

Lect. univ. dr. Gheorghe-Iulian IONIȚĂ

*INFRAȚIUNILE DIN SFERA CRIMINALITĂȚII
INFORMATICE*

INCRIMINARE, INVESTIGARE, PREVENIRE ȘI COMBATERE
ediția a II-a, revăzută și adăugită

Lect. univ. dr. GHEORGHE-IULIAN IONIȚĂ

**INFRAȚIUNILE DIN SFERA
CRIMINALITĂȚII
INFORMATICE**

**INCRIMINARE, INVESTIGARE,
PREVENIRE ȘI COMBATERE**

ediția a II-a, revăzută și adăugită



Copyright © 2013, **Editura Pro Universitaria**

Toate drepturile asupra prezentei ediții aparțin
Editurii Pro Universitaria

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

Descrierea CIP a Bibliotecii Naționale a României

IONIȚĂ, GHEORGHE IULIAN

**Infracțiunile din sfera criminalității informatice :
incriminare, investigare, prevenire și combatere /**

Ioniță Gheorghe-Iulian. - Ed. a 2-a, rev. și adăug. -

București : Pro Universitaria, 2013

Bibliogr.

ISBN 978-606-647-909-7

343.23:004(075.8)

Mulțumiri

Prezenta are ca bază **teza de doctorat „Criminalitatea informatică”** susținută la Academia de Poliție „Alexandru Ioan Cuza” din București (iulie, 2009).

Consider că **se cuvine**, înainte de toate, *să-mi exprim recunoștința* față de cei, fără de care, realizarea atât a tezei de doctorat, cât și a prezentei lucrări, nu era posibilă.

În primul rând, față de domnul profesor gl. lt. (r) **ION SUCEAVĂ**, conducătorul de doctorat, sub a cărui îndrumare mi-am desfășurat cercetarea doctorală timp de șapte ani (perioada 2002-2009) și am structurat teza, și căruia îi mulțumesc nu numai pentru suportul științific, ci și pentru înțelepciunea și înțelegerea cu care mi-a tolerat multe pe parcursul acestor ani.

O contribuție majoră, și nu numai la elaborarea tezei de doctorat, ci și la formarea mea ca persoană și specialist, a avut-o domnul profesor **FLORIN SANDU**.

Trebuie amintit suportul științific și moral acordat în perioada de pregătire doctorală, în special, de domnii profesori **COMAN FLORIN, ALEXANDRU BOROI, ȘTEFAN COCOȘ**, doamna profesor **GEORGETA UNGUREANU**, dar și de **alte cadre didactice** din cadrul Academiei de Poliție „Alexandru Ioan Cuza” și Universității Româno-Americane București.

În aceeași ordine de idei, trebuie subliniat ajutorul acordat, pentru lămurirea unor aspecte tehnice, și nu numai, de către doi specialiști criminaliști în domeniul investigării sistemelor informatice din cadrul Institutului de Criminalistică, **IANCU ANEL** și **CONSTANTIN ALEXANDRA**.

De asemenea, sunt onorat și recunoscător pentru sprijinul real, necondiționat, al domnilor profesori **VASILE LĂPĂDUȘI, GEORGE ANTONIU** și **OVIDIU PREDESCU**.

Nu în ultimul rând, cele mai profunde mulțumiri le adresez familiei, **soției, IONIȚĂ-BURDA ȘTEFANIA-DIANA, și copiilor, IONIȚĂ ANDREI-IULIAN și IONIȚĂ MARIA-IULIA**, pe care i-am privat de atenția meritată și care au suportat toate.

Abrevieri

cap.	capitol
par.	paragraf
alin.	alineat
nr.	număr
lit.	literă
Ed.	editură
ed.	ediție
v.	versiune
DL	Decret Lege
OG	Ordonanță a Guvernului
OUG	Ordonanță de Urgență a Guvernului
HG	Hotărâre a Guvernului
C. pen.	Cod penal
C. pr. pen.	Cod de procedură penală
C. pen. fed.	Cod penal federal
UN	Organizația Națiunilor Unite
US	Statele Unite ale Americii
CoE	Consiliul Europei
EU	Uniunea Europeană
US DoJ	Ministerul de Justiție al Statelor Unite ale Americii
MAI	Ministerul Administrației și Internelor
US SS	Serviciul Secret al Statelor Unite ale Americii
US FBI	Biroul Federal de Investigații al Statelor Unite ale Americii
DIICOT	Direcția de Investigare a Infrafracțiunilor de Criminalitate Organizată și Terorism
DCCO	Direcția de Combatere a Criminalității Organizate

Considerații introductive

În prezent, activitatea ilegală nu se produce numai în spațiul material ci și în cel digital.

