ROMÂNIA
MINISTERUL AFACERILOR INTERNE
Academia de Poliţie „*Alexandru Ioan Cuza*”

POLGAR (SLABU) IRINA

TEZĂ DE DOCTORAT
- REZUMAT -

DOMENIUL: *„Drept“*

Conducător de doctorat
Profesor universitar doctor
VLAD BARBU

- BUCUREŞTI, 2018 **–**

MINISTERUL AFACERILOR INTERNE
ACADEMIA DE POLIŢIE *„Alexandru Ioan Cuza”*
Nr……din…….

NECLASIFICAT
Exemplar nr……

POLGAR (SLABU) IRINA

TEZĂ DE DOCTORAT

TEMA: PREVENIREA ŞI COMBATEREA CRIMINALITĂŢII INFORMATICE ÎN DREPTUL NAŢIONAL ŞI DREPTUL COMPARAT

Conducător de doctorat
Profesor universitar doctor
VLAD BARBU

Teza elaborată în vederea obţinerii
titlului de DOCTOR în ***„Drept“***

- BUCUREŞTI, 2018 **–**

CUPRINS

5.1. Organizaţii internaţionale şi regionale

- Consiliul Europei
- Grupul G7
- Interpol
- Organizaţia Tratatului Atlanticului de Nord
- Centrul Sud-Est European de Aplicare a Legii
- Organizaţia pentru Cooperare şi Dezvoltare
- Grupul APEC
- Comunitatea Naţiunilor (Commonwealth)
- Liga Statelor Arabe
- Uniunea Africană
- Organizaţia Statelor Americane
- Organizaţia pentru Cooperare de la Shanghai

5.2. Structuri care funcţionează sub auspiciile Uniunii Europene

- Agenţia Uniunii Europene pentru Formare în Materie de Aplicare a Legii – CEPOL
- Agenţia Europeană pentru Poliţia de Frontieră şi Garda de Coastă - Frontex
- Unitatea de Cooperare Judiciară a Uniunii Europene – EUROJUST

5.3. Rolul şi activitatea Agenției Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii - Europol

Capitolul VI Măsuri de prevenire şi combatere a criminalităţii informatice în dreptul comparat

6.1. Elemente de drept comparat în legislaţia unor state membre ale Uniunii Europene

- Austria
- Belgia
- Bulgaria
- Franţa
- Germania

- Grecia
- Italia
- Letonia
- Lituania
- Marea Britanie
- Olanda

6.2. Elemente de drept comparat în legislaţia altor state

- Elveţia
- Republica Moldova
- Rusia
- Statele Unite ale Americii
- Mauritius
- Africa de Sud
- Nigeria
- Australia
- India
- Singapore
- Peru
- Canada

Capitolul VII Concluzii şi propuneri de lege ferenda privind perfecţionarea activităţii de prevenire şi combatere în plan intern şi internaţional a criminalităţii informatice

7.1. Concluzii

7.1.1. Concluzii privind fenomenul criminalităţii informatice la nivel naţional

7.1.2. Concluzii privind fenomenul criminalităţii informatice la nivel internaţional

7.2. Propuneri de lege ferenda

7.2.1. Propuneri de lege ferenda ce vizează reglementarea infracţiunilor informatice

ABREVIERI ŞI ACRONIME

AIEA – Agenţia Internaţională pentru Energie Atomică

ANV – Autoritatea Naţională a Vămilor

APEC – Organizaţia de Cooperare Economică Asia-Pacific (Asia – Pacific Economic Cooperation)

Art. – Articolul

ATM – Bancomat/Casier automat (Automated Teller Machine)

BIRD – Banca Internaţională pentru Reconstrucţie şi Dezvoltare

C.A. – Curte(a) de apel

C. pen. – Codul penal

C. proc. pen. – Codul de procedură penală

C-PROC - Oficiul Consiliului Europei în domeniul criminalităţii informatice

CEPOL – Agenţia Uniunii Europene pentru Formare în Materie de Aplicare a Legii

CIPC – Comisia Internaţională de Poliţie Criminală

CSAT – Consiliul Suprem de Apărare a Ţării

DGA – Direcţia Generală Anticorupţie

DIICOT – Direcţiei de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism

EC3 – Centrul european de combatere criminalităţii informatice (European Cybercrime Centre)

ENISA – Agenţia Europeană pentru Securitatea Reţelelor şi a Informaţiilor

ETS – Programul european de formare în materie de aplicare a legii (European Training Scheme)

EUROJUST– Unitatea de Cooperare Judiciară a Uniunii Europene

Europol – Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a

Legii

FAO – Organizaţia Naţiunilor Unite pentru Alimentaţie şi Agricultură

FIDA – Fondul Internaţional pentru Dezvoltare Agricolă

FMI – Fondul Monetar Internaţional

Frontex – Agenţia Europeană pentru Poliţia de Frontieră şi Garda de Coastă

ICSID – Centrul Internaţional pentru Reglementarea Diferendelor Relative la Investiţii

ICT – Tehnologia informaţiei şi comunicaţiilor (Information and Communications Technology)

ID – Date de identificare (Identification Data)

IDA – Asociaţia Internaţională pentru Dezvoltare

IFC – Societatea Financiară Internaţională

IGPR – Inspectoratul General al Poliţiei Române

IGPF– Inspectoratul General al Poliţiei de Frontieră

Î.C.C.J. – Înalta Curte de Casaţie şi Justiţie

Lit. – litera

MAI – Ministerul Afacerilor Interne

MIGA – Agenţia Multilaterală de Garantare a Investiţiilor

M. Of. – Monitorul Oficial

NATO – Organizaţia Tratatului Atlanticului de Nord

Nr. – numărul

NCP – Noul Cod penal

OACI – Organizaţia Aviaţiei Civile Internaţionale

OECD – Organizaţia pentru Cooperare şi Dezvoltare Economică

OUG – Ordonanţa de urgenţă a Guvernului

OIM – Organizaţia Internaţională a Muncii

OMI – Organizaţia Maritimă Internaţională

OMS – Organizaţia Mondială a Sănătăţii

OMM – Organizaţia Mondială de Meteorologie

OMPI – Organizaţia Mondială a Proprietăţii Intelectuale

ONU – Organizaţia Naţiunilor Unite

ONUDI – Organizaţia Naţiunilor Unite pentru Dezvoltare Industrială

PIN – Cod numeric personal/Număr personal de identificare (Personal Identification Number)

S. pen. – Secţie penală

SELEC – Centrul de Aplicare a Legii pentru Europa de Sud-Est (Southeast European Law Enforcement Center)

TIC – Tehnologia informației și a comunicațiilor

TFUE - Tratatul privind funcționarea Uniunii Europene

TUE - Tratatul privind Uniunea Europeană

Trib. – Tribunalul

UE – Uniunea Europeană

UIT– Uniunea Internaţională a Telecomunicaţiilor

UNESCO – Organizaţia Naţiunilor Unite pentru Educaţie, Ştiinţă şi Cultură

UPU – Uniunea Poştală Universală

INTRODUCERE

Motto: „Răul nu vine de la tehnologie, ci de la cei care o folosesc în mod greşit,intenţionat sau accidental.”
Jacques Ives Cousteau[1]

Într-o eră în care termeni ca „pornografie infantilă”, „hacker”, „phishing”[2], „furt de identitate”, „cloud”[3] sunt întâlniţi tot mai frecvent în societatea noastră, se impune cunoaşterea profundă a acestora, precum şi întreprinderea unor măsuri legislative extrem de necesare care să apere individul, dar să şi sprijine statele lumii în lupta împotriva criminalităţii informatice. Având în vedere dezvoltarea tehnologică fără precedent, extinderea tipologiei infracţiunilor cibernetice, precum şi ameninţările continue la adresa siguranţei şi securităţii naţionale şi internaţionale, lucrarea de faţă se constituie a fi un pilon de consolidare a luptei împotriva criminalităţii informatice, aducând în prim plan ceea ce trebuie să facă legiuitorul în viitor şi nu caută să explice cauza săvârşirii infracţiunilor informatice, cauză care se cunoaşte: dorinţa rapidă de obţinere a unor câştiguri.

Am tratat aceasta temă în domeniul infracţiunilor informatice, pornind de la premisa că nu ştim niciodată suficient de mult în lupta cu ameninţările mediului

[1] Ofiţer francez, oceanograf, cercetător, explorator, scriitor, fotograf, producător de film, inventator, inovator. Nu a fost om de ştiinţă, ci mai degrabă impresar de oameni de ştiinţă, după cum bine se definea, informaţie disponibilă pe site-ul https://ro.wikipedia.org/wiki/Jacques-Yves_Cousteau, consultat la data de 2 ianuarie 2016, ora 12:08.

[2] Transmiterea unor e-mail-uri sau spam-uri false scrise să apară ca şi cum ar fi fost trimise de bănci sau organizaţii respectabile, cu intenţia de a ademeni destinatarul să divulge informaţii importante, cum ar fi nume de utilizatori, parole, ID-uri de cont, coduri PIN ale unor carduri de credit.

