracțiunilor de Criminalitate Organizată şi Terorism
D.G.A.	Direcția Generală Anticorupție
D.O.S.	Denial of Service
D.N.A.	Direcția Națională Anticorupție
D.N.S.	Domain Name System
E.M.S.	Enhanced Message Service
E.N.F.S.I.	European Network of Forensic Science Institutes
E.S.N.	Electronic Serial Number
G.S.M.	Global System for Mobile Communications
G.P.S.	Global Positioning System
G.P.R.S.	General Packet Radio Service
H.L.R.	Home Location Register
H.T.M.L.	HyperText Markup Language
H.T.T.P.	HyperText Transfer Protocol
I.A.B.	Internet Activity Board
I.A.C.I.S.	International Association of Computer Investigative Specialists
I.C.A.N.N.	Internet Corporation for Assigned Names and Numbers
I.C.T.	Information and Communication Technology Intrusion Detection Systems
I.L.A.C.	International Laboratory Accreditation Cooperation
I.M.E.I.	International Mobile Equipment Identity

I.M.S.I	International Mobile Subscriber Identity
I.O.C.E.	International Organization on Computer Evidence
I.P.	Internet Protocol
I.R.C.	Internet Relay Chat
I.S.O.C.	Internet Society
I.S.P.	Internet Service Provider
I.T.	Information Technology
M.A.C.	Media Access Control
M.B.R.	Master Boot Record
M. Of.	Monitorul Oficial
N.F.A.T.	Network Forensic Analysis Tools
N.I.C.	Network Interface Card
N.I.S.T.	National Institute of Standards and Technology
N.S.R.L.	National Software Reference Library
P.I.N.	Personal Identification Number
P.I.M.	Personal Information Management
P.K.I.	Public Key Infrastructure
P.O.S.	Point of Sale
R.A.D.I.U.S.	Remote Authentication Dial In User Service
R.F.C.	Request for Comments
S.A.M.	Security Account Manager
S.E.M.	Security Event Management
S.I.M.	Subscriber Identity Module
S.M.S.	Short Message Service
S.O.P.	Standard Operating Procedure
S.W.G.D.E.	Scientific Working Group on Digital Evidence
T.C.P.	Transmission Control Protocol
U.M.T.S.	Universal Mobile Telecommunications System
U.R.L.	Uniform Resource Locator
V.L.R.	Visitor Location Register
V.O.I.P.	Voice Over IP
V.P.N.	Virtual Private Network

Capitolul I

ASPECTE INTRODUCTIVE PRIVIND FENOMENUL DE CRIMINALITATE INFORMATICĂ

1.1. Introducere

Una dintre cuceririle mari ale ştiinţei contemporane o reprezintă elaborarea noţiunii de informaţie. S-ar putea spune că noţiunea de informaţie joacă în zilele noastre rolul pe care l-a jucat elaborarea noţiunii de energie, când diferite domenii ale fizicii şi chimiei, care păreau că nu au nimic în comun, au fost apropiate, legate prin elaborarea acestei noţiuni, care a avut un rol fundamental în aceste domenii.

Ştiinţa în permanentul ei progres, prin acumulări de fapte noi, prin extinderea procesului de generalizare face posibil ca în prezent să se stabilească trăsături comune pentru ramuri, care până ieri păreau că nu au nimic în comun. Peste prăpastia care despărţea lumea fiinţelor vii de lumea mecanismelor a fost aruncată o punte. Această punte se numeşte informaţie. La mecanisme şi la fiinţele vii, pe lângă procesele energetice a căror diversitate este foarte mare, au loc şi alte procese de o natură cu totul diferită, care se prezintă unitar, şi anume au loc procese de transmitere a informaţiei.

Informaţiile sunt date care au fost organizate sau structurate într-un anumit fel, plasate într-un context şi având un înţeles[1].

Prin „dată" se înţelege un set de fapte discrete despre evenimente sau despre lumea înconjurătoare[2].

„Schimbul de informaţii ca esenţă a comunicării se realizează prin limbaj – văzut ca sistem de semnale, a cărui funcţie de bază este, după Henri Bergson, aceea de a stabili o comunicare în vederea unei cooperări"[3].

Semnalele purtătoare de informaţie pot fi semnale continue (analogice), reprezentate prin funcţii continue, în domeniul timpului sau pot fi discrete (digitale), reprezentate printr-o dublă discontinuitate în domeniul timpului şi al valorilor pe care le iau. Suportul fizic al semnalelor este variat, de la valoarea unei tensiuni electrice, la intensitatea luminoasă a unui fascicol laser. Într-o

---

[1] Ioana Vasiu, Lucian Vasiu, *Prevenirea criminalităţii informatice*, Ed. Hamangiu, 2006, Bucureşti, p. 20.

[2] *Ibidem*.

[3] Monica Şerbănescu, Ilie Botoş, Dumitru Zamfir, *Law & Crime. Net*, Ed. Tritonic, 2003, Bucureşti, p. 33.

transmisie continuă, semnalul continuu este transmis nemodificat. În transmisia discretă, semnalul continuu este în prealabil discretizat pentru ca la recepție să se refacă semnalul continuu. Transmisia discretă a semnalelor este cea mai utilizată datorită avantajelor pe care le are: stabilitate ridicată la perturbații, posibilitatea utilizării unor comunicații sigure la mari distanțe etc.[1]

Teoria transmisiei informației se bazează pe un rezultat fundamental obținut de Shannon, care constă în faptul că orice proces de transmisie este în esență un proces discret, având în vedere faptul că la recepție într-un interval finit de timp se pot distinge un număr finit de mesaje[2].

