

Marin RUIU

*METODOLOGIA INVESTIGĂRII CRIMINALISTICE
A UNOR GENURI DE INFRAȚIUNI*

Marin RUIU

***METODOLOGIA INVESTIGĂRII
CRIMINALISTICE A UNOR GENURI
DE INFRAȚIUNI***

Universul Juridic

București

-2014-

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

Copyright © 2014, S.C. Universul Juridic S.R.L.

Toate drepturile asupra prezentei ediții aparțin

S.C. Universul Juridic S.R.L.

Nicio parte din acest volum nu poate fi copiată fără acordul scris al

S.C. Universul Juridic S.R.L.

**NICIUN EXEMPLAR DIN PREZENTUL TIRAJ NU VA FI
COMERCIALIZAT DECÂT ÎNSOȚIT DE SEMNĂTURA
ȘI ȘTAMPILA EDITORULUI, APLICATE PE INTERIORUL
ULTIMEI COPERTE.**

Descrierea CIP a Bibliotecii Naționale a României

RUIU, MARIN

**Metodologia investigării criminalistice a unor genuri
de infracțiuni / Marin Ruiu. - București : Universul Juridic,
2014**

Bibliogr.

ISBN 978-606-673-470-7

343.9

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

Aspecte introductive

Evoluția științifică la care asistăm în prezent, explozia informațională din toate domeniile, complexitatea ridicată a anumitor domenii ce prezintă interes pentru știința criminalistică, dar și schimbarea radicală a realităților sociale într-un timp foarte rapid fac dificilă integrarea în spațiul social a unor direcții de cercetare standardizate. Dificultatea rezidă din evoluția foarte rapidă a mijloacelor de operare pe care le folosesc infractorii, din nivelul de avansare a tehnologiei electronice, dar și din cauza discrepanțelor socio-economice accentuate la care asistăm. Dacă acum aproximativ o jumătate de secol specialiștii din domeniul tehnologiei electronice păseau rapid în crearea primelor suporturi de memorie pe disc, străbunicul hard-disk-ului, de o capacitate infimă ca spațiu de stocare comparativ mediile electronice de stocare actuală, în prezent putem spune că ceea ce acum jumătate de secol părea a fi o ficțiune, astăzi este o realitate socială. Relația om-tehnologie devine inseparabilă, omul ca ființă socială fiind dependent categoric de noile tehnologii.

În prezent criminalitatea informatică ocupă un loc important, poate chiar primul în lista priorităților criminalistice și criminologice actuale, fiind un fenomen cu o expansiune fulminantă la nivel atât național, cât și internațional.

Ușurința cu care poate fi manevrat un computer, dar și lacunele reglementărilor juridice oferă utilizatorilor de Internet posibilitatea de acces la o diferită gamă de instrumente de acces neautorizat și atac informatic. Cel mai grav fapt este că majoritatea instrumentelor de atac informatic sau acces neautorizat sunt disponibile pentru descărcare gratuită în marea majoritate a cazurilor, fapt ce creează pentru societatea modernă globală noi amenințări, noi pericole sociale iminente ce necesită pregătirea temeinică a unor specialiști în domeniul prevenirii infraționalității informatice, cât și o adaptabilitate în timp a acestora la evoluția tehnologică din domeniul informatic.

În mare parte, majoritatea infracțiunilor informatice își au baza în vulnerabilitățile sistemelor informatice.

Majoritatea infracțiunilor săvârșite în domeniul informatic se realizează prin intermediul unei rețele unde există diferite conexiuni între diferite sisteme de calcul. Marea greșeală în interpretarea sistemelor de rețele este aceea că este confundată cu rețeaua Internet, însă o rețea de calculatoare poate exista independent, fără a fi conectată la Internet, fapt ce conferă situației de fapt, în ceea ce privește o eventuală cercetare criminalistică o diferită perspectivă.

Când se face referire la rețeaua globală Internet ne referim la totalitatea computerelor interconectate cu diferite sisteme de calcul la nivel mondial, iar când ne referim la o rețea de calculatoare de sine stătătoare ne referim la intranet. Toate computerele și sistemele computerizate interconectate din rețeaua Internet respectă anumite reguli conform protocoalelor de comunicare TCP (Transmission Control Protocol) și IP (Internet Protocol) și sunt întâlnite în sistemele informatice în formula TCP/IP.