[3] Termenul provine din limba engleză, însemnând „nor”. În prezent, putem vorbi de o lărgire semantică a termenului, acesta reprezentând un concept modern, care îi permite utilizatorului să aibă acces la sisteme de resurse de calcul configurabile, prin intermediul internetului. Aplicaţiile şi datele utilizatorului sunt accesate de la distanţă, fiind salvate în altă parte, nu pe serverele şi staţiile utilizatorului. În funcţie de utilizator, putem identifica: cloud privat, cloud de comunitate, cloud public şi cloud hibrid. Cloudul privat reprezintă o infrastructură care poate fi utilizată de o singură organizaţie cu mai mulţi consumatori. Cloudul public reprezintă o infrastructură care este deţinută şi coordonată de un singur furnizor specializat de servicii, cu rol în protejarea eficientă a datelor din sistemul său. După cum spune şi denumirea, cloudul de comunitate este dedicat utilizării exclusive de o comunitate de consumatori cu interese comune. Cloudul hibrid constă în existenţa a două sau mai multe structuri cloud distincte, legate împreună de aceeaşi tehnologie, dar cu proprietăţi unice distincte.

cibernetic şi că factorul uman este de cele mai multe ori responsabil. În plus, fenomenul este destul de nou în ţara noastră care nu se poate mândri cu o literatură cibernetică vastă ca a altor state, în special pentru că oamenii sunt mai puţin familiarizaţi cu tehnologia ca parte integrantă a vieţii de zi cu zi. Alegerea temei de cercetare a fost determinată de amploarea pe care fenomenul o înregistrează în zilele noastre, mai ales la nivel naţional. Amploarea este dată în primul rând de mass-media care relatează zilnic infracţiuni ce intră sub incidenţa criminalităţii informatice, dar şi de scăpările legislative care fac ca infractorii să fie în libertate.

Tema aleasă contribuie la eforturile activităţii de cercetare în domeniul incident, prin lărgirea universului de cunoaştere în domeniul criminalităţii organizate în sens mai larg, iar în particular, a reglementării criminalităţii informatice din perspectivă naţională şi internaţională. Teza îşi propune să reliefeze aspecte teoretice şi practice referitoare la natura juridică, la definirea, conţinutul şi evoluţia criminalităţii informatice. Totodată, cuprinsul lucrării conţine aspecte semnificative ale criminalităţii informatice cu care organele de aplicare a legii se confruntă, dar şi eforturile pe care statele lumii le întreprind în vederea combaterii fenomenului. Urmărind criminalitatea informatică de la origini şi până în prezent, am încercat să evidenţiez rolul important pe care ţara noastră îl are la nivel european, dar şi mondial, precum şi faptul că este esenţialmente importantă cooperarea internaţională, aşa cum rezultă din rapoartele de evaluare ale unor agenţii implicate în domeniul de referinţă, dar şi din lucrările de cercetare ale unor reputaţi specialişti români şi străini.

Demersul de cercetare ştiinţifică ce a stat la baza redactării prezentei lucrări nu a fost unul uşor, ci sinuos, cauzat de faptul că domeniul de studiu este unul dinamic, spectaculos, cu care se confruntă din ce în ce mai multe state.

Din păcate, criminalitatea informatică reprezintă un „aşa-trebuie", *un mod de viaţă al infractorilor*[4], fiind preferată de aceştia pentru că-şi pot ascunde identitatea şi masca activităţile ilegale. După cum Lucius Annaeus Seneca[5] afirma că *„omul*

[4] Maxim, Dobrinoiu, *Provocarea legislativă a reţelelor Wi-Fi,* Revista Intelligence, Anul VI nr. 16, iulie 2009, p. 1.
[5] Lucius Annaeus Seneca (4 î.e.n – 65 e.n.) a fost filosof şi om de stat roman. Este autorul lucrărilor „Medeea", „Fedra", „Lucrări către Lucilius".

este ceva sfânt pentru om" (Homo res sacra homini), putem concluziona că şi calculatorul este ceva sfânt pentru infractor.

Privind înapoi spre începutul acestui secol mult încercat, observăm cu uşurinţă că tehnologia informaţiei este într-un proces continuu de schimbare, de modernizare, fapt ce afectează din temelii toate componentele existenţiale: politica, economia, industria, securitatea, precum şi psihicul uman. Evoluţia tehnologiei informatice a adus beneficii uriaşe omenirii, uşurând activitatea noastră zilnică, dar în acelaşi timp a creat condiţiile propice declanşării celui de-al Treilea Război Mondial, *Războiul Cibernetic*[6]. Putem face, desigur, o parafrazare a spuselor lui André Malraux, care afirma că *„secolul XXI va fi religios sau nu va fi deloc"*, concluzionând: *secolul XXI va fi un secol cibernetic sau nu va fi deloc*.

Dacă în timpul Primului Război Mondial, lupta s-a purtat între statele mari ale lumii, împărţite în cele două tabere : Antanta (Tripla Înţelegere)[7] şi Puterile Centrale (Tripla Alianţă)[8] sau în timpul celui de-al Doilea Război Mondial, supranumit şi Războiul Rece, când au fost afectate marile puteri ale lumii, situaţia se schimbă radical în Războiul Cibernetic, deoarece statele mici, slab dezvoltate din punct de vedere economic atacă marile puteri sau chiar supraputerile mondiale dominante. De data aceasta, cea mai importantă armă de luptă nu mai este bomba atomică, ci virusul informatic, specialiştii estimând existenţa a peste un milion de viruşi informatici. *„Cu Stuxnet*[9] *am deschis o nouă eră în istoria omenirii. Acum nu mai există nicio cale de a opri sau controla proliferarea armelor cibernetice.*[10]*"*

Virusul Stuxnet, troianul Duqu sau virusul Flame sunt numai câteva exemple din ceea ce ţările mai puţin dezvoltate economic au creat în lupta cu marile puteri. *The Washington Post* a publicat un articol la data de 19 iunie 2012, unde preciza că virusul Flame a fost dezvoltat de NSA, CIA şi armata israeliană,

---

[6] Afirmaţia este controversată, deoarece unii specialişti conchid că atacurile de la 11 septembrie 2001 au fost motorul declanşator al celui de-al Treilea Război Mondial împotriva terorismului. Atentatele sângeroase care au înspăimântat omenirea s-au soldat cu 2978 de morţi, fiind comise de 19 membri ai grupării teroriste Al-Qaeda care au deturnat patru avioane.

[7] Franţa, Anglia, Rusia, Japonia, Italia şi România.

[8] Germania, Austro-Ungaria, Imperiul Otoman şi Bulgaria.

[9] Primul virus utilizat pentru atacul asupra centralei nucleare din Iran.

[10] Ralph Langner, expert german în securitate.

cu cinci ani în urmă, în vederea strângerii unor informaţii despre programul nuclear iranian. Colectarea informaţiilor a fost parte a unor operaţiuni secrete cu numele de cod „Jocurile Olimpice”[11].

După cum observăm, ramurile criminalităţii informatice nu afectează numai individul, persoana fizică, ci TOTUL. *„Victimele războiului în spaţiul virtual pot fi persoanele fizice, marile corporaţii sau concerne industriale şi economice şi chiar statele, ţintele fiind infrastructurile informatice guvernamentale, agenţiile din domeniul intelligence-ului sau al apărării, infrastructura critică a unei ţări: reţele de distribuţie a energiei electrice şi a gazelor, centrale electrice, nucleare, sisteme de comunicaţii, reţele de transport etc.”*[12]

Este foarte importat ca statele lumii să lupte pentru o strategie de securitate cibernetică puternică care să sprijine guvernele în lupta cu această ciumă a secolului XXI. Combaterea criminalităţii informatice nu mai constituie apanajul exclusiv al fiecărui stat în parte, ci reprezintă o problemă comună a statelor lumii, bazată pe valori universale.

Internetul[13] este cel mai uşor mijloc de a săvârşi o infracţiune. Cu un simplu „click” se pot câştiga milioane de euro sau pagubele pot fi atât de mari, încât nu se mai poate recupera nimic. Ira Winkler[14] spunea: *„Pe internet, fiecare calculator este o frunză dintr-un copac. Este suficient să tai o creangă şi rezultatul echivalează cu tăierea frunzei. Asta înseamnă că, deşi aveţi cel mai bun sistem de securitate, eu pot să vă distrug imediat, tăindu-vă contactul cu restul lumii”.*

Inovaţia ştiinţifică a lucrării constă în faptul că aceasta aduce un plus problematicii de referinţă, prezentând fenomenul criminalităţii informatice macro-contextual, la nivel european în strânsă legătură cu problematica globală. Lucrarea nu se rezumă în a prezenta doar o vedere de ansamblu asupra fenomenului, pentru că acesta este rolul literaturii de specialitate, ci subliniază un adevăr: criminalitatea

[11] Radu, Moinescu, *Viruşii – risc şi ameninţare asupra sistemelor informatice*, Revista Intelligence nr. 23/2012, p. 5-7.
[12] Carmen, Postelnicu; Sorana, Marmandiu, *Perspective teoretice asupra ameninţărilor cu incidenţă în domeniul securităţii*, Revista Intelligence nr. 23/2012, p.44.
[13] La nivel internaţional se foloseşte şi termenul "cyberspace". Acesta a fost introdus în 1982 de scriitorul William Gibson (cunoscut publicului după romanul "Neuromancer"), în nuvela publicată "Burning Chrome".
[14] Unul dintre cei mai mari specialişti în testarea securităţii calculatoarelor, director la NCSA.

informatică nu este un domeniu de nepătruns, al secretelor virtuale, ci reprezintă o problemă concretă cu care omenirea se confruntă şi pentru care cooperarea internaţională este vitală.