Istoria calculatorului este legată de numele lui Alan Mathison Turing, care a lansat noțiunea de calculabilitate şi a adaptat noțiunea de algoritm la calculul funcțiilor inventând o maşină abstractă şi teoretică, „maşina Turing", capabilă să rezolve orice funcție calculabilă[3].

Matematicianul Johannes von Neumann a introdus conceptul de „program înregistrat" prin introducerea programelor într-un sector al memoriei calculatorului, aceste calculatoare fiind cunoscute ca „maşinile lui Neumann"[4].

Savantul Norbert Wiener a pus bazele teoretice ale calculatorului electronic, care a fost realizat cu tuburi electronice şi a utilizat un sistem de calcul binar. Acest calculator avea posibilitatea de a efectua operații matematice şi logice, cu posibilitatea de a stoca datele şi informațiile prelucrate[5].

Descoperirea tranzistorului şi a circuitelor integrate reprezintă mari evenimente tehnologice care au contribuit la o dezvoltare fără precedent a calculatoarelor şi a tehnologiei informației, culminând cu cel mai mare eveniment tehnologic şi social în acelaşi timp, al secolului al XX-lea, Internetul.

Internetul nu reprezintă numai un fenomen tehnologic, ci şi un fenomen social, determinat de participarea utilizatorilor la dezvoltarea lui actuală[6]. Nimeni nu are o autoritate unică de conducere şi nu poate pretinde că reprezintă autoritatea Internetului.

Protocoalele care guvernează funcționarea Internetului sunt standarde benevole care sunt respectate de orice rețea care se conectează la Internet.

Aceste protocoale permit schimbul de informații de la un sistem de calcul la altul. Elaborarea standardelor se efectuează la nivelul organizației

---

[1] Ion Marghescu, Gheorghe Bădescu, *Transmiterea discretă a semnalelor*, Ed. Tehnică, 1978, Bucureşti, p. 7.

[2] Edmond Nicolau, Alexandru Popovici, *Introducere în cibernetica sistemelor hibride*, Ed. Tehnică, 1975, Bucureşti, p. 11.

[3] Monica Şerbănescu, Ilie Botoş, Dumitru Zamfir, *op. cit*., p. 10.

[4] *Ibidem*, p. 14.

[5] *Ibidem*, p. 11 şi 12.

[6] Mihai Drăgănescu, *Societatea informațională şi a cunoaşterii. Vectorii societății cunoaşterii*, p. 6, articol disponibil pe site-ul: http://www.academiaromana.ro/pro_pri/pag_com01socinf_tem.htm, consultat la 31.01.2010.

Internet Society (ISOC), care este supravegheată de un consiliu care se numeşte Internet Activity Board (IAB), acesta fiind alcătuit din specialişti care au participat la proiectarea şi punerea în practică a protocoalelor specifice Internetului. Rezolvarea problemelor de cercetare în legătură cu Internetul este realizată de grupuri de lucru formate din voluntari, acestea fiind subordonate unor grupuri de conducere aflate în supravegherea Consiliului IAB[1].

Aspectele de ordin tehnic sunt rezolvate de organizația Internet Engineering and Task Force (IETF), care are ca atribuție şi alocarea adreselor pentru cei care doresc să se conecteze la Internet.

Toate documentele importante care se referă la funcționarea şi administrarea Internetului sunt disponibile în rețea sub numele de Request for Comments (RFC) şi pot fi identificate printr-un număr format din patru cifre[2].

Dezvoltarea Internetului a determinat transformarea societății într-o societate informațională şi apariția fenomenului de globalizare. În acest sens, Academicianul Mihai Drăgănescu declară: „Este normal să gândim că şi globalizarea ca efect al Internetului să ia forma la care să participe toți participanții la globalizare. Aceasta este lecția Internetului, care s-a dovedit un mare succes în istoria tehnologică şi socială a omenirii, arătând şi calea pe care trebuie s-o urmeze procesul de globalizare, aceea a participării tuturor în moduri care urmează a fi generate în mare măsură de utilizatorii globalizării. Ca şi Internetul, globalizarea nu va putea fi strict ierarhică pentru a fi o reuşită a omenirii[3]".

Aşadar, putem spune că societatea informațională creează premisele apariției unui nou tip de societate, societatea bazată pe cunoaştere. Societatea cunoaşterii are semnificația unei noi economii în care principalul element îl constituie procesul de inovare[4].

Noua economie se caracterizează prin influența Internetului ca piață în societatea informațională şi prin recunoaşterea importanței valorii bunurilor intangibile, care sunt nemateriale, au valoare şi creează valoare[5].

La nivel internațional se manifestă un consens în terminologia Internetului, folosindu-se termenul de *cyberspace*. Acest termen a fost folosit pentru prima dată de William Gibson, în romanul science-fiction „Neuromancer"[6].