Societatea (în general, nu numai specialiștii) și-a pus întrebarea (și și-o pune în continuare) dacă această dependență de sistemele informatice și rețelele de comunicații (Internet-ul, în special), în contextul problemelor pe care utilizarea acestora le generează, necesită o reanalizare față de percepția actuală.

„Informatizarea” vieții sociale și „tehnologizarea” infractorilor au constituit premisele apariției (sau grefarea elementelor „clasice” de criminalitate) unei noi forme de manifestare a criminalității (în general), ***criminalitatea informatică***¹.

Această conduită incriminată penal, dezvoltată prin intermediul sau în legătură cu utilizarea sistemelor informatice și/sau a rețelelor de comunicații este una dintre cele mai serioase probleme.

Criminalitatea informatică, ca fenomen, ne conduce spre o adevărată problemă, aceea a *modului de utilizare a noilor tehnologii*.

Este de necontestat faptul că apariția și dezvoltarea sistemelor informatice și rețelelor de comunicații a reprezentat o adevărată revoluție în societate, care a avut ca principală consecință tranziția de la Societatea Industrială la Societatea Informațională.

Astfel, calculatorul a devenit o componentă vitală a activității noastre cotidiene iar dezvoltarea tehnologiei comunicațiilor (Internet-ul, în special) a produs transformări în întreaga societate.

Infrațiunile din sfera criminalității informatice constituie o adevărată tentație pentru grupările criminale întrucât sistemele informatice și rețelele de comunicații facilitează nu numai comiterea

¹ Sandu F., Ioniță G.I., *Criminologie teoretică și aplicată*, Ed. Universul Juridic, București, 2005, p. 265.

infracțiunilor (de orice tip) dar ușurează și reciclarea „produselor” respectivelor infracțiuni¹.

În prezent, asistăm nu doar la o explozie, diversificare și specializare a criminalității, ci și la o congruență între infracțiunile din sfera criminalității informatice și infracțiunile „tradiționale”.

Acest fenomen este generat de faptul că sistemele informatice nu sunt doar ținta infracțiunilor ci și instrumentul prin care sunt comise alte infracțiuni sau, pur și simplu, acestea facilitează, prin funcțiile lor, comiterea mai „ușoară” sau mai „sigură” a infracțiunilor „tradiționale” (de drept comun, care puteau și pot fi comise și fără intervenția sistemelor informatice).

În acest context, multe dintre investigațiile unor infracțiuni „tradiționale” (indiferent de natura acestora) vor include sistemele informatice ce pot conține date despre motivația, identitatea, locația, conexiunile făptuitorilor/complicilor etc., și care pot ușura finalizarea respectivelor investigații.

Se consideră (și pe bună dreptate) că multe dintre reglementările și procedurile legale „tradiționale” nu mai corespund, în timp ce multe dintre reglementările și procedurile nou introduse ridică multe probleme, date fiind diferențele dintre mediul real și mediul digital.

Problematica cercetării/investigării infracțiunilor din sfera criminalității informatice, procedurile care trebuie urmate, activitățile care trebuie desfășurate, pașii care trebuie parcurși, este încă în faza dezbaterilor.

Este firesc, dat fiind caracteristicile acestei forme de manifestare a criminalității, dar și caracterului relativ recent, să mai dureze până când aceste activități să se cristalizeze și să fie general acceptate.

În aceste condiții, se desprinde motivația demersului științific realizat, aceea de a prezenta problemele pe care le generează dependența de sistemele informatice și rețelele de comunicații, factorii care au generat dezvoltarea (fără precedent a) fenomenului, provocările cu care se confruntă organele de aplicare a legii și mijloacele (juridice și tehnice, în special) pe care le au la dispoziție în încercarea de a preveni și combate criminalitatea informatică.