La întocmirea prezentei lucrări, am utilizat metode de cercetare precum analiza istorică, comparativă, logică şi prospectivă, având în vedere că acestea urmăresc evoluţia integrală a fenomenului, cauzele, în vederea fundamentării unor strategii. Principalele surse consultate au fost: *primare* (documente oficiale, acte normative de la nivel naţional şi global, date statistice, interviuri, fotografii, fişiere electronice), *secundare* (analize, comentarii) şi *terţiare* (analize, cronologii, cursuri, manuale). Regula cea mai importantă este ca „fiecare dovadă şi sursă să fie analizate în mod sceptic şi critic”[15].

Lucrarea cuprinde o parte teoretică, şapte capitole, inclusiv propuneri de lege ferenda, concluzii şi bibliografie.

[15] Peter Pappas: http://www.edteck.com/dbq/more/analyzing.htm, site consultat la data de 1ianuarie 2016, ora 17:51.

CAPITOLUL I
CONSIDERAŢII GENERALE CU PRIVIRE LA CRIMINALITATEA INFORMATICĂ

Primul capitol al tezei este dedicat conceptului de criminalitate informatică în strânsă legătură cu evoluţia societăţii, trecerea de la Războiul Rece la Războiul Cibernetic care a schimbat radical cursul firesc al omenirii. Principalul motor care a declanşat această schimbare îl constituie calculatorul[16] care a devenit indispensabil în activitatea noastră zilnică. Nicio altă invenţie nu va putea egala în însemnătate ceea ce astăzi numim CALCULATOR. De la un simplu mediu de stocare a informaţiilor, de achiziţionare a unor produse, acesta a ajuns să reprezinte o unealtă de temut pentru multe persoane fizice, societăţi comerciale, sisteme bancare, organisme guvernamentale, lista putând continua.

Matematicianul american, Norbert Wiener[17], a pus bazele calculatorului electronic care avea posibilitatea de a efectua operaţii matematice şi logice, cu posibilitatea de a stoca datele şi informaţiile prelucrate. Specialiştii au agreat că descoperirea tranzistorului şi a circuitelor integrate a avut o dezvoltare fulminantă care a condus la apariţia internetului. Aceasta a depins evident de tehnologie, dar în egală măsură de factorii sociali care s-au îmbinat cu factorii tehnologici pentru ca internetul să ajungă ceea ce a devenit astăzi. Odată instaurat în fibrele societăţii, internetul a produs şi produce consecinţe noi pentru societate[18]. Din păcate, aceste consecinţe sunt nefaste şi se regăsesc frecvent în rata crescândă a criminalităţii. Apariţia şi dezvoltarea galopantă a internetului au condus la globalizare, fenomen

[16] Cuvântul „calculator” (engl. computer; fr. ordinateur; Germ. elektronische rechenmashine) desemnează maşina capabilă să efectueze automat operaţii aritmetice şi logice, plecând de la programe care definesc secvenţa acestor operaţii, cf. Dictionnaire de notre temps, Ed. Hachette, Paris, 1988.

[17] A trăit în perioada 26.11.1894 – 18.03.1964. Şi-a pus amprenta asupra matematici şi ciberneticii, fiind premiat în 1963 cu Medalia naţională pentru ştiinţă.

[18] Acad. Mihai, Drăgănescu, *Societatea informaţională şi a cunoaşterii. Vectorii societăţii cunoaşterii*, informaţie disponibilă pe site-ul http://www.academiaromana.ro/pro_pri/pag_com01socinf_tem.htm, consultat la data de 1 ianuarie 2016, ora 17:53

disputat la momentul actual.

Definirea termenului de criminalitate informatică[19] a stat la baza a numeroase întâlniri, conferinţe, organizate la nivel european, dar şi mondial, întrucât combaterea acestui flagel al secolului XXI constituie nu o problemă naţională, europeană, ci una mondială. Adesea efectele benefice ale calculatorului sunt înlocuite de cele negative, acesta fiind considerat o unealtă de săvârşire rapidă a unor infracţiuni.

Unii specialişti au definit fenomenul drept *„orice acţiune ilegală în care un calculator constituie instrumentul sau obiectul delictului”* sau *„orice infracţiune al cărei mijloc sau scop este influenţarea funcţiei calculatorului”*. Conform altei definiţii, delictul informatic reprezintă *„orice incident legat de tehnica informatică, în care o victimă a suferit sau ar fi putut să sufere un prejudiciu şi din care autorul a obţinut sau ar fi putut obţine intenţionat un profit”*.

În momentul actual, nu există o definiţie unanim acceptată a noţiunii de „criminalitate informatică”. Încercările de definire a termenului sunt multiple, acest lucru explicându-se prin complexitatea şi amploarea cu care fenomenului se manifestă.

Privind înapoi la momentul zero al criminalităţii informatice, trebuie să menţionăm anul 1983, când au avut loc primele încercării de definire a termenului. Organizaţia pentru Cooperare şi Dezvoltare Economică a hotărât la Paris constituirea unui grup de specialişti care să analizeze infracţiunile informatice şi crearea unui cadrul legislativ.

În 1986, raportul experţilor definea noţiunea de *„infracţiune informatică”,* ca fiind *„orice comportament ilegal, non-etic sau neautorizat ce priveşte un tratament automat de date şi/sau o transmisie de date”*[20]. Profesorul Tudor Amza

[19]La nivel internaţional, este folosit şi termenul criminalitate cibernetică/cybercrime. Din punct de vedere etimologic, "cybercrime", alătură termenii "crime" şi "cyber" de la "cybernetic”, de la grecescul „kybernetes”, care înseamnă „a conduce” sau „a guverna”. Ulterior, termenul a fost introdus de matematicianul Norbert Wiener în 1948, în cartea sa "Cybernetics". Mediul cibernetic include toate tipurile de activităţi digitale, indiferent dacă sunt întreprinse prin intermediul reţelelor fără frontiere. Astfel, noţiunea de criminalitate informatică/computer crime cuprinde infracţiunile săvârşite prin intermediul Internetului, toate infracţiunile digitale, precum şi pe cele din cadrul reţelelor de telecomunicaţii.

[20] International Telecommunication Union, Cybercrime Legislation Resources, *Understanding Cybercrime: A Guide for Developing Countries,* disponibil la adresa: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding

defineşte criminalitatea informatică ca fiind *„acea faptă prevăzută de legea penală, comisă cu vinovăţie, de către o persoană sau un grup de persoane care folosesc un calculator, şi, cu ajutorul comunicării informaţiilor prin cablu, comit o faptă care prezintă pericol social ce aduce prejudicii unei persoane, unei societăţi comerciale ori intereselor statului*[21]".

La nivel internaţional, au fost folosiţi pentru prima oară termenii *"computer crime"* (criminalitate informatică) şi *"computer related crime"* (criminalitate în legătură cu utilizarea calculatorului), în legislaţiile Statelor Unite ale Americii şi ale Regatului Unit al Marii Britanii şi al Irlandei de Nord. Adrian Cristian Moise[22] precizează faptul că infracţiunile prezente în legislaţiile invocate erau reduse ca număr, menţionând furtul de servicii utilizând computerul, accesul neautorizat la computerele protejate; pirateria software şi alterarea sau furtul de informaţii stocate electronic; stoarcerea de bani comisă cu ajutorul computerului, accesul neautorizat în reţelele bancare, traficul cu parole furate şi transmiterea de viruşi distructivi sau comenzi.

ONU a acceptat utilizarea simultană a celor doi termeni, făcând precizări şi în ceea ce priveşte distincţia dintre *"computer abuse"* (abuz informatic) şi *"computer misuse"* (utilizarea greşită a calculatorului). Primul termen semnifică intenţia voită de fraudă, în timp ce al doilea se referă la accesarea involuntară a calculatorului. Un alt termen utilizat la nivel internaţional în referire la criminalitatea informatică este termenul *"cybercrime"*[23] (criminalitate cibernetică), care se referă la infracţiunile comise utilizând computerele şi reţeaua internet.

Majoritatea ghidurilor, a rapoartelor sau publicaţiilor privind criminalitatea informatică au sesizat diferenţa între „criminalitatea informatică" şi „criminalitate în legătură cu utilizarea calculatorului". Astfel, prima noţiune are un sens mai restrâns decât cea de-a doua care implică o reţea de calculatoare.

- cybercrime -guide.pdf, consultat la data de 1 ianuarie 2016, ora 19:39.

[21] Tudor, Amza; Cosmin-Petronel Amza, op. citată, p.54.

[22] Adrian, Cristian Moise, *Metodologia investigării criminalităţii infracţiunilor informatice***,** Ed. Universul Juridic, Bucureşti, 2011, p.16

[23] În unele studii se întâlneşte termenul high-technology (înaltă tehnologie).

Myriam Quéméner[24] afirmă că noţiunea menţionată cuprinde ansamblul infracţiunilor săvârşite într-un mediu virtual, cu ajutorul internetului. Aceste infracţiuni se împart în două categorii[25]: 1) cele care au la bază accesul neautorizat la date şi sisteme în vederea săvârşirii unor fapte ilegale, 2) referitoare la fraudă, falsificare, deturnare de fonduri, obţinere de câştig ilicit, defăimare prin intermediul serviciilor on-line.