De-a lungul timpului s-a dovedit că Internetul este un sistem vulnerabil. Principalul element de vulnerabilitate îl constituie atacurile pe rețeaua Inter-

---

[1] Monica Şerbănescu, Ilie Botoş, Dumitru Zamfir, *op. cit*., p. 125.
[2] *Ibidem*.
[3] Mihai Drăgănescu, *op. cit*., p. 6.
[4] *Ibidem*, p. 38.
[5] *Ibidem*, p. 39.
[6] Pedro Verdelho, *Cybercrime and electronic evidence*, Revista Electronic Newsletter On The Fight Against Cybercrime, nr. 1/iulie 2009, p. 1, articol disponibil pe site-ul http://www.cybex.es/enac/en/presentation.html#, consultat la 31.01.2010.

net apărută într-o perioadă când nu existau astfel de probleme. Datorită rolului pe care Internetul îl are în societate, vulnerabilitatea sa devine o nouă problemă a societății umane[1].

Principalele avantaje ale rețelei Internet (accesibilitatea; uşurința în utilizare; independența de distanță; posibilitatea unor aplicații în domeniul afacerilor; surse relativ egale pentru toți utilizatorii), precum şi vulnerabilitățile sale au creat un cadru favorabil pentru activitățile criminale, determinând apariția unei noi forme de manifestare a criminalității, *criminalitatea informatică*[2].

Criminalitatea informatică şi tehnologia vor converge din ce în ce mai mult, iar infractorii din domeniul informatic utilizează noutățile tehnologice pentru a săvârşi astfel de infracțiuni în domeniul cyberspace-ului.

Noua tehnologie le conferă infractorilor din domeniul informatic posibilitatea de a se sustrage anchetelor penale[3].

1.2. Definiția noțiunii de criminalitate informatică

În ceea ce priveşte definirea noțiunii de *criminalitate informatică*, găsirea unei definiții unice, e foarte greu de realizat, problema definiției fiind punctul de pornire la orice încercare de uniformizare a incriminărilor în această materie. *Criminalitatea informatică* reprezintă o formă de criminalitate transnațională, iar punerea ei în evidență necesită cooperare internațională[4]. Aceasta poate avea şanse de reuşită numai în prezența unui cadru comun de înțelegere a problematicii şi modalităților de soluționare a acesteia.

Astfel o definiție standard şi date statistice semnificative sunt importante pentru a educa opinia publică în legătură cu amenințările informatice şi pentru a implica comunitatea în combaterea ei. Analiza infracțiunilor informatice are un rol fundamental în prevenirea fenomenului infracțional de acest tip. Înțelegerea tipurilor de infracțiuni informatice care se săvârşesc, unde şi când s-au produs, cine este implicat în acestea sunt necesare în dezvoltarea unor planuri de prevenire proactive[5].

Dacă nu utilizăm toți aceleaşi definiții sau cel puțin definiții similare, este imposibil ca personalul IT, utilizatorii sau victimele acestui tip de criminalitate, ofițerii de poliție, procurorii, judecătorii să comenteze infracțiunile informatice în mod inteligibil.

---

[1] Mihai Drăgănescu, *op. cit.*, p. 17.

[2] Monica Şerbănescu, Ilie Botoş, Dumitru Zamfir, *op. cit.*, p. 119.

[3] *Ibidem*, p. 97.

[4] Teodor Popa, *Frauda Informatică*, Ed. Universității din Oradea, 2002, Oradea, p. 70.

[5] Michael Cross, *Scene of the Cybercrime*, ed. a II-a, Ed. Syngress Publishing Inc., 2008, Rockland, Massachusetts, p. 9.

Mişcarea în direcția standardizării definiției noțiunii de criminalitate informatică este dificilă, în lipsa unui acord în privința unei terminologii de bază. Diferite încercări au fost făcute pentru a dezvolta un limbaj standard, care să descrie aspectele variate ale noțiunii de *criminalitate informatică*.

În acest context, au existat multe dezbateri între experții din acest domeniu în privința utilizării unor definiții pentru a descrie infracțiunile din domeniul informatic. În mod neîndoielnic şi dincolo de orice dezbatere, toți cercetătorii au recunoscut că fenomenul există, însă de fiecare dată definițiile date comportamentului infracțional au fost variate şi circumscrise conținutului studiilor realizate. Astfel, deşi dezbaterile durează de câțiva ani buni, tot nu s-a reuşit a se adopta o definiție internațional recunoscută a fenomenului criminalității informatice.

Chiar dacă o definiție standard a criminalității informatice nu a fost obținută, în schimb există în acest moment mai multe definiții funcționale ale acestui fenomen.

Primele încercări de definire a termenului de criminalitate informatică au avut loc în anul 1983, când Organizația pentru Cooperare şi Dezvoltare Economică a decis la Paris numirea unui comitet de experți care să analizeze problema infracțiunilor în legătură cu utilizarea calculatorului şi necesitatea modificării legislațiilor penale[1]. Acest comitet de experți şi-a finalizat activitatea în anul 1986 prin publicarea unui raport care analiza legislația curentă şi făcea propuneri în lupta împotriva criminalității informatice[2]. Tot în cadrul acestui raport s-a definit şi noțiunea de infracțiune informatică, ca fiind „orice comportament ilegal, neetic sau neautorizat ce priveşte un tratament automat de date şi/sau o transmitere de date". Totuşi se poate observa că aceşti experți nu au considerat utilă precizarea expresiei „criminalitatea informatică", în schimb au reținut o definiție funcțională, ca bază de studiu[3]. Alți experți în domeniul criminalității informatice au definit infracționalitatea informatică, drept „orice acțiune ilegală în care un calculator este instrumentul sau obiectul delictului, altfel spus, orice infracțiune al cărei mijloc sau scop este influențarea funcției calculatorului"[4]. Totodată, profesorul Tudor Amza

---

[1] *International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, Geneva 28 June-1 July 2005, Stein Schjolberg, Amanda M. Hubbard*, „Harmonizing National Legal Approaches On Cybercrime", June 2005, p. 8, disponibilă pe site-ul: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf, consultat la 18.02.2010.