¹ *Idem.*

Partea I

**ASPECTE GENERALE PRIVIND
SECURITATEA SISTEMELOR
INFORMATICE
ȘI CRIMINALITATEA INFORMATICĂ**

CAPITOLUL I

Amenințări actuale și tendințe viitoare în ce privește securitatea sistemelor informaticice și rețelelor de comunicații

Secțiunea I

Considerații generale

Încă de la apariția sistemelor informatice și rețelelor de comunicații au fost căutate vulnerabilităților acestora, fie în scopul îmbunătățirii performanțelor și siguranței în exploatare fie în scopul compromiterii lor.

Vulnerabilitățile sistemelor informatice și rețelelor de comunicații sunt acele caracteristici/puncte slabe care creează condițiile apariției amenințărilor.

Atacul asupra sistemelor informatice și rețelelor de comunicații presupune identificarea și exploatarea vulnerabilităților, cu alte cuvinte, punerea în practică a acestor amenințări.

Incidentele privind securitatea sistemelor informatice și rețelelor de comunicații presupun încălcarea (sau amenințarea iminentă cu încălcarea) politicilor de securitate, politicilor privind folosirea acceptabilă sau a practicilor standard de securitate a acestora.

Secțiunea a II-a

Principalele taxonomii dezvoltate în sfera securității sistemelor informatice și rețelelor de comunicații

Taxonomia, conform definiției¹, este mai mult decât o clasificare, în sensul că aceasta descrie principiile conform cărora clasificarea a fost făcută dar și procedura care trebuie urmată pentru clasificarea unui obiect nou².

În sfera securității sistemelor informatice și a rețelelor de comunicații, taxonomiile au apărut din nevoia de a oferi consecvență și coerență în limbajul utilizat pentru descrierea și clasificarea vulnerabilităților și atacurilor asupra acestora și a se evita astfel (pe cât posibil) confuziile.

De asemenea, aceste taxonomii permit aplicarea cunoștințelor anterioare amenințărilor noi, cât și un mod organizat de percepere a acestora (amenințărilor).

O **taxonomie satisfăcătoare** prezintă următoarele **caracteristici**³:
- **acceptată** (Howard, 1997)/**adevătată** (Amoroso, 1994), în sensul de a fi structurată de o asemenea manieră astfel încât să fie aprobată în general;

¹ Taxonomia este considerată „știința legilor de clasificare” (a se vedea Academia Română Institutul de lingvistică, Iorgu Iordan, *Dicționar explicativ al limbii române*, ed. a II-a, Ed. Univers Enciclopedic, București, 1998, p. 1072) sau „știința care se ocupă cu stabilirea legilor de clasificare și sistematizare a domeniilor din realitate cu o structură complexă” (a se vedea DEX online, la <http://dexonline.ro/search.php?Cuv=taxonomie>).

² A se vedea și Berghe C. V., Riordan J. Piessens F., *A Vulnerability Taxonomy Methodology applied to web Services*, L.P. 4, disponibilă la http://chris.vandenbergher.org/publications/vulnerability_taxonomy_nerdsec2005.pdf.

³ Lough D. L., *A Taxonomy of Computer Attack with Application to Wireless Networks*, teză de doctorat susținută la Virginia Polytechnic Institute and State University, Virginia, (apr.), 2001, p. 37-39, disponibilă și la <http://scholar.lib.vt.edu/theses/available/etd-04252001-234145/unrestricted/lough.dissertation.pdf>. Lough compilează proprietățile unei taxonomii din lucrările a cinci autori Amoroso E. G. (*Fundamentals of Computer Security Technology*, Prentice Hall, Englewood Cliffs, N.J., 1994), Bishop M. (*How Attackers Break Programs, and How to Write Programs More Securely*, 8th net, USENIX Security Symposium, aug., 1999), Howard J. D. (*An Analysis of Security Incident on the Internet*, 1989-1995, teză de doctorat susținută la Purdue University, apr., 1997), Krsul I. V. (*Software Vulnerability Analysis*, teză de doctorat susținută la Purdue University, mai, 1998) Lindqvist U. și Johnsson E., (*How to Systematically Classify Computer Security Intrusions*, IEEE Security and Privacy, 1997).