Într-un studiu[26] privind criminalitatea informatică realizat în China, Sun Tianzhu şi Cao Peizhong susţin că aceasta include toate infracţiunile care au la bază utilizarea calculatorului ca principal instrument, precum şi pe cele care urmăresc obţinerea unor bunuri cu ajutorul calculatorului. Infracţiunile sunt săvârşite de persoane care au cunoştinţe vaste de specialitate, prin metode extrem de tehnice din lumea virtuală. În definiţia lui Chen Junjing[27] privind criminalitatea informatică sunt incluse următoarele infracţiuni: fraudă, pornografie virtuală şi hărţuire sexuală, traficul şi vânzarea de bunuri interzise, încălcarea vieţii private, precum şi producerea şi distribuirea unor viruşi.

Cercetătorii japonezi au agreat că majoritatea infractorilor virtuali săvârşesc infracţiuni precum prostituţia, traficul de droguri, furtul parolei, transferul neautorizat de fonduri, precum şi distribuirea unor materiale cu drept de autor.

În Olanda[28], termenul este folosit drept „concept-umbrelă" pentru toate infracţiunile în care ICT joacă un rol esenţial: accesul neautorizat, frauda informatică, sabotajul informatic, pornografia infantilă şi infracţiuni săvârşite prin violenţă.

Spre deosebire de definiţiile prezentate care sunt mult mai restrânse conceptual, Departamentul de Justiţiei al Statelor Unite ale Americii consideră ca

[24] Fost auditor al Institut des Hautes Études de Défense National din Paris (Institutul de Înalte Studii şi Apărare), expert al Consiliului Europei şi conducător al sedinţei privind criminalitatea informatică în cadrul École Nationale de la Magistrature (Şcoala Naţională de Magistratură) de la Bordeaux.

[25] Glenn, Curtis; Ronald, Dolan; Seth, Elan; Noël, Ivey; Carl, Minkus; Eric, Solsten; Taru, Spiegel; Tomoko, Steen; *Cybercrime: An Annotated Bibliography of Selected Foreign-language Academis Literature*, November 2009, disponibil pe site-ul https://www.ncjrs.gov/pdffiles1/nij/231832.pdf, consultat la data de 1 februarie 2016, ora 18:00.

[26] Glenn Curtis, Ronald Dolan, Seth Elan, Noël Ivey, Carl Minkus, Eric Solsten, Taru Spiegel, Tomoko Steen, *stud.cit.*

[27] A realizat studiul privind aspectele legale ale criminalităţii informatice.

[28] *Cybercrime in the Netherlands 2009 a picture on the basis of police files*, disponibil la adresa: http:// http://www.slideshare.net/socialmediadna/cybercrime-in-the-netherlands-2009, consultat la data de 1 ianuarie 2016, ora 18:02.

fiind infracţiuni informatice orice fapte de natură penală care implică cunoaşterea tehnologiei computerelor în ceea ce priveşte săvârşirea, investigarea sau anchetarea acestora[29].

Consider că cea mai cuprinzătoare definiţie a fenomenului o reprezintă cea elaborată de experţii în domeniu, sub îndrumarea profesorului Solange Ghernaouti – Hélie[30], unde criminalitatea informatică este considerată a fi o extensie a activităţii criminale obişnuite. Astăzi, actele criminale sunt săvârşite în mediul virtual, folosind mijloace neconvenţionale într-o manieră care este complementară infracţiunilor obişnuite.

În ceea ce priveşte tipologia infracţiunilor informatice, putem afirma negreşit că este foarte variată. Acest lucru se explică prin faptul că tehnica de lucru a infractorilor este una extrem de specializată, cunoştinţele în domeniu foarte vaste, iar setea de documentare a lor pentru săvârşirea infracţiunilor este mare. Lumea ICT este fină, în ea reuşind să trăiască numai cei care ajung să-i cunoască secretele foarte bine. Tehnologia evoluează la fiecare secundă şi de aceea infracţiunile sunt atât de diferite. Ceea ce este îngrijorător este faptul că tinerii, la o vârstă extrem de fragedă sunt pătrunşi de această sete de nou, sete care este dusă la extrem, până la săvârşirea unor infracţiuni, întărind ideea potrivit căreia calculatorul va fi implicat în toate formele de delincvenţă.

Mulţi scolastici au încercat să identifice tipurile de infracţiuni informatice. Parker[31] a propus clasificarea lor în funcţie de rolul calculatorului în timpul săvârşirii infracţiunii: calculatorul ca obiect al infracţiunii, calculatorul ca subiect al infracţiunii, calculatorul ca mijloc de săvârşire a infracţiunii şi calculatorul ca simbol.

[29] Mohamed, Chawki, *A Critical Look at the Regulation of Cybercrime*, disponibil la adresa: http://www.crime-research.org/articles/Critical/, consultat la data de 1 ianuarie 2016, ora 20:20.
[30] Din cadrul Universităţii de la Laussanne – Facultatea de Afaceri şi Economie din Elveţia. Studiul este disponibil pe site-ul http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf, consultat la data de 1 ianuarie 2016, ora 18:12.
[31] D.B. Parker, *Crime by Computer*, New York: Charles Scribner's Sons, 1976; D.B. Parker, *Fighting Computer Crime*, New York: Charles Scribner's Sons, 1983, p.283.

David Wall[32] (2001) face două distincţii în legătură cu criminalitatea informatică, în funcţie de generaţii: prima generaţie care foloseşte calculatoarele pentru activitate infracţională, în timp ce a doua este implicată în reţele. Cea de-a treia generaţie care ia naştere este automată şi mediată de tehnologie.

Majid Yar (2006)[33] clasifică infracţiunile informatice în funcţie de obiectul sau ţinta infracţiunii: infracţiuni contra patrimoniului, infracţiuni contra moralităţii, infracţiuni contra persoanei şi infracţiuni contra statului.

Michael Cross (2008)[34] împarte infracţiunile informatice în: gulere albe (încălcarea spaţiului informatic, furtul pe internet, infracţiuni informatice distructive sau fraude on-line), cu non-violenţă (jocurile de noroc pe internet, spălarea de bani pe internet şi reclama/solicitarea de servicii de prostituţie), cu violenţă sau cu potenţial violenţă (terorismul cibernetic, atacul prin ameninţare, hărţuirea electronică şi pornografia infantilă).

În 2011, în India, specialiştii[35] implicaţi în cercetarea infracţiunilor informatice au afirmat că, criminalitatea informatică poate fi definită ca orice infracţiune împotriva unei organizaţii sau individ, făptuitorul folosind un calculator sau orice parte a acestuia pentru a săvârşi delictul. Clasificarea infracţiunilor propusă este mult mai amplă, căutând să lărgească spectrul, astfel:

1. Interceptarea neautorizată: accesul neautorizat; interceptarea; furtul de timp.
2. Modificarea datelor stocate în calculator: bomba logică; calul Troian; virusul, viermele.
3. Frauda în legătură cu calculatorul: bancomat; falsul informatic; manipularea

[32] David S. Wall, *The Transformation of Crime in the Information Age*, 2007, Polity Press, Cambridge, UK, studiul este disponibil la adresa: http://www.gobookee.net/get_book.php?u=aHR0cDovL3d3dy5jeWJlcmNyaW1lam91cm5hbC5jb20vSGlldGFuZW5ib29rcmV2aWV3SnVseTIwMDkucGRmCkJvb2sgUmV2aWV3IG9mIEN5YmVyY3JpbWU6IFRoZSBUcmFuc2Zvcm1hdGlvbiBvZiBDcmltZSBpbiB0aGUgLi4u., consultat la data de 01.01.2016, ora 18:23. David Wall este profesor de criminologie şi directorul Şcolii de Ştiinţe Sociale Aplicate din cadrul Universităţii Durham din Anglia.

[33]Neil, Robison; Emma, Disley; Dimitris, Potoglou; Anais, Reding; Deidre, Culley; Maryse, Penny; Maarten, Botterman; Gwendolyn, Carpenter; Colin, Blackman and Jeremy, Milliard, **Feasibility Study for a European** *Cybercrime Center, Final Report***,** studiul este disponibil pe site-ul: http://www.rand.org/content/dam/rand/pubs/technical_reports/2012/RAND_TR1218.pdf., consultat la data de 1 ianuarie 2016, ora 18:25.

[34] Ibidem.

[35] J. Keziya, Rani; S. Prem, Kumar; U. Ram, Mohan; C. Uma, Shankar, *Laptop Theft Analysis for Digital Investigations, International Journal of Computer& Organization Trends* – Volume1Issue 2- 2011, p.5

de program; pirateria de program; frauda la punctele de plată.

4. Reproducerea neautorizată:

   Pirateria software

5. Sabotajul informatic: sabotajul hardware; sabotajul software.
6. Infracţiuni informatice amestecate: furtul secretelor comerciale; distribuirea materialelor cu conţinut antisocial; spionajul electronic; piggybacking[36] şi tailgating[37]; baleiajul şi reutilizarea; scanarea; atacurile asincronice; furtul unor dispozitive IT.