Spațiul cibernetic nu trebuie confundat cu Internetul real (ca rețea), ci trebuie privit ca însumând aspectele psihologice și sociale pe care i le conferă, prin utilizare, psihicul

uman individual și societatea în ansamblu. Acesta cuprinde, prin urmare, identitățile și obiectele care există în rețele de calculatoare folosite de indivizii umani în diverse scopuri¹.

Deși majoritatea sistemelor de rețele intranet sunt la rândul lor conectate prin intermediul marii rețele Internet există și situația când rețele de tipul prim menționat nu sunt conectate celei de a doua.

După cum a fost menționat, din punct de vedere al cercetării criminalistice, relevanța criminalistică reiese din cercetarea propriu-zisă a perimetrului infracțional. Din punct de vedere criminalistic interesează această problemă deoarece în cazul în care suntem în prezența unei infracțiuni săvârșite prin intermediul rețelei Internet, calculatorul folosit pentru săvârșirea infracțiunii, indiferent de tipul infracțiunii informatice, se poate afla într-un stat, iar calculatorul victimă sau sistemul informatic prejudiciat într-un altul.

În cazul unei rețele informatice de tip intranet perimetrul infracțional este de obicei limitat, fapt ce conferă un timp de cercetare mai scurt, fiind prezentă o cercetare criminalistică optimă, unde probele digitale sau în legătură cu infracțiunea de tip informatic ajung a fi transpuse în diferite acte de cercetare judiciară pentru a servi justiției cu celeritate.

Terminologia cuvântului Internet provine din alăturarea parțială a două cuvinte ce provin din limba engleză, și anume, interconnected care înseamnă interconectat și network care are înțelesul de rețea, din care rezultă cuvântul tot de proveniență engleză Internet(Inter-net). Internetul reprezintă o rețea mondială omogenă de interconexiuni între diferite sisteme informatice mai mult sau mai puțin complexe.

1. DIMENSIUNEA CRIMINALITĂȚII INFORMATICE

1.1. Conceptul de criminalitate informatică. Definiția și noțiunea de criminalitate informatică

Datele statistice arată că nivelul conectivității la rețeaua globală Internet a crescut dramatic, pe cale de consecință este previzibilă schimbarea fenomenologică asupra criminalității informatice, în sensul că atât timp cât numărul de sisteme informatice conectate la rețeaua Internet va crește și criminalitatea informatică va crește și va avea un trend ascendent direct proporțional cu numărul conexiunilor, indiferent de natura acestora.

În anul 2011 cel puțin 2,3 miliarde de oameni, echivalentul a mai mult decât o treime din populația totală a planetei, aveau acces la serviciile de Internet. Țările dezvoltate din punct de vedere economic prezintă o rată de acces la aceste servicii într-un procent de 70% față de țările în curs de dezvoltare unde procentul este de 24%. Deși accesul la internet este în procent mai mare în țările dezvoltate, interesant este că numărul de utilizatori ai Internetului în țările în curs dezvoltare este în procent 62%. În ambele cazuri, persoane din ce în ce mai tinere folosesc mediul de conectivitate globală comparativ cu persoanele în vârstă. Astfel, un procent de 45% din utilizatorii de Internet

¹ D. Dumbravă, *Agresiunile în spațiul cibernetic*, Revista Română de Studii de Inteligență nr. 6/2011, p. 166.

au vârsta sub 25 de ani, segment demografic care corespunde în linii mari cu grupul de persoane care prezintă, de cele mai multe ori, un potențial grup cu caracter criminogen. Actual, în ceea ce privește conectivitatea prin Internet mobil în bandă largă există aproximativ 1,2 miliarde de abonamente, acest număr fiind de două ori mai mare decât posesorii de abonamente în bandă largă fixă. Acest procent menționat corespunde cu aproximativ 16% din populația globală.

Principalele efecte ale impactului erei informaționale asupra mediului social, dar și asupra altor medii cu caracter special în societate se apreciază a fi următoarele: timpul și distanța devin tot mai puțin importante în spectrul constrângerilor, evenimentele pot fi influențate de o serie de factori transnaționali, granițele de orice natură devin tot mai nesemnificative, tendințele de regionalizare și globalizare vor avea un curs ascendent, iar inegalitatea dintre bogați și săraci se va adânci¹. Tehnologia informațiilor produce schimbări continue în organizarea și structura tuturor componentelor societății, fluxurile informaționale neavând constrângeri de distanță sau ordin ierarhic².