[2] *International Telecommunication Union, Cybercrime Legislation Resources*, „Understanding Cybercrime: A Guide for Developing Countries", April 2009, p. 102, disponibil pe site-ul: http://www.itu.int/ITU-D/cyb/cybersecurity/legislation.html, consultat la 14.02.2010.

[3] Ioana Vasiu, *Criminalitatea Informatică*, ed. a II-a, Ed. Nemira, 2001, Bucureşti, p. 26.

[4] *Ibidem*, p. 27.

defineşte şi el termenul de „criminalitate informatică", care „reprezintă totalitatea faptelor comise în zona noilor tehnologii, într-o anumită perioadă de timp şi pe un anumit teritoriu bine determinat"[1].

Comitetul European pentru Probleme Criminale consideră că toate tentativele de definire a criminalității informatice „prezintă unele inconveniente ce nu se împacă uşor cu obiectivul conciziei formulării şi cu acela de a nu se mai lăsa nicio îndoială asupra importanței sau utilizării definiției"[2]. Toate aceste încercări de definire a criminalității informatice au condus Comitetul European pentru Probleme Criminale spre adoptarea aceleaşi definiții ca şi cea a grupului de experți ai Organizației pentru Cooperare şi Dezvoltare Economică, fără a da o definiție proprie infracționalității informatice. În final, Comitetul European pentru Probleme Criminale, adoptă expresia „criminalitatea în relație cu calculatorul" (*computer-related crime*) şi lasă la latitudinea legiuitorilor naționali de a adapta această definiție la propriul lor sistem judiciar şi la tradițiile lor istorice[3].

La nivel internațional au fost folosiți pentru prima dată termenii *criminalitate informatică* (computer crime) şi *criminalitate în legătură cu utilizarea calculatorului* (computer-related crime), în legislația Statelor Unite ale Americii (U.S. Computer Fraud and Abuse Act), cât şi în legislația Regatului Unit al Marii Britanii (U.K. Computer Abuse Act)[4]. Aceste legi se referă la un set limitat de infracțiuni, cum ar fi: furtul de servicii utilizând computerul, accesul neautorizat la computerele protejate; pirateria software şi alterarea sau furtul de informații stocate electronic; stoarcerea de bani comisă cu ajutorul computerului, accesul neautorizat în rețelele bancare, traficul cu parole furate şi transmiterea de viruşi distructivi sau comenzi.

Una dintre principalele dificultăți în definirea criminalității informatice este situația care apare, când computerul sau rețeaua nu sunt implicate direct într-o infracțiune, dar încă conțin probe digitale în legătură cu infracțiunea. De exemplu, un suspect care pretinde că utiliza Internetul în momentul săvârşirii unei infracțiuni. Cu toate că, computerul nu a jucat nici un rol în comiterea infracțiunii, totuşi el conține probe digitale importante în legătură cu infracțiunea. Aşadar, pentru a adapta acest tip de situație, termenul de infracțiune

---

[1] Tudor Amza, Cosmin-Petronel Amza, *Criminalitatea Informatică*, Ed. Lumina Lex, 2003, Bucureşti, p. 13.

[2] Maxim Dobrinoiu, *Infracțiuni în domeniul informatic*, Ed. C.H. Beck, 2006, Bucureşti, p. 62.

[3] *Ibidem*, p. 63.

[4] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, ed. a II-a, Ed. Elsevier Academic Press, 2004, San Diego, California, p. 19.

în legătură cu utilizarea calculatorului (*computer-related crime*) este utilizat în infracțiuni care implică computere şi rețele, cât şi în infracțiuni care nu implică computerul în comiterea infracțiunii (rolul computerului fiind de a depozita probe digitale referitoare la infracțiune)[1].

În privința definirii termenului de „infracționalitate informatică", şi Organizația Națiunilor Unite a acceptat utilizarea concomitentă a celor doi termeni (*computer crime* şi *computer-related crime*), considerându-i echivalenți din punctul de vedere al semnificației pe care o reprezintă[2]. Tot în acelaşi document al Organizației Națiunilor Unite se subliniază şi diferența în ceea ce priveşte semnificația termenilor: „abuz informatic" (*computer abuse*) şi „utilizarea greşită a calculatorului" (*computer misuse*). Primul termen, noțiunea de „abuz informatic" semnifică intenția de fraudă, prin accesul neautorizat la un computer. Al doilea termen, „utilizarea greşită a unui calculator" (*computer misuse*) se referă la acționarea greşită a unui calculator. În ceea ce priveşte intenția de fraudă putem da un exemplu: dacă un angajat primeşte o parolă de la un alt angajat pentru a accesa o anumită bază de date, atunci acest angajat nu poate fi acuzat că a comis o infracțiune, deoarece acest angajat a accesat baza de date neştiind că nu are acces la aceasta; situația este diferită când acelaşi angajat fură parola de la colegul lui pentru a accesa baza de date, dar de data aceasta el ştie că nu este autorizat să acceseze această bază de date, caz în care el va fi acuzat de comiterea unei infracțiuni.

Un alt termen des utilizat la nivel internațional în ceea ce priveşte terminologia fenomenului de *criminalitate informatică* este termenul de *criminalitate cibernetică* (cybercrime).

