Marin RUIU

METODOLOGIA INVESTIGĂRII CRIMINALISTICE A UNOR GENURI DE INFRACȚIUNI

Marin RUIU

METODOLOGIA INVESTIGĂRII CRIMINALISTICE A UNOR GENURI DE INFRACȚIUNI

Universul Juridic
București
-2014-

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

Descrierea CIP a Bibliotecii Naționale a României
RUIU, MARIN
Metodologia investigării criminalistice a unor genuri de infracțiuni / Marin Ruiu. - Bucureşti : 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 păşeau 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.

Uşurința 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 specialişti în domeniul prevenirii infracționalității 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 săvârşite în domeniul informatic se realizează prin intermediul unei rețele unde există diferite conexiuni între diferite sisteme de calcul. Marea greşeală 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 priveşte 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 şi societatea în ansamblu. Acesta cuprinde, prin urmare, identităţile şi obiectele care există în reţele de computere folosite de indivizii umani în diverse scopuri[1].

Deşi majoritatea sistemelor de reţele intranet sunt la rândul lor conectate prin intermediul marii reţele Internet există şi situaţia când reţele de tipul prim menţionat nu sunt conectate celei de a doua.

După cum a fost menţionat, din punct de vedere al cercetării criminalistice, relevanţa criminalistică reiese din cercetarea propriu-zisă a perimetrului infracţional. Din punct de vedere criminalistic interesează această problemă deoarece în cazul în care suntem în prezenţa unei infracţiuni săvârşite prin intermediul reţelei Internet, computerul folosit pentru săvârşirea infracţiunii, indiferent de tipul infracţiunii informatice, se poate afla într-un stat, iar computerul victimă sau sistemul informatic prejudiciat într-un altul.

În cazul unei reţele informatice de tip intranet perimetrul infracţional 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 infracţiunea de tip informatic ajung a fi transpuse în diferite acte de cercetare judiciară pentru a servi justiţiei cu celeritate.

Terminologia cuvântului Internet provine din alăturarea parţială a două cuvinte ce provin din limba engleză, şi anume, interconnected care înseamnă interconectat şi network care are înţelesul de reţea, din care rezultă cuvântul tot de provenienţă engleză Internet(Inter-net). Internetul reprezintă o reţea mondială omogenă de interconexiuni între diferite sisteme informatice mai mult sau mai puţin complexe.

1. DIMENSIUNEA CRIMINALITĂŢII INFORMATICE

1.1. Conceptul de criminalitate informatică. Definiţia şi noţiunea de criminalitate informatică

Datele statistice arată că nivelul conectivităţii la reţeaua globală Internet a crescut dramatic, pe cale de consecinţă este previzibilă schimbarea fenomenologică asupra criminalităţii informatice, în sensul că atât timp cât numărul de sisteme informatice conectate la reţeaua Internet va creşte şi criminalitatea informatică va creşte şi va avea un trend ascendent direct proporţional cu numărul conexiunilor, indiferent de natura acestora.

În anul 2011 cel puţin 2,3 miliarde de oameni, echivalentul a mai mult decât o treime din populaţia totală a planetei, aveau acces la serviciile de Internet. Ţările dezvoltate din punct de vedere economic prezintă o rată de acces la aceste servicii într-un procent de 70% faţă de ţările în curs de dezvoltare unde procentul este de 24%. Deşi accesul la internet este în procent mai mare în ţările dezvoltate, interesant este că numărul de numărul de utilizatori ai Internetului în ţările 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 spaţiul cibernetic*, Revista Română de Studii de Inteligence 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 priveşte 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 şi asupra altor medii cu caracter special în societate se apreciază a fi următoarele: timpul şi 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 şi globalizare vor avea un curs ascendent, iar inegalitatea dintre bogați şi săraci se va adânci[1]. Tehnologia informațiilor produce schimbări continue în organizarea şi structura tuturor componentelor societății, fluxurile informaționale neavând constrângeri de distanță sau ordin ierarhic[2].

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

Astfel, termenul de criminalitate informatică, deşi aparent acceptat şi 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 priveşte definirea termenilor creează probleme aproape în toate domeniile de investigare ale fenomenului având impact negativ în ceea ce priveşte prevenirea acestuia, cât şi remedierea incidentelor cu caracter criminal din domeniul informatic[3]. La fel ca şi crimele[4] clasice, infracțiunile informatice îmbracă diferite forme care se produc într-o mare varietate şi pot fi întalnite într-o multitudine de medii sociale.

În literatura de specialitate, atât națională, cât şi 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 şi comunicațiilor sunt convergente la nivel global şi pot fi folosite pentru comiterea unor infracțiuni cu caracter transnațional.

Comiterea unuei 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 acelaşi timp[5].

---

[1] După – Col. Drd. D. Neacşu, Buletinul Național al Universității Naționale de Apărare Carol I nr. 3, anul 2012, *Riscuri, amenințări şi vulnerabilități de natură informațională asupra domeniului militar. Tendințe şi 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 şi de pe un computer care este închis în timpul unei măsurători a fenomenului sau de un sistem informatic privit ca entitate individuală neconectată rețelei[1].