Având în vedere aceste considerente de ordin social și statistic, de maximă importanță în ceea ce privește investigarea fenomenului criminal-informatic, atât din punct de vedere criminologic, cât și criminalistic, putem afirma că înțelegerea fenomenului este imperativ-necesară și de necontestat în contextul unei lumi moderne în continuă schimbare.

Astfel, termenul de criminalitate informatică, deși aparent acceptat și aparent înțeles prin promovarea acestuia prin diferite mijloace de informare, poate fi privit prin prisma mai multor puncte de vedere. Lipsa clarității în ceea ce privește definirea termenilor creează probleme aproape în toate domeniile de investigare ale fenomenului având impact negativ în ceea ce privește prevenirea acestuia, cât și remedierea incidentelor cu caracter criminal din domeniul informatic³. La fel ca și crimele⁴ clasice, infracțiunile informatice îmbracă diferite forme care se produc într-o mare varietate și pot fi întâlnite într-o multitudine de medii sociale.

În literatura de specialitate, atât națională, cât și internațională, se admite faptul că nu există o definiție unanim acceptată a criminalității informatice. Nucleul conceptului de criminalitate informatică, în concepția prezentă a fenomenului, se referă la faptul că tehnologia informației și comunicațiilor sunt convergente la nivel global și pot fi folosite pentru comiterea unor infracțiuni cu caracter transnațional.

Comiterea unei fapte interzise cu caracter informatic nu implică prezența neapărat fizică a făptuitorului în locul unde este situată victima. Un număr important de infracțiuni cibernetice, având în vedere cele exprimate anterior, afectează din punct de vedere al locului comiterii, mai multe țări în același timp⁵.

¹ După – Col. Drd. D. Neacșu, Buletinul Național al Universității Naționale de Apărare Carol I nr. 3, anul 2012, *Riscuri, amenințări și vulnerabilități de natură informațională asupra domeniului militar. Tendințe și orientări ale politicilor de apărare în era informațiilor*, Central and Eastern European Online Library, p. 8.

² *Ibidem*, op. cit., p. 9.

³ După – S. Gordon, R. Ford, *On the definition and classification of cybercrime*, Journal in Computer Virology, Ed. Springer, 2006, p. 13.

⁴ N.R. - Crima privită în sens larg.

⁵ Handbook of Identity - related Crime; UNODC - United Nations Office on Drugs and Crime, aprilie 2011 Biroul Națiunilor Unite Viena, p. 22.

Amplasând atenția numai asupra sistemelor informatice conectate la Internet în timp real este o eroare de măsurare a fenomenului deoarece infracțiuni informatice pot fi comise și de pe un computer care este închis în timpul unei măsurători a fenomenului sau de un sistem informatic privit ca entitate individuală neconectată rețelei¹.

Definițiile criminalității informatice au evoluat și au fost construite în principal prin experiența specialiștilor cumulată în timp. Astfel, acestea se deosebesc în funcție de percepția atât a observatorilor, cât și a aceloră în sarcina cărora revine protecția victimelor, iar parțial aceste considerente legate de percepție sunt o funcție a faptelor incriminate, care au legătură cu mediul cibernetic sau sunt săvârșite în acesta, ce prezintă o evoluție geografică². Termenul de criminalitate informatică reprezintă totalitatea faptelor comise în zona noilor tehnologii, într-o anumită perioadă de timp și pe un anumit teritoriu bine determinat³.

Sintagma „criminalitate informatică” reunește numeroase tipuri de activități, dar se referă în principal la infracțiunile comise și/sau facilitate cu ajutorul mediilor electronice.

Prin comparație cu criminalitatea obișnuită, criminalitatea informatică necesită mai puține resurse raportat la pagubele susceptibile de a fi produse; infracțiunile informatice pot fi săvârșite într-un stat fără ca făptuitorul să fie prezent în mod fizic și, în numeroase țări, aceste infracțiuni sunt definite într-un mod inadecvat sau nu sunt deloc definite, astfel încât autorii lor se expun unui risc minor, iar probabilitatea ca ei să fie descoperiți este mică⁴.