Cybercrime (criminalitatea cibernetică) reprezintă un termen vast şi generic care se referă la infracțiunile comise utilizând computerele şi rețeaua Internet[3].

La al zecelea Congres al Organizației Națiunilor Unite privind „Prevenirea infracțiunilor şi tratamentul infractorilor", într-o sesiune de lucru dedicată problemei infracțiunilor care au legătură cu rețelele de computer, termenul de *cybercrime* a fost definit astfel[4]:

1. **Cybercrime** în sens restrâns (*computer crime*): „Orice comportament ilegal condus prin intermediul unor operații electronice, care au ca țintă securitatea sistemelor de computer şi datele prelucrate de acestea".

---

[1] *Ibidem.*

[2] *International review of criminal policy*-United Nations Manual on the prevention and control of computer-related crime, pct. 21, disponibil pe site-ul: http://www.uncjin.org/Documents/EighthCongress.html, consultat la 31.01.2010.

[3] Michael Cross, *op. cit*., p. 2.

[4] *Ibidem*.

2. **Cybercrime** în sens larg (*computer-related crime*): „Orice comportament ilegal săvârşit prin mijlocul/sau în relația cu un sistem de computer sau rețea, care include astfel de infracțiuni cum ar fi posesia ilegală şi oferirea şi distribuirea de informații prin intermediul unui sistem de computer sau rețea".

Tot în cadrul aceluiaşi Congres au fost date exemple de infracțiuni informatice:

– accesul neautorizat;

– distrugerea datelor sau programelor din computer;

– sabotajul informatic;

– interceptarea neautorizată a comunicațiilor;

– spionajul informatic.

Termenul de *infracțiune cibernetică* (cybercrime) mai este definit şi în următorul fel: „acea faptă prevăzută de legea penală, comisă cu vinovăție, de către o persoană sau un grup de persoane care folosesc un calculator, şi, cu ajutorul comunicării informațiilor prin cablu, comit o faptă care prezintă pericol social ce aduce prejudicii unei persoane, unei societăți comerciale ori intereselor statului"[1].

Criminalitatea cibernetică (*cybercrime)* mai este definită ca „infracțiunea în care computerele şi rețeaua sunt utilizate fiecare ca ținte sau instrumente ale infracțiunii"[2].

Un alt termen utilizat în definirea criminalității informaticii este termenul *high-technology crime* (criminalitate de înaltă tehnologie).

Termenul de înaltă tehnologie (*high-technology*) poate fi definit ca o formă de dispozitive electronice cum ar fi de exemplu: computerele, telefoanele celulare şi alte dispozitive de comunicații digitale[3].

Activitatea infracțională implică utilizarea performanțelor acestor dispozitive în comiterea diferitelor infracțiuni cum ar fi de exemplu: furtul de bani sau date prin intermediul computerului; utilizarea telefoniei mobile în activitățile care privesc traficul de droguri etc.[4]

Exemple de astfel de infracțiuni informatice (*high-technology crimes*):

– hacking-ul (accesul neautorizat);

– phone phreaking-ul (accesul neautorizat într-o rețea de comunicare prin utilizarea telefonului mobil);

– child pornography (pornografia infantilă);

---

[1] Tudor Amza, Cosmin Petronel Amza, *op. cit*., p. 54.

[2] Robert Moore, *Search and Seizure of Digital Evidence*, LFB Scholary Publishing LLC, 2005, New York, p. 6.

[3] Larry Coutorie, *The future of high-technology crime: A parallel Delphi study*, Journal of Criminal Justice, vol. 23, Issue 1, 1995, p. 13-27, articol disponibil pe site-ul: http://www.sciencedirect.com/science?ob=ArticleListURL&method=list&Article, consultat la 02.02.2010.

[4] *Ibidem*.

– identity theft (furtul de identitate).

Departamentul de Justiție al Statelor Unite ale Americii (*U.S. Department of Justice*) defineşte şi el noțiunea de *criminalitate informatică* (computer crime), ca „orice încălcare a legislației penale care implică o cunoaştere a tehnologiei computerului pentru comiterea, investigarea sau incriminarea infracțiunilor”[1].

Ghidul introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică, defineşte noțiunea de infracțiune informatică, atât în sens larg, cât şi în sens restrâns, definiție care se regăseşte şi în documentele Organizației Națiunilor Unite[2]:

1. Prin **infracțiune informatică** *în sens larg* se înțelege: „orice infracțiune în care un calculator sau o rețea de calculatoare este obiectul unei infracțiuni, sau în care un calculator sau o rețea de calculatoare este instrumentul sau mediul de înfăptuire a unei infracțiuni.”

2. Prin **infracțiune informatică** *în sens restrâns* se înțelege: „orice infracțiune în care făptuitorul interferează, fără autorizare, cu procesul de prelucrare automată a datelor.”

Recomandarea nr. R(95)13 privind problemele de drept procedural penal legate de tehnologia informației a definit conceptul de *criminalitate informatică* în felul următor: „orice activități infracționale pentru care autoritățile de investigare trebuie să obțină accesul la informațiile care sunt prelucrate sau transmise în sistemele computerizate, sau în sistemele de prelucrare a datelor electronice”[3].

O altă definiție a noțiunii de *infracțiune informatică* o găsim şi în lucrarea „Black’s Law Dictionary” din anul 1999: „infracțiunea informatică reprezintă o infracțiune care necesită cunoştințe despre tehnologia computerului, cum ar fi sabotajul sau furtul datelor din computer, sau utilizarea computerului pentru a comite o altă infracțiune”[4].