Definițiile criminalității informatice au evoluat şi au fost construite în principal prin experiența specialiştilor cumulată în timp. Astfel, acestea se deosebesc în funcție de percepția atât a observatorilor, cât şi a acelora 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 săvârşite în acesta, ce prezintă o evoluție geografică[2]. Termenul de criminalitate informatică reprezintă totalitatea faptelor comise în zona noilor tehnologii, într-o anumită perioadă de timp şi pe un anumit teritoriu bine determinat[3].

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

Prin comparație cu criminalitatea obişnuită, criminalitatea informatică necesită mai puține resurse raportat la pagubele susceptibile de a fi produse; infracțiunile informatice pot fi săvârşite într-un stat fără ca făptuitorul să fie prezent în mod fizic şi, 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 mică[4].

Majoritatea ghidurilor, publicațiilor şi 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 infracțională[5].

În opinia anumitor autori[6], Convenția Europeană asupra criminalității informatice foloseşte 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 definția este mult mai extinsă, aceasta referindu-se şi la activități, precum: fraudele informatice, accesul neautorizat într-un sistem informatic, pornografie infantilă, urmărirea şi hărțuirea anumitor persoane prin intermediul mediului virtual (cyberstalking[7]).

---

[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, Bucureşti, 2003, p. 13.

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

[5] Dr. M. Gercke, *Undestanding cybercrime – A Guide For developing countries*, ITU – International Telecomunication Union (ITU), ICT Applications and Cybersecurity Division - Policies and Strategics Departament – Bureau for Telecomunications 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 şi hărțui persoane sau grupuri de persoane şi poate include acuzații false, monitorizare, amenințări - intimidări, furt de identitate, avariere de echipamente, solicitarea de a întreține acte sexuale cu minori.

Manualul Națiunilor Unite[1] privind prevenirea şi controlul asupra infracțiunilor în legătură cu computerul include, în afară de fraudă şi acces neautorizat, şi 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.

Deşi este o definiție generică, aceasta înglobează în mare parte caracterele infracțiunilor din domeniul informatic. În opinia celor mai mulți specialişti din domeniul tehnologiei informației şi 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) 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). 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[2].

Experții Organizației pentru Cooperare Economică şi Dezvoltare (OECD[3]) defineau în 1983 faptele de natură penală ca fiind orice comportament ilegal, neetic sau neautorizat ce priveşte un tratament automat al datelor şi/sau o transmitere de date.

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

Institutul Națiunilor Unite din Asia şi Extremul Orient pentru prevenirea crimei şi tratamentul delincvenților (UNAFEI) prin infracțiune informatică nuanțează două definiții, şi 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 datelor[4].

---

[1] În literatura de specialitate se mai întâlneşte în formula Manualul Națiunilor Unite pentru prevenirea şi controlul infracționalității informatice.

[2] A.C. Moise, *Metrodologia investingării criminalistice a infracțiunilor informatice*, Ed. Universul Juridic, Bucureşti, 2011, p. 16.

[3] În engleză Organisation for Economic Cooperation and Developement; în franceză Organisation de Coopération et de Développment 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 criminalităţii informatice

Computerul sau dispozitivul informatic poate fi în ecuaţia infracţională atât dispozitivul pe care se realizează infracţiunea, cel care facilitează săvârşirea unei infracţiuni, cât şi victima unei infracţiuni. Infracţiunea informatică poate avea loc într-un singur computer, privit ca o entitate singulară, dar poate fi continuată şi în alte locaţii. Criminalitatea informatică poate fi mai bine înţeleasă 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 infracţiuni informatice. De exemplu, victima fără să ştie descarcă de pe Internet un Cal Troian (Trojan Horse) care instalează pe dispozitivul acesteia un keystroke logger[1]. Alternativ victima atacului primeşte un e-mail care conţine un link care provine de la o entitate cunoscută, dar în realitate este o ameninţare web.

b) Este de obicei facilitată de programe crimeware[2], precum keystroke loggers, viruşi, rootkits[3], Trojan Horse.

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

2. Criminalitate informatică de tipul II include în afară de cyberstalking şi hărţuire, pornografie infantilă, deturnare de fonduri, manipularea pieţelor de capital, şantaj, spionaj corporativ şi spionaj industrial, plănuirea de atacuri teroriste. Acest tip de criminalitate are următoarele caracterisitici:

a) Este în general un lanţ cauzal la unei serii de evenimente care implică interacţiuni repetate cu ţinta atacului. De exemplu, victima este dintr-un mediu de relaţionare virtuală de genul chat room, iar în timp se încearcă obţinerea unei relaţii apropiate cu acesta de către atacator. În cazul în care relaţionarea virtuală va reuşi, atacatorul va profita şi va comite infracţiunea.

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

[1] Keystroke logging-ul se referă la acţiunea de înregistrare a tastelor în momentul acţionării acestora, de obicei realizată într-o manieră ascunsă, astfel încât, persoana care utilizează tastatura respectivă să nu ştie că este monitorizată. Există numeroase modalităţi de keystroke logging plecând de la abordări atât harware şi software, până la analiză acustică.

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

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