Majoritatea ghidurilor, publicațiilor și rapoartelor de specialitate din domeniul criminal-informatic încep prin definirea criminalității informatice. Una dintre cele mai comune definiții ale criminalității informatice descrie acest fenomen ca fiind activitatea care implică folosirea computerelor sau rețelelor de comunicații ca fiind instrumentul, ținta sau locul unde are loc activitatea infracțională⁵.

În opinia anumitor autori⁶, Convenția Europeană asupra criminalității informatice folosește termenul de criminalitate informatică referindu-se la gama de acțiuni infracționale care aduc atingere mediilor de stocare a datelor sau încalcă drepturile de proprietate intelectuală. Având în vedere cele menționate anterior, alți autori din literatura de specialitate sunt de părere că definiția este mult mai extinsă, aceasta referindu-se și la activități, precum: fraudele informatice, accesul neautorizat într-un sistem informatic, pornografie infantilă, urmărirea și hărțuirea anumitor persoane prin intermediul mediului virtual (cyberstalking⁷).

¹ Comprehensive Study on Cybercrime – Februarie 2013, aut. cit., UNODC – United Nations Office on Drugs and Crime; United Nations; New, York 2013, p. 122.

² S. Gordon, R. Ford, *op. cit.*, p. 13-14.

³ T. Amza, C.-P. Amza, *Criminalitatea informatică*, Ed. Lumina Lex, București, 2003, p. 13.

⁴ L. Giurea, O. Vară, *Conexiunea dintre traficul de droguri și noile tehnologii*, Revista de investigare a criminalității nr. 5/2010, editată de Ed. Universul Juridic, p. 106.

⁵ Dr. M. Gercke, *Understanding cybercrime – A Guide For developing countries*, ITU – International Telecommunication Union (ITU), ICT Applications and Cybersecurity Division - Policies and Strategies Departament – Bureau for Telecommunications Union, Place des Nations, 1211 Geneva 20, Elveția, p. 17.

⁶ N.R.- S. Gordon, R. Ford, *op. cit.*, p. 14.

⁷ Acest termen se referă la folosirea internetului sau a altor mijloace tehnice electronice folosite pentru a urmări și hărțui persoane sau grupuri de persoane și poate include acuzații false, monitorizare, amenințări - intimidări, furt de identitate, avariere de echipamente, solicitarea de a întreține acte sexuale cu minori.

Manualul Națiunilor Unite¹ privind prevenirea și controlul asupra infracțiunilor în legătură cu computerul include, în afară de fraudă și acces neautorizat, și termenul de fals în definiția criminalității informatice.

Cea mai simplă definiție pe care o poate îmbrăca criminalitatea informatică este: Actul infracțional să fie îndreptat către un computer sau către o rețea de computere ori sisteme cu caracter informatic. O altă definiție a criminalității informatice se referă la orice crimă care este facilitată sau comisă prin utilizarea unui computer, rețele sau dispozitiv informatic.

Deși este o definiție generică, aceasta înglobează în mare parte caracterele infracțiunilor din domeniul informatic. În opinia celor mai mulți specialiști din domeniul tehnologiei informației și domeniul juridic se acceptă tacit ideea că definițiile pentru criminalitatea informatică derivă din norme juridice.

La nivel internațional au fost folosiți pentru prima dată termenii criminalitate informatică (computer crime) și criminalitate în legătură cu utilizarea calculatorului (computer-related crime) în legislația Statelor Unite ale Americii (U.S. Computer Fraud and Abuse Act), cât și în legislația Regatului Unit al Marii Britanii (U.K. Computer Abuse Act). 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 și alterarea sau furtul de informații stocate electronic; stoarcerea de bani comisă cu ajutorul computerului, accesul neautorizat în rețelele bancare, traficul cu parole furate și transmiterea de viruși distructivi sau comenzi².

Experții Organizației pentru Cooperare Economică și Dezvoltare (OECD³) defineau în 1983 faptele de natură penală ca fiind orice comportament ilegal, neetic sau neautorizat ce privește un tratament automat al datelor și/sau o transmitere de date.

Deși această definiție a fost formulată acum trei decenii și-a dovedit utilitatea prin faptul că a permis și permite în continuare integrarea ulterioară a dezvoltărilor tehnologice din domeniul informatic.