---

[1] Joseph Audal, Quincy Lu, Peter Roman, *Computer Crimes*, The American Criminal Law Review, Chicago, Spring 2008, vol. 45, Issue 2, disponibil pe site-ul: http://proquest.umi.com/pqdweb?did=1485910751&sid=2&Fmt=2&clientId=65082&RQT=309&VName=PQD, consultat la 02.02.2010 .

[2] *Romanian Information Technology Initiative şi Guvernul României*, „Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică”, 2004, Bucureşti, p. 51, disponibil pe site-ul: http://www.riti-internews.ro/ro/ghid.htm, consultat la 02.02.2010.

[3] *International Telecommunication Union, WSIS Thematic Meeting on Cybersecurity, Geneva 28 June-1 July 2005, Stein Schjolberg, Amanda M. Hubbard*, „Harmonizing National Legal Approaches On Cybercrime”, June 2005, p. 4, disponibilă pe site-ul: http://www.itu.int/osg/spu/cybersecurity/presentations/session12schjolberg.pdf, consultat la 18.02.2010.

[4] Bryan A. Garner, *Black's Law Dictionary*, ed. a VII-a, Ed. West Group, 1999, Saint Paul, Minnesota, p. 377.

Din analiza tuturor definițiilor în legătură cu criminalitatea informatică, consider că cea mai cuprinzătoare şi inteligibilă definiție este cea prezentată în *Ghidul introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică,* şi anume definiția *infracțiunii informatice* în sens larg.

1.3. Clasificarea infracțiunilor informatice

Conținutul infracțiunilor informatice este deosebit de variat, fiind abordat din diferite puncte de vedere în cadrul lucrărilor de specialitate.

Astfel infracțiunile informatice cuprind pe lângă actele infracționale clasice (fraudă, contrafaceri, prostituție, înşelăciune) şi fapte proprii domeniului cibernetic (pirateria software, furtul de carduri sau falsificarea instrumentelor de plată electronică, virusarea rețelelor, terorismul electronic, hărțuirea prin e-mail)[1].

Recomandarea nr. R(89)9 asupra criminalității în relație cu calculatorul, una dintre cele mai importante recomandări ale Consiliului Europei, are meritul de a fi realizat o clasificare a infracțiunilor informatice în două secțiuni intitulate: lista minimală şi lista facultativă.

Lista minimală de infracțiuni cuprinde[2]:

– *Frauda în legătură cu calculatorul*: Introducerea, alterarea, ştergerea sau înlocuirea datelor sau programelor informatice, sau orice altă interferare în cursul procesării datelor care influențează rezultatul procesării datelor, prin aceasta producând pierderi economice sau orice altă pierdere în proprietatea unei alte persoane cu intenția de a obține un câştig economic ilegal pentru el însuşi sau pentru o altă persoană;

– *Falsul informatic*: Introducerea, alterarea, ştergerea sau înlocuirea datelor sau programelor informatice, sau orice altă interferare în cursul procesării datelor într-o manieră sau în condiții precum cele prevăzute în legea națională astfel încât ar constitui infracțiunea de fals dacă ar fi fost comisă cu un obiect tradițional al unui asemenea tip de infracțiune;

– *Deteriorarea datelor sau a programelor informatice*: Ştergerea, deteriorarea sau înlocuirea datelor sau programelor informatice fără drept;

– *Sabotajul informatic*: Introducerea, alterarea, ştergerea sau înlocuirea datelor sau programelor informatice sau interferarea cu sistemele informatice, cu intenția de a împiedica funcționarea calculatorului sau a sistemului de telecomunicații;

– *Accesul neautorizat*: Accesarea fără drept a unui sistem informatic sau a unei rețele prin violarea măsurilor de securitate;

---

[1] Emilian Stancu, *Tratat de Criminalistică*, ed. a III-a, Ed. Universul Juridic, 2004, Bucureşti, p. 697.

[2] *International review of criminal policy* – United Nations Manual on the prevention and control of computer–related crime, pct. 121, disponibil pe site-ul: http://www.uncjin.org/Documents/EighthCongress.html, consultat la 31.01.2010.

– *Interceptarea neautorizată*: Interceptarea făcută fără drept şi prin măsuri tehnice, a comunicațiilor la, de la şi în cadrul unui sistem informatic sau a unei rețele;

– *Reproducerea neautorizată a programelor informatice protejate*: Reproducerea, distribuirea sau comunicarea către public fără drept a unui program informatic care este protejat de lege;

– *Reproducerea neautorizată a unei topografii*: Reproducerea fără drept a unei topografii protejată de lege, a unui produs semiconductor, sau o exploatare comercială sau importul pentru acest scop, făcute fără drept, a unei topografii sau a unui produs semiconductor realizat prin folosirea topografiei.