Infracţiunile informatice sunt săvârşite fie din dorinţa câştigului care poate apărea în urma comiterii lor, fie dintr-o pornire interioară, rezultată din „cyberdependenţă". Interesant este de urmărit dacă persoanele care petrec foarte mult timp în faţa calculatorului sunt viitorii infractori. Într-un studiu[38] publicat de Şcoala de medicină a Universităţii Standford din California a reieşit că aproximativ 14% dintre utilizatorii de Net americani dau semne de „cyberdependenţă". Studiul a fost realizat pe un eşantion de 2513 persoane de la nivelul celor 50 de state americane, fiind primul de acest tip cu rolul de a măsura utilizarea excesivă a internetului şi cauzele care pot apărea ulterior. Dr. Elias Abujaud, directorul clinicii pentru tulburări de control al impulsurilor, în cadrul Departamentului de psihiatrie şi medicină comportamentală de la Standford a precizat faptul că timpul excesiv petrecut pe internet nu se limitează la site-uri pornografice sau cazinouri on-line: el se extinde la bloguri, la verificarea mail-urilor din cinci în cinci minute sau la site-uri specializate pe teme de bursă sau pieţe financiare. Cyberdependenţa, prea puţin cunoscută sau studiată la noi trebuie pusă în strânsă legătură cu criminalitatea informatică. Un comportament aparent nevinovat, o simplă accesare a unei pagini de internet poate duce în timp la săvârşirea unei infracţiuni. Doctorul menţionat a concluzionat: *„O parte semnificativă a populaţiei prezintă semne suficient de tangibile pentru a putea fi catalogate drept o problemă, chiar dacă nu*

[36] Accesul la internet, „călărind pe spatele altuia", stabilirea unei conexiuni wireless la internet, folosind serviciul wireless de internet al unui abonat, fără permisiunea acestuia.
[37] A urmări pe cineva pentru a obţine datele financiare de identificare (ex. la ATM).
[38] A apărut în Jurnalul de sănătate, supliment de sănătate al cotidianului Jurnalul Naţional, 2007, p.9

se poate vorbi încă despre o dependenţă de internet". Comiterea infracţiunilor informatice are la bază o utilizare frecventă a calculatorului, o bună însuşire a termenilor de specialitate, precum şi aprofundarea domeniului în care acestea vor fi săvârşite.

Cercetarea fenomenului criminalităţii informatice trebuie să se facă în strânsă legătură cu evoluţia criminalităţii organizate. Criminalitatea informatică reprezintă o ramificaţie a criminalităţii organizate, singura diferenţă fiind că prima cunoaşte o activitatea de pregătire mult mai profundă şi inteligentă, utilizând cele mai performante mijloace.

Sociologii susţin că anumite medii sunt prielnice delicvenţei care sprijină dezvoltarea criminalităţii organizate. Consider că cea mai completă definiţie dată acesteia este a FBI –ului care o considera a fi *„acea organizaţie care foloseşte şi perpetuează conspiraţia criminală, are o structură organizată, îşi bazează existenţa pe teamă şi teroare, corupţie şi manipulări ilicite şi urmăreşte obţinerea de beneficii financiare şi alte avantaje"*[39].

Privită în ansamblu, ca fenomen, criminalitatea informatică este o creaţie a secolului nostru, menită să aducă profituri uriaşe prin săvârşirea unor infracţiuni (trafic de persoane, trafic de droguri, spălarea de bani, prostituţie, trafic de arme). Din punct de vedere juridic, criminalitatea reprezintă totalitatea infracţiunilor săvârşite pe un teritoriu determinat într-o anumită perioadă de timp.

„Visul american al infractorilor[40]" este acela de săvârşire a unor infracţiuni informatice pe raza altor teritorii, pentru că de foarte multe ori acestea rămân nepedepsite.

Ca o concluzie, putem spune că istoria criminalităţi informatice este o competiţie între cei care săvârşesc fapte şi cei care încearcă să prevină înfăptuirea lor.

---

[39] National Security Council, *International Crime Threat Assessment*, disponibil pe site-ul http://fas.org/irp/threat/pub45270index.html, consultat la data de 1 ianuarie 2016, ora 21:35.

[40] Cel mai cunoscut hacker este Kevin Mitnick care la vârsta de 17 ani a fost condamnat. Deşi era în închisoare, reprezenta o adevărată ameninţare pentru siguranţa calculatoarelor.

CAPITOLUL II
PRINCIPALELE MANIFESTĂRI ALE CRIMINALITĂŢII INFORMATICE ÎN STATELE MEMBRE ALE UNIUNII EUROPENE

Cel de-al doilea capitol cuprinde principalele manifestări ale criminalităţii informatice la nivel naţional, precum şi cele apărute în spaţiul european.

Deşi criminalitatea informatică pare a fi la început la nivel naţional, prin multitudinea infracţiunilor şi zonelor acoperite, putem să deducem că infractorii naţionali din domeniu şi-au performat tehnica încât îi întrec cu mult pe cei din afară, creând uneori adevărate enigme pentru reprezentanţii autorităţilor străine de aplicare a legii. Fenomenul „a atras" infractorii prin anumite caracteristici: profitabilitate, vulnerabilitate, posibilitatea ca locul de comitere să fie mereu altul, uşurinţa de a înşela persoanele foarte tinere sau pe cele în vârstă etc. Ceea ce s-a obţinut până în prezent a fost producerea unei discrepanţe cantitative între nivelul de pregătire a personalului implicat în combaterea fenomenului şi diversificarea mediului infracţional. Cu toate că majoritatea prevederilor Convenţiei Consiliului Europei privind criminalitatea informatică, instrumentul principal de luptă împotriva fenomenului acoperă sfera infracţionalităţii informatice, din 2001 şi până în prezent, autorităţile nu au mai putut găsi un numitor comun şi modifica actul normativ menţionat. Putem spune că acesta este un punct în minus al statelor faţă de infractorii care îşi menţin tehnica la un nivel avansat. Softurile şi infracţiunile sunt direct proporţionale, în sensul că, cu cât tehnica informaţiilor avansează, modus operandi al infractorilor se îmbunătăţeşte. În schimb, autorităţile de aplicare a legii sunt în urmă şi cu activitatea legislativă şi cu procesul de modernizare a tehnicii.

Anul 2010 a cunoscut o intensificare a fenomenului infracţional informatic, în sensul că spectrul infracţiunilor în domeniul de referinţă s-a lărgit din cauza dezvoltării tehnologiei informaţionale. Pornografia infantilă a apărut sub diverse forme: prin sisteme informatice, reţele de comunicare, suporţi de stocare a datelor sau prin intermediul mult controversatelor reţele de socializare.

În anul 2012 şi-au făcut apariţia la nivel naţional cazurile de „ransomware”[41], viruşi derivaţi din virusul Zeus[42], pornografia infantilă, cele mai frecvente fiind licitaţiile frauduloase. Deşi ţara noastră nu înregistrează foarte multe cazuri de pornografie infantilă, anchetatorii au confirmat existenţa cazurilor de *„filmare/fotografiere în timpul raportului sexual şi postarea imaginilor pe internet, dar şi fapte grave de molestare a unor minori urmate de filmarea/fotografierea agresiunii şi schimbul de astfel de imagini prin intermediul internetului”*.

În urma Raportului pentru anul 2013 al companiei americane de telecomunicaţii Verizon Communications Inc. privind investigaţiile referitoare la încălcarea securităţii datelor cu caracter personal ("2013 Data Breach Investigations Report"), România ocupa locul doi în topul infracţiunilor privind accesul neautorizat, după China[43].

Deşi în ţara noastră predominante sunt infracţiunile de tipul organizării de licitaţii frauduloase, phishingului[44] sau skimmingului[45], autorităţile de aplicare a legii s-au implicat activ în soluţionarea tuturor cererilor internaţionale în care se solicită sprijinul. În cadrul vizitei sale la Bucureşti la data de 24.01.2013, secretarul general al Interpolului, domnul Ronald Noble afirma: *„Aveţi una dintre cele mai*

---

[41] Aplicaţie malware care împiedică utilizarea calculatorului până când este plătită o sumă de bani unei persoane/grupări aflată/e la distanţă

[42] Este de tip troian, se instalează în calculator şi rămâne inactiv în computer, până când utilizatorul îşi accesează contul bancar. Virusul este produsul unei organizaţii criminale din Rusia care săvârşea infracţiuni precum furtul de identitate sau pornografia infantilă. Virusul Zeus şi-a făcut apariţia îndeosebi pe Facebook. Potrivit unui studiu făcut de compania Kaspersky, acesta *„a fost vândut cel mai bine pe piaţa neagră”,* probabil pentru că a fost generator de profituri uriaşe.

[43] Statistica este îngrijorătoare, ţara noastră depăşind mari puteri ale lumii. Primele zece ţări, în care hackingul este o activitate în top sunt: China, România, Statele Unite ale Americii, Bulgaria, Rusia, Olanda, Armenia, Germania, Columbia şi Brazilia.

[44] 80% dintre infracţiunile săvârşite în România sunt îndreptate asupra cetăţenilor americani.

[45] 80% dintre infracţiunile săvârşite de români sunt îndreptate asupra cetăţenilor din vest.

active şi profesioniste poliţii din lume. România este o ţară sigură. Dacă în România este siguranţă, în Europa este siguranţă şi în lume este siguranţă”.

Raportul activităţii DIICOT pentru anul 2015 evidenţiază un trend ascendent al cauzelor (2677) având ca obiect infracţiuni privind criminalitatea informatică, o creştere cu 28,83% faţă de anul precedent. În urma analizei activităţii de urmărire penală, observ numărul crescut al cauzelor având ca obiect infracţiuni comise în România de cetăţeni letoni, ucraineni, bulgari şi moldoveni, care au dezvoltat adevărate scheme infracţionale, cele mai des întâlnite fiind cele de tip skimming. Anul 2015 s-a remarcat prin apariţia unor forme grave de molestare a unor minori, circumscrise pornografiei infantile, fapte urmate de filmarea agresiunii şi, ulterior, distribuirea acestora prin intermediul internetului sau transmise în direct.