Institutul Națiunilor Unite din Asia și Extremul Orient pentru prevenirea crimei și tratamentul delincvenților (UNAFEI) prin infracțiune informatică nuanțează două definiții, și anume:

a) În sens larg, prin infracțiune informatică 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.

b) În sens restrâns, prin infracțiune informatică se înțelege orice infracțiune în care făptuitorul interferează, fără autorizare, cu procesele de prelucrare automată a datelor⁴.

¹ În literatura de specialitate se mai întâlnește în formula Manualul Națiunilor Unite pentru prevenirea și controlul infracționalității informatice.

² A.C. Moise, *Metodologia investigării criminalistice a infracțiunilor informatice*, Ed. Universul Juridic, București, 2011, p. 16.

³ În engleză Organisation for Economic Cooperation and Development; în franceză Organisation de Coopération et de Développement Économiques; Această organizație a condus un grup de studiu asupra criminalității cibernetice între anii 1983-1985, iar în anul 1986 a publicat o serie de fapte informatice ce trebuiau incriminate ca fiind fapte penale.

⁴ Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică, USAID, Internnews Network, RITI dot-GOV, p. 51.

1.2. Clasificări ale criminalității informatice

Computerul sau dispozitivul informatic poate fi în ecuația infracțională atât dispozitivul pe care se realizează infracțiunea, cel care facilitează săvârșirea unei infracțiuni, cât și victima unei infracțiuni. Infracțiunea informatică poate avea loc într-un singur computer, privit ca o entitate singulară, dar poate fi continuată și în alte locații. Criminalitatea informatică poate fi mai bine înțeleasă divizând-o în două categorii, după cum urmează:

1. Criminalitate informatică de Tipul I care are următoarele caracteristici:

a) Este în general reprezentată de un eveniment izolat când este privită din perspectiva victimei unei infracțiuni informatice. De exemplu, victima fără să știe descarcă de pe Internet un Cal Troian (Trojan Horse) care instalează pe dispozitivul acesteia un keystroke logger¹. Alternativ victima atacului primește un e-mail care conține un link care provine de la o entitate cunoscută, dar în realitate este o amenințare web.

b) Este de obicei facilitată de programe crimeware², precum keystroke loggers, viruși, rootkits³, Trojan Horse.

c) Defectele software și vulnerabilitățile sistemelor informatice oferă de cele mai multe ori sprijin infractorului informatic în rezoluția infracțională. De exemplu, criminalii care controlează un anumit site web pot profita de vulnerabilitățile care se regăsesc în browser-ul web pentru a plasa o amenințare informatică de tip Trojan Horse.

2. Criminalitate informatică de tipul II include în afară de cyberstalking și hărțuire, pornografie infantilă, deturnare de fonduri, manipularea piețelor de capital, șantaj, spionaj corporativ și spionaj industrial, plănuirea de atacuri teroriste. Acest tip de criminalitate are următoarele caracteristici:

a) Este în general un lanț causal la unei serii de evenimente care implică interacțiuni repetate cu ținta atacului. De exemplu, victima este dintr-un mediu de relaționare virtuală de genul chat room, iar în timp se încearcă obținerea unei relații apropiate cu acesta de către atacator. În cazul în care relaționarea virtuală va reuși, atacatorul va profita și va comite infracțiunea.

b) În general este facilitată de programe care nu cad sub incidența genului de programe crimeware. De exemplu, conversațiile se pot realiza prin utilizarea unui program

¹ Keystroke logging-ul se referă la acțiunea de înregistrare a tastelor în momentul acționării acestora, de obicei realizată într-o manieră ascunsă, astfel încât, persoana care utilizează tastatura respectivă să nu știe că este monitorizată. Există numeroase modalități de keystroke logging plecând de la abordări atât hardware și software, până la analiză acustică.

² Crimeware – este un tip de malware proiectat pentru a comite automat o infracțiune informatică. Malware-ul este un program informatic creat cu rea-intenție pentru afectarea fizică a unui computer sau accesul ascuns la fișierele acestuia. Crimeware-ul este folosit de infractori pentru furtul de identitate în scopul de a avea acces la diferite conturi online sau pentru a uza de aceste conturi în scopul tranzacțiilor frauduloase în scopul dobândirii de bani sau bunuri patrimoniale.

³ Rootkit – este un program de calculator ascuns construit de așa manieră încât să nu poată fi detectat prin metodele normale pe care le folosește un program de detecție (genul antivirus sau softuri care vin odată cu sistemul de operare) în scopul de a obține accesul privilegiat la un anumit computer.