Lista opțională de infracțiuni cuprinde[1]:

– *Alterarea datelor sau programelor informatice*: Alterarea datelor sau programelor fără drept;

– *Spionajul informatic*: Însuşirea prin mijloace improprii sau divulgarea, transferul sau folosirea unui secret comercial fără drept sau orice altă justificare legală, cu intenția de a cauza o pierdere economică unei persoane care are dreptul de a deține acel secret, sau de a obține un avantaj economic ilegal pentru sine sau pentru o terță persoană;

– *Utilizarea neautorizată a unui calculator*: Folosirea unui sistem computerizat sau a unei rețele fără drept care fie:

i. Este făcută cu acceptarea riscului unei pierderi semnificative cauzate persoanei îndreptățite de a folosi sistemul sau dăunează sistemului sau funcționării sale; sau

ii. Este făcută cu intenția de a cauza pierderi persoanei îndreptățite de a folosi sistemul sau de a dăuna sistemului sau funcționării sale; sau

iii. Produce pierderi persoanei îndreptățite de a folosi sistemul sau dăunează sistemului sau funcționării sale;

– *Utilizarea neautorizată a unui program informatic protejat*: Folosirea fără drept a unui program informatic care este protejat de lege şi care a fost copiat fără drept cu intenția de a obține un câştig economic, ilegal pentru sine sau pentru o altă persoană sau de a cauza daune deținătorului acestui drept.

O altă clasificare importantă a infracțiunilor informatice, este prezentată în „Manualul Națiunilor Unite pentru prevenirea şi controlul infracțiunilor informatice", în care sunt enumerate cinci dintre cele mai răspândite infracțiuni informatice[2]:

1) Frauda prin manipularea computerului

---

[1] *International review of criminal policy* – United Nations Manual on the prevention and control of computer–related crime, pct. 122, disponibil pe site-ul: http://www.uncjin.org/Documents/EighthCongress.html. consultat la 31.01.2010.

[2] *International review of criminal policy* – United Nations Manual on the prevention and control of computer–related crime, pct. 61-83, disponibil pe site-ul: http://www.uncjin.org/Documents/EighthCongress.html. consultat la 31.01.2010.

Frauda informatică realizată prin manipularea datelor de intrare este cea mai des întâlnită infracțiune informatică, deoarece este uşor de comis şi greu de detectat.

Aceasta nu necesită cunoştințe informatice sofisticate şi poate fi comisă de către oricine are acces la funcțiile normale de prelucrare de date în faza de intrare a acestora.

Manipularea de programe reprezintă un alt tip de fraudă realizată prin manipularea computerului. Acest tip de fraudă implică schimbarea programelor existente în sistemul computerizat sau inserarea de noi programe sau rutine. O metodă obişnuită des utilizată o reprezintă calul troian, prin care instrucțiunile informatice sunt plasate pe ascuns într-un program computerizat, astfel încât acesta va efectua o funcție neautorizată simultan cu funcția sa normală. Un cal troian poate fi programat să se autodistrugă, fără să lase nici o probă a existenței sale în afară de probele pe care le-a produs.

Un alt tip de fraudă realizată prin manipularea computerului o reprezintă manipularea datelor de ieşire ale sistemului computerizat. Un exemplu este frauda bancomatelor realizată prin falsificarea instrucțiunilor calculatorului în etapa intrării datelor. Tradițional, o astfel de fraudă implică utilizarea de carduri bancare furate.

Mai există şi un alt tip de fraudă realizată prin manipularea computerului, care profită de repetările automate ale proceselor informatice. O astfel de manipulare este caracteristică metodei de tip „salam", prin care tranzacțiile financiare sunt extrase şi transferate în mod repetat în alt cont.

2) Falsul informatic

Atunci când datele sunt modificate în legătură cu documentele stocate în formă computerizată, infracțiunea care se săvârşeşte este cea de fals informatic, caz în care sistemele computerizate sunt ținta activității infracționale.

3) Alterarea sau modificarea datelor sau a programelor pentru calculator

Această categorie de activitate infracțională implică accesul neautorizat fie direct, fie acoperit la un sistem computerizat, prin introducerea de noi programe cunoscute sub numele de „viruşi", „viermi" sau „bombe logice". Modificarea neautorizată sau ştergerea de date informatice cu intenția de a afecta funcționarea normală a sistemului reprezintă o activitate infracțională şi este adesea denumită sabotaj informatic.

Sabotajul informatic poate fi considerat un mijloc de a obține avantaje economice față de un concurent, de a promova activitățile ilegale ale unor terorişti motivați ideologic sau de a fura date sau programe cu scopul de a şantaja.

Un „virus" reprezintă o serie de coduri de program, care au proprietatea de a se ataşa la programe legitime şi de a se propaga către alte programe de calculator. Un „vierme" are aceleaşi proprietăți cu cele ale unui „virus", cu deosebirea că el nu se poate reproduce.

O „bombă logică" implică programarea distrugerii sau modificării datelor informatice într-un anumit moment din viitor.

4) Accesul neautorizat la sisteme şi servicii informatice

Accesul intenționat şi nejustificat realizat de către o persoană care este neautorizată de către proprietarii sau operatorii unui sistem poate constitui activitate infracțională.

În general, accesul neautorizat se realizează dintr-o locație îndepărtată prin intermediul unei rețele de telecomunicații, utilizând mai multe metode. Prima metodă este aceea prin care infractorul profită de măsurile lejere de securitate pentru a obține accesul, sau ar putea utiliza parole obişnuite sau parole de întreținere găsite în sistem.

A doua metodă este reprezentată de spargerea parolelor sistemelor de computere prin utilizarea unor dicționare de parole, elaborate de comunitatea infractorilor.

A treia metodă o reprezintă metoda „trapdoor" (metoda trapei) prin care accesul neautorizat este obținut prin puncte de acces create în scopuri legitime, cum ar fi de exemplu, întreținerea sistemului.