Şi in cursul anului 2016, s-a înregistrat o creştere a inculpaţilor trimişi în judecată, cu 1,87% faţă de anul anterior.

O grupare de hackeri ruşi[46], condusă de Dmitriy Kvasov, a furat 860 000 € de la 32 ATM-uri aparţinând Băncii Raiffeisen România. Anchetatorii au subliniat că atacatorii au vizat numai sisteme din România, dar odată ce au compromis reţeaua bancară, au fost capabili să controleze orice ATM din lume aparţinând instituţiei financiare.

Având în vedere modificările legislative de la nivel european, structurile specializate din România sunt implicate activ în prevenirea şi combaterea tuturor formelor de criminalitate informatică, de la cele mai simple, precum accesarea telefonului, a contului de socializare la forme complexe, activităţi desfăşurate de grupuri de criminalitate organizată. Aşa se explică şi numărul mare de la an la an al inculpaţilor trimişi în judecată prin faptul că magistraţii apelează la toate instrumentele pentru identificarea şi pedepsirea acestora. Având în vedere spectrul larg al infracţiunilor informatice, autorităţile de aplicare a legii trebuie să-şi dedice activitatea asupra studierii modului de operare şi a tendinţelor pe termen lung.

[46] http://securityaffairs.co/wordpress/70046/cyber-crime/raiffeisen-cyber-heist.html, consultat la data de 11 martie 2018, ora 22:49

Anul 2017 a marcat întărirea cooperării între autorităţile naţionale şi cele din Olanda, SUA şi Marea Britanie pentru identificarea autorilor unui atac de tip ransomware (CTB Locker). La nivel global s-a manifestat o nouă tendinţă care a afectat şi România, deep insert skimming, un attack de tip skimming, care s-a răspândit rapid din Europa spre America de Nord şi ţările zonei Asia-Pacific.

În urma analizei tipurilor de infracţiuni informatice săvârşite de conaţionali, putem să identificăm cu uşurinţă trendul din domeniu: infracţiuni uşor de săvârşit, cu o tehnică modernă, generatoare de profituri maxime. Grupurile de criminalitate informatică sunt foarte organizate, structurate şi bine pregătire, evidenţiindu-se o bună cunoaştere a informaticii, a reţelelor.

Asigurarea securităţii informaţionale de la nivel internaţional poate fi realizată printr-o bună cooperare internaţională între organismele abilitate în lupta contra criminalităţii informatice, dar şi între cele două sectoare: privat şi public care pot face faţă dinamismului tehnologiei informaţionale.

În urma raportului realizat de Symantec în 2017, Norton Cyber Security Insights Report, 978 milioane de consumatori de la nivel global au fost victime ale criminalității informatice. Astfel, 53% au avut un dispozitiv infestat de virus ori s-au confruntat cu altă amenințare la adresa securității, 38% au avut experiențe negative legate de fraude cu carduri de credit sau de debit, 34% au avut parola contului personal compromisă, 34% s-au confruntat cu accesul neautorizat sau "hacking" la contul de e-mail/rețea de socializare, 33% au făcut achiziţii on-line care s-au dovedit a fi escrocherii. În concluzie, la nivel global, consumatorii care au fost victime ale infracţiunilor cibernetice au pierdut 172 miliarde de dolari, în medie 142 dolari/victimă şi aproximativ 24 de ore (3 zile de muncă) în care s-au confruntat cu urmările infracţiunilor.

Cel mai mare atac cibernetic de tip ransomware din istorie, WannaCry (vrei să plângi), s-a produs în luna mai 2017, lovind instituţii şi companii din peste o sută de ţări, România fiind pe locul nouă. Atacul s-a răspândit rapid, hackerii profitând de o vulnerabilitate existentă în sistemul de operare Microsoft.

Majoritatea atacurilor au vizat Rusia, Ucraina şi Taiwan. Aceştia au solicitat o recompensă de 300 de dolari pentru decriptarea fişierelor, în monedă virtuală.

După cum putem observa, atacurile informatice devin tot mai sofisticate şi se manifestă asupra marilor puteri ale lumii care sunt de cele mai multe ori nepregătite să le facă faţă. Deşi la nivel mondial conducătorii se luptă să adopte strategii în vederea combaterii flagelului, atacurile informatice sunt din ce în ce mai dinamice şi frecvente. Cu cât ne pregătim mai mult în faţa unor posibile acţiuni informatice de natură teroristă, cu atât suntem mai vulnerabili şi nepregătiţi atunci când acestea se manifestă. Vulnerabilitatea se traduce prin apariţia unor viruşi mereu noi. Putem face analogia cu lumea medicală, în sensul că, cu cât luăm mai multe antibiotice, cu atât organismul nu mai reacţionează la viruşi. Aşa este şi în cazul criminalităţii informatice, lumea este din ce în ce mai pregătită, atât teoretic, cât şi tehnologic, dar, de fapt, vulnerabilitatea ei atinge cote alarmante.

CAPITOLUL III
ANALIZA UNOR INFRACŢIUNI INFORMATICE ÎN LEGISLAŢIA NAŢIONALĂ

Moto: „Cel mai trist aspect al vieţii actuale este că ştiinţa acumulează cunoştinţe mai repede decât acumulează societatea înţelepciune. [47] (*Isaac Asimov*[48])

În cel de-al treilea capitol, am analizat cele mai importante infracţiuni din domeniul incident, după cum urmează: falsul informatic, frauda informatică, accesul ilegal la un sistem informatic, interceptarea ilegală a unei transmisii de date informatice, alterarea integrităţii datelor informatice şi perturbarea funcţionării sistemelor informatice

Codul penal român defineşte falsul informatic în cadrul articolului 325 după cum urmează: *„Fapta de a introduce, modifica sau şterge, fără drept, date informatice ori de a restricţiona, fără drept, accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecinţe juridice, constituie infracţiune şi se pedepseşte cu închisoare de la unu la 5 ani”.*

Potrivit definiţiei prezentate, falsul informatic reprezintă fapta persoanei de a introduce, modifica sau şterge date informatice ori de a restricţiona accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecinţe juridice.

Legiuitorul român a realizat o armonizare a legislaţiei naţionale cu cea europeană, în primul rând cu *Convenţia Consiliului Europei privind criminalitatea informatică*, unde falsificarea informatică este prevăzută în Titlul 2 (Infracţiuni informatice), la articolul 7: *„introducerea, alterarea, ştergerea sau suprimarea intenţionată şi fără drept a datelor informatice, din care să rezulte date*

[47] "The saddest aspect of life right now is that science gathers knowlegde faster than society gathers wisdom."
[48] Biochimist şi autor american, născut în Rusia.

neautentice, cu intenţia ca acestea să fie luate în considerare sau utilizate în scopuri legale ca şi cum ar fi autentice, chiar dacă sunt sau nu sunt în mod direct lizibile şi inteligibile", răspunderea penală putând fi condiţionată de existenţa unei intenţii frauduloase sau a unei alte intenţii delictuale; cu Decizia-cadru 2001/413 JAI privind combaterea fraudei şi a falsificării mijloacelor de probă, altele decât numeralul; Directiva 2013/40/UE a Parlamentului European şi a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice şi de înlocuire a Deciziei-cadru 2005/JAI a Consiliului.

Codul penal român definește frauda informatică la art. 249 după cum urmează: *„Introducerea, modificarea sau ştergerea de date informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane, se pedepseşte cu închisoarea de la 2 la 7 ani."*

Potrivit definiţiei prezentate, frauda informatică constă în acţiunile de introducere, modificare sau ştergere de date informatice, prin restricţionarea accesului la aceste date sau prin împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul.

Definiţia a fost preluată de legiuitorul român din *Convenţia Consiliului Europei privind criminalitatea informatică*, unde frauda informatică este prevăzută în Titlul 2 (Infracţiuni informatice), la articolul 8[49]: „*fapta intenţionată şi fără drept de a cauza un prejudiciu patrimonial unei alte persoane:*

a) prin orice introducere, alterare, ştergere sau suprimare a datelor informatice;

[49] Art. 8 Computer-related fraud : "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a) any input, alteration, deletion or suppression of computer data;
b) any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person."

b) prin orice formă care aduce atingere funcţionării unui sistem informatic, cu intenţia frauduloasă sau delictuală de a obţine fără drept un beneficiu economic pentru el însuşi sau pentru altă persoană".

Codul penal român defineşte infracţiunea de acces ilegal la un sistem informatic în cadrul articolului 360 după cum urmează:

„(1) Accesul, fără drept, la un sistem informatic se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă.

(2) Fapta prevăzută în alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoarea de la 6 luni la 5 ani.

(3) Dacă fapta prevăzută în alin. (1) a fost săvârşită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricţionat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea de la 2 la 7 ani".

Noul Cod penal vine cu modificări în raport cu vechiul Cod penal, infracţiunea analizată fiind incriminată de cel nou, preluată din Legea nr. 161/2013, într-o formă simplă şi două forme agravante.

Ca şi în cazul celorlalte infracţiuni din cuprinsul tezei, legiuitorul român a ţinut cont de Dispoziţiile Convenţiei Europene privind criminalitatea informatică.

În *Convenţia Consiliului Europei privind criminalitatea informatică*[50], accesarea[51] ilegală este prevăzută în Titlul 1 (Infracţiuni împotriva confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice), la articolul 2, fiind considerată ca infracţiune: *„accesarea intenţionată şi fără drept a ansamblului ori a unei părţi a unui sistem informatic"* - existenţa infracţiunii putând fi condiţionată de „violarea măsurilor de securitate" sau de „intenţia de a obţine date informatice ori cu altă intenţie delictuală" sau de „legătura dintre încălcarea respectivă şi un sistem informatic conectat la alt sistem informatic".

Codul penal român defineşte infracţiunea de interceptarea ilegală a unei transmisii de date informatice la art. 361 după cum urmează: *(1) Interceptarea,*

[50] Din 23 noiembrie 2001 (Budapesta) – publicată în Monitorul Oficial al României, Partea I, nr. 343 din 20.04.2004
[51] Nu sunt specificate mijloacele de comunicare. În acest sens, luăm în considerare toate mijloacele de intrare într-un sistem informatic, atacurile în reţeaua Internet, precum şi accesul ilegal la reţelele fără fir.

fără drept, a unei transmisii de date informatice care nu este publică şi care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic constituie infracţiune şi se pedepseşte cu închisoare de la unu la 5 ani. (2) Cu aceeaşi pedeapsă se sancţionează şi interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic, ce conţine date informatice care nu sunt publice.

Din analiza art. 361 C. pen, rezultă că putem avea un nou gen de infracțiune asemănătoare ca formă infracţiunii de spionaj. Interceptarea, fără drept, a unei transmisii de date informatice care nu este publică şi care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic reprezintă infracţiune. De asemenea, interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic, ce conţine date informatice care nu sunt publice.

Săvârşirea infracţiunii prevăzute de art. 361 reclamă cunoştinţe de specialitate în domeniu, deoarece este nevoie de înţelegerea modului de organizare şi transmitere a datelor.

Neexistând în vechiul Cod penal, infracţiunea incidentă are drept sursă *Convenţia Consiliului Europei privind criminalitatea informatică*[52], unde aceasta este prevăzută în Titlul 1 (Infracţiuni împotriva confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice), la articolul 3: *„interceptarea intenţionată şi fără drept, efectuată prin mijloace tehnice, a transmisiilor de date informatice care nu sunt publice, destinate, provenite sau aflate în interiorul unui sistem informatic, inclusiv a emisiilor electromagnetice provenind de la un sistem informatic care transportă asemenea date”*, existenţa infracţiunii putând fi condiţionată de „comiterea încălcării respective cu intenţie delictuală” sau de „legătura dintre încălcarea respectivă şi un sistem informatic conectat la alt sistem informatic”.

Codul penal român defineşte infracţiunea de alterare a integrităţii datelor informatice în cadrul articolului 362 după cum urmează: *„Fapta de a modifica,*

[52] Din 23 noiembrie 2001 (Budapesta) – publicată în Monitorul Oficial al României, Partea I, nr. 343 din 20.04.2004

şterge sau deteriora date informatice ori de a restricţiona accesul la aceste date, fără drept, se pedepseşte cu închisoarea de la unu la 5 ani."

Legiuitorul român defineşte alterarea integrităţii datelor informatice ca fiind un şir de acţiuni, de a modifica, şterge sau deteriora sau de a restricţiona accesul la aceste date, fără drept. În vechiul Cod penal, infracţiunea era inexistentă, legiuitorul armonizând prevederile cu cele incluse în *Convenţia Consiliului Europei privind criminalitatea informatică*, unde fapta de alterare a integrităţii datelor informatice este prevăzută în Titlul 1 (Infracţiuni împotriva confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice), la articolul 4, fiind considerată ca infracţiune: „*fapta comisă intenționat şi fără drept de a distruge, şterge, deteriora, modifica sau elimina date informatice",* existenţa infracţiunii putând fi condiţionată de producerea unor rezultate grave.

Codul penal român definește infracţiunea de perturbare a funcţionării unui sistem informatic în cadrul articolului 363 după cum urmează: *„Fapta de a perturba grav, fără drept, funcţionarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice sau prin restricţionarea accesului la date informatice, se pedepseşte cu închisoarea de la 2 la 7 ani."*

Funcţionarea în condiții optime a sistemelor informatice reprezintă o condiție sine-qua-non a existenței noastre. Perturbarea prin orice mijloace are repercusiuni grave asupra mediului în care trăim, asupra vieţii înseşi.

Legiuitorul român a realizat o armonizare a legislaţiei naţionale cu cea europeană şi în cazul acestei infracţiuni, în primul rând cu *Convenţia Consiliului Europei privind criminalitatea informatică*, afectarea integrităţii sistemului este prevăzută în Titlul 1 (Infracţiuni împotriva confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice), la articolul 5, fiind considerată ca infracţiune: *„afectare gravă, intenţionată şi fără drept a funcţionării unui sistem informatic, prin introducerea, transmiterea, periclitarea, ştergerea, deteriorarea, alterarea sau suprimarea datelor informatice".*

CAPITOLUL IV
STUDIUL INSTRUMENTELOR JURIDICE INTERNAŢIONALE ŞI A CELOR APLICATE ÎN UNIUNEA EUROPEANĂ

Spaţiul cibernetic este unul deschis, oferă foarte multe provocări şi are ca trăsătură definitorie lipsa frontierelor, nefiind necesar portul unui act de identitate/paşaport informatic. În cea de-a doua jumătate a anului 2017[53], s-au înregistrat peste trei miliarde şi jumătate de utilizatori la nivel global, repartizaţi, astfel: 49,7% în Asia; 17 ,0 % în Europa; 8,2 % în America de Nord; 10,4% în America Latină şi Caraibe; 10,0 % în Africa; 3,8% în Orientul Mijlociu şi 0,7 % în Oceania/Australia. Cifrele sunt îngrijorătoare dacă ne raportăm la rata crescândă a criminalităţii organizate. Unele voci au explicat că cifrele mari nu sunt altceva decât o strategie de marketing pentru a speria marile organizaţii să-şi achiziţioneze softuri performante. Astfel, acestea reuşesc să cheltuiască mult mai mulţi bani pe tehnologie securizată decât cheltuiesc infractorii pentru săvârşirea infracţiunilor informatice.

Lupta împotriva criminalităţii informatice este una timpurie, încă de la primele semne ale apariţiei acesteia. Părintele cunoştinţelor legate de criminalitatea informatică este considerat a fi Donn B. Parker[54] din SUA care a fost implicat în cercetarea criminalităţii şi securităţii informatice la începutul anilor 1970. Alţi teoreticieni ai fenomenului pe continentul american au fost August Bequai şi Jay Bloombecker. Activitatea de documentare referitoare la criminalitatea informatică nu fost singulară pe continentul american. În Europa, s-au remarcat Ulrich Sieber[55], recunoscut drept academician în cadrul Universităţii din Freiburg şi H. W. K. Kaspersen, academician şi „părintele" Convenţiei Consiliului Europei

[53] http://www.internetworldstats.com/stats.htm, consultat la data de 31.12.2017, ora 20:02.
[54] A elaborat manualul adresat forţelor de aplicare a legii în SUA *"Computer Crime – Criminal Justice Resource Manual"* (1979).
[55] A sprijinit multe organizaţii internaţionale, precum OECD în 1983 şi Naţiunile Unite.

privind criminalitatea informatică, prin iniţiativa sa din 1997. Pe continentul australian, K. E. Brown, ofiţer de poliţie la Melbourne s-a implicat activ în lupta împotriva criminalităţii informatice.

Iniţiativele cercetătorilor menţionaţi nu au rămas fără însemnătate, prinzând glas în cadrul unor organizaţii internaţionale sau regionale, unele fiind puncte de plecare şi sprijin pentru statele lumii în lupta împotriva criminalităţii organizate.

Capitolul al IV-lea este dedicat instrumentelor elaborate de către Organizaţia Naţiunilor Unite, de instituţiile specializate ale sale, precum şi a celor elaborate de către Uniunea Europeană.

Unul dintre cele mai importante documente adoptate la nivel european în ceea ce priveşte securitatea cibernetică îl constituie Directiva (UE) 2016/1148 a Parlamentului European şi a Consiliului din 6 iulie 2016 *privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.* Aceasta vine cu un set de măsuri în vederea asigurării unui nivel comun de securitate a reţelelor şi sistemelor informatice la nivel european, în urma creşterii incidentelor de securitate. Statele membre au trebuit să transpună şi să adopte în legislaţia naţională acte normative până la data de 9 mai 2018. Actul normativ reglementează cadrul de cooperare la nivel naţional şi de participare la cel internaţional în ceea ce priveşte asigurarea securităţii reţelelor şi sistemelor informatice, va stabili autorităţile cu competenţe şi responsabilităţi, punctul unic de contact la nivel naţional de a echipei de răspuns la incidente de securitate informatică, va stabili cerinţele de securitate şi de notificare pentru operatorii de servicii esenţiale şi furnizorii de servicii digitale.

CAPITOLUL V
STRUCTURI ŞI ORGANIZAŢII INTERNAŢIONALE ŞI REGIONALE CU PREOCUPĂRI ÎN MATERIA PREVENIRII ŞI COMBATERII CRIMINALITĂŢII INFORMATICE

Deşi fenomenul criminalităţii informatice pare unul nou, acesta a stat la baza a numeroase discuţii, dezbateri, conferinţe de-a lungul secolului trecut. Noutatea rezidă din amploarea şi rapiditatea cu care tehnologia, respectiv internetul avansează. Într-un secol dominat de termeni precum „a loga", „mouse" sau „click", organele şi organizaţiile internaţionale trebuie să fie cu un pas înaintea noilor apariţii tehnologice, să adopte o practică unitară în lupta împotriva criminalităţii informatice. Având în vedere complexitatea fenomenului, putem vorbi de un „caracter transfrontalier al infracţiunilor informatice"[56]. În general, autorii infracţiunilor informatice nu acţionează la nivel naţional, în ţările din care fac parte, ci la nivel altor state, legând chiar continente, sperând astfel că nu vor putea fi depistaţi. Globalizarea activităţii infracţionale şi anonimatul cu care infractorii speră că pot trece „graniţele informatice" este o problemă reală, cu un potenţial ridicat de a afecta fiecare ţară, ofiţer de poliţie, cetăţean[57].

Securitatea europeană reprezintă o condiţie sine qua non de existenţă a Uniunii Europene, dar şi a celorlalte state ale lumii. Pentru realizarea acesteia, statele europene trebuie să conlucreze în vederea asigurării unui climat optim de existenţă, prin întărirea graniţelor externe, prin combaterea criminalităţii organizate, prin realizarea şi armonizarea politicii externe a Uniunii.

---

56 Adrian Cristian Moise, *op.cit*., p. 349.

57 Michael A.Sussmann, *The critical challenges from international high-tech and computer-related crime at the millenium,* Duke Journal of Comparative&International Law, 1999, Volume 9, p.457.

În perioada 24-25 septembrie 2013 a avut loc prima Conferinţă[58] privind criminalitatea informatică organizată de Europol şi Interpol, la Haga. Este prima iniţiativă de acest gen a specialiştilor în domeniu care s-au întrunit pentru a elabora strategii pentru protejarea spaţiului cibernetic de exploatarea infractorilor. Acestea au vizat: aducerea împreună a unităţilor de criminalitate informatică pentru a îmbunătăţi relaţiile existente, schimbul de cunoştinţe, experienţa şi expertiza a structurilor de aplicare a legii cu partenerii din sectorul privat, precum şi identificarea de noi iniţiative care să depăşească provocările viitoare pe care spaţiul cibernetic le scoate în cale. Domnul Noboru Nakatani, director executiv în cadrul Interpol a întărit ideea[59] potrivit căreia criminalitatea informatică reprezintă o criminalitate transnaţională care cere soluţii globale, bazate pe valori universale. Nicio ţară, nicio organizaţie internaţională nu va putea rezolva problema pe cont propriu, ci numai o alianţă globală care să lupte continuu împotriva criminalităţii informatice. Interpolul îşi doreşte să fie un catalizator puternic în această alianţă, împreună cu Centrul european pentru criminalitate informatică, punând accentul asupra intersecţiei dintre infracţionalitate şi tehnologie, într-o lume care devine din ce în ce mai mult interconectată.

În cadrul celei de-a 43-a ediţie a *Conferinţei regionale europene a Interpolului*, desfăşurată la Bucureşti în perioada, 19 – 21 mai 2015, participanţii la întâlnire au susţinut ca lupta împotriva criminalităţii informatice să se facă printr-un schimb continuu de informaţii, inclusiv prin anchete comune, dar nu în ultimul rând, prin utilizarea mijloacelor pe care Interpol le pune la dispoziţie.

În perioada 4 – 7 iulie 2017[60], a avut loc la Singapore Congresul mondial al Interpol. Cu această ocazie, președintele Meng Hongwei a subliniat importanța colaborării internaționale între toate sectoarele în mai multe domenii-cheie pentru a

[58] În cadrul acesteia au participat peste 250 de participanţi din 42 de ţări. Activitatea se va desfăşura anual, alternând între Haga şi Singapore. Începând cu 2014 funcţionează la Singapore un centru care coordonează lupta împotriva criminalităţii informatice. Acesta se axează asupra a trei laturi: infracţiunile on-line săvârşite de grupuri de crimă organizată, aducătoare de profituri uriaşe; infracţiunile care produc mult rău victimelor, precum exploatarea sexuală a copiilor; atacurile îndreptate asupra infrastructurilor informatice din Europa.

[59] http://www.interpol.int/News-and-media/News-media-releases/2013/N20130925, consultat la data de 2 ianuarie 2016, ora 17:48.

[60] https://www.interpol.int/News-and-media/News/2017/N2017-087, site consultat la data de 6 ianuarie 2018, ora 22.22.

dezvolta un răspuns global la infracţionalitatea sprijinită de tehnologie: schimbul de informații, intelligence, conștientizarea și formarea publicului.

„În era globalizării”, Uniunea Europeană trebuie să sprijine statele membre şi să facă faţă nenumăratelor provocări privind securitatea şi libertatea cetăţenilor, provocări care urmează să primească răspunsuri bazate pe o cooperare poliţienească eficientă, profesionalism şi responsabilitate din partea UE.

CAPITOLUL VI
MĂSURI DE PREVENIRE ŞI COMBATERE A CRIMINALITĂŢII INFORMATICE ÎN DREPTUL COMPARAT

Dacă se poate reproşa ceva statelor lumii implicate în combaterea criminalităţii informatice e nearmonizarea legislativă, denumirile variate sub care există infracţiunile informatice, adoptarea unor măsuri care au apărut după ce infracţionalitatea informatică a prins contur. În acest capitol, voi prezenta secvenţial elemente din legislaţia celor şase continente: America de Nord, America de Sud, Africa, Asia, Australia şi Europa. Analiza pe care am făcut-o în cadrul acestui capitol reliefează modul cum Convenţia Consiliului Europei privind criminalitatea informatică a fost transpusă în legislaţiile naţionale, dar şi măsurile interne pe care statele lumii le-au adoptat pentru minimalizarea efectelor infracţionalităţii informatice.

CAPITOLUL VII
CONCLUZII ŞI PROPUNERI DE LEGE FERENDA PRIVIND PERFECŢIONAREA ACTIVITĂŢII DE PREVENIRE ŞI COMBATERE ÎN PLAN INTERN ŞI INTERNAŢIONAL A CRIMINALITĂŢII INFORMATICE

Moto: „Un calculator în fiecare casă"

(Bill Gates[61])

Aşa cum am precizat în capitolele anterioare ale acestei teze, literatura română nu beneficiază de studii vaste în domeniu criminalităţii informatice. Dar, specialiştii în domeniul de referinţă nu au rămas indiferenţi la amploarea pe care fenomenul a luat-o şi au întreprins măsuri rapide în vederea armonizării legislaţiei naţionale cu cea internaţională în vederea combaterii fenomenului.

Dreptul la internet este sau ar trebui să fie perceput şi tratat ca unul din drepturile fundamentale ale omului secolului XXI, reuşind să se impună prin întreaga sa evoluţie în toate compartimentele societăţii, pentru tot cetăţenii săi, fără nicio deosebire, rămâne un subiect tabu faţă de legiuitorul român care nu a reuşit să-l codifice.

În România, tipologia infracţiunilor informatice nu este atât de vastă, lucru care nu face decât să bucure autorităţile de aplicare a legii. Criminalitatea informatică a prins contur târziu, abia în secolul al XXI-lea, cetăţenii români săvârşind mai mult infracţiuni pe teritoriul altor state decât pe teritoriul naţional. Fenomenul este îngrijorător la nivel naţional, deoarece România s-a transformat din ţară ai cărei cetăţeni lansau atacuri cibernetice asupra altor state în ţară spre care se îndreaptă din ce în ce mai multe ameninţări de natură cibernetică.

Trebuie remarcat faptul că metodele utilizate de infractorii informatici sunt

[61] Visul său din 1977 – "A computer in every home". Moto-ul a fost ales pornind de la considerentul că dacă în fiecare care casa vom avea cel puţin un calculator, ne vom confrunta cu diverse forme ale criminalităţii informatice, din ce în ce mai numeroase şi sofisticate.

din ce în ce mai variate, acest lucru depinzând de dezvoltarea tehnologică fără precedent. Organele abilitate ale statului trebuie să se implice mai mult în combaterea acestor fapte. Deşi zilnic suntem avertizaţi prin intermediul mass-media de importanţa păstrării parolelor, dar naivitatea face ca din ce în ce mai mulţi oameni să devină victime. Ceea ce este esenţialmente necesar este o campanie de educaţie computaţională pentru a conştientiza la ce ne expunem zilnic: contactul cu noii viruşi informatici şi solicitările unor informaţii personale sau financiare atunci când efectuăm plăti on-line. Cu fiecare pas pe care îl facem, suntem tot mai aproape de un război cibernetic. Consider ca primă măsură, extrem de importantă în lupta împotriva criminalităţii informatice conştientizarea maselor cu privire la ameninţările cibernetice, lansate de diverse entităţi la nivel global care pot afecta oricând securitatea naţională[62].

Analiza fenomenului criminalităţii informatice la nivel naţional şi internaţional, sub toate formele de manifestare, de la stadiul primitiv (apariţia calculatorului) şi până la cel mai avansat stadiu (transformarea calculatorului într-o armă de temut) a scos în evidenţă noi riscuri şi ameninţări la care societatea se expune, dar şi noi direcţii către care autorităţile de aplicare a legii trebuie să se îndrepte. Neacordarea unei atenţii deosebite din partea organelor competente asupra riscurilor şi direcţiilor