Sistemele de telecomunicații moderne, ca şi alte sisteme de computer sunt de asemenea susceptibile abuzului prin intermediul accesului de la distanță.

5) Reproducerea neautorizată a programelor informatice protejate de lege

Reproducerea neautorizată a programelor de calculator poate consta într-o pierdere economică substanțială pentru proprietarii legitimi.

Această problemă a căpătat dimensiuni transnaționale odată cu apariția traficului de astfel de reproduceri neautorizate prin intermediul rețelelor de telecomunicații moderne.

În anul 1998, în studiul „Aspectele legale ale infracționalității informatice în cadrul societății informaționale", care a fost efectuat la cererea Comisiei Europene de către profesorul Ulrich Sieber de la Universitatea din Würzburg din Germania, sunt prezentate următoarele categorii de infracțiuni informatice[1]:

1. Infracțiuni împotriva dreptului la viață privată:

– încălcări ale cerințelor formale de protecție a vieții private;

– încălcări ale drepturilor subiective la viața privată.

2. Infracțiuni economice:

– pirateria software;

– spionajul informatic;

– sabotajul informatic;

[1] Ulrich Sieber, *Legal Aspects of Computer-Related Crime in the Information Society*, p. 25-32, studiu disponibil la adresa: http://www.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html consultat la 01.02.2010.

– falsul informatic;
– frauda informatică.

3. Infracțiuni referitoare la protecția drepturilor de proprietate intelectuală, care vizează:

– programele informatice;
– bazele de date;
– semiconductorii.

4. Infracțiuni legate de utilizarea de conținuturi ilicite şi dăunătoare:

– difuzarea de materiale pornografice, materiale rasiste, xenofobe.

Convenția privind criminalitatea informatică[1] adoptată în cadrul Consiliului Europei, cuprinde nouă categorii de infracțiuni informatice, clasificându-le în patru mari titluri:[2]

1. Infracțiuni împotriva confidențialității, integrității şi disponibilității datelor şi sistemelor informatice:

– accesarea ilegală;
– interceptarea ilegală;
– afectarea integrității datelor;
– afectarea integrității sistemului;
– abuzurile asupra dispozitivelor.

2. Infracțiuni informatice:

– falsificarea informatică;
– frauda informatică.

3. Infracțiuni referitoare la conținut:

– pornografia infantilă.

4. Infracțiuni referitoare la atingerile aduse proprietății intelectuale şi drepturilor conexe:

– infracțiuni referitoare la atingerile aduse proprietății intelectuale şi drepturilor conexe.

Legea nr. 161/2003[3] privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției, introduce o serie de infracțiuni care corespund clasificărilor şi definițiilor prezentate în cuprinsul Convenției Consiliului Europei privind criminalitatea informatică. Aşadar, aceste infracțiuni sunt prezentate în Capitolul al III-lea din Titlul III „Prevenirea şi combaterea criminalității informatice" al Legii nr. 161/2003:

---

[1] *Convenția Consiliului Europei privind criminalitatea informatică* a fost ratificată de România prin Legea nr. 64/2004, publicată în M. Of. nr. 343 din 20.04.2004.

[2] *Convenția Consiliului Europei privind criminalitatea informatică* a fost semnată la Budapesta la data de 23.11.2001 şi este disponibilă pe site-ul: http://www.conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, consultat la 05.02.2010.

[3] M. Of. nr. 279 din 21.04.2003.

Infracțiuni contra confidențialității şi integrității datelor şi sistemelor informatice:

– infracțiunea de acces ilegal la un sistem informatic;

– infracțiunea de interceptare ilegală a unei transmisii de date informatice;

– infracțiunea de alterare a integrității datelor informatice;

– infracțiunea de perturbare a funcționării sistemelor informatice;

– infracțiunea de a realiza operațiuni ilegale cu dispozitive sau programe informatice.

Infracțiuni informatice:

– infracțiunea de fals informatic;

– infracțiunea de fraudă informatică.

Pornografia infantilă prin intermediul sistemelor informatice:

– infracțiunea de pornografie infantilă prin intermediul sistemelor informatice.

Comitetul European pentru Probleme Criminale prezintă de asemenea, o clasificare a infracțiunilor informatice. Astfel potrivit Comitetului European pentru Probleme Criminale, infracțiunile informatice sunt grupate în următoarele categorii:[1]

– infracțiunea de fraudă informatică;

– infracțiunea de fals în informatică;

– infracțiunea de prejudiciere a datelor sau programelor informatice;

– infracțiunea de sabotaj informatic;

– infracțiunea de acces neautorizat la un calculator;

– infracțiunea de interceptare neautorizată;

– infracțiunea de reproducere neautorizată a unui program informatic protejat de lege;

– infracțiunea de reproducere neautorizată a unei topografii;

– infracțiunea de alterare fără drept a datelor sau programelor informatice;

– infracțiunea de spionaj informatic;

– infracțiunea de utilizare neautorizată a unui calculator;

– infracțiunea de utilizare neautorizată a unui program informatic protejat de lege.

Un alt tip de clasificare a infracțiunilor informatice, pe care îl vom prezenta, este următorul[2]:

1. *Infracțiuni informatice comise prin violență*.

2. *Infracțiuni informatice săvârşite prin nonviolență*.

---

[1] Gabriel Ion Olteanu şi colectiv, *Cercetarea activităților structurilor infracționale*, Ed. Sitech, 2008, Craiova, p. 484.

[2] Michael Cross, *op. cit*., p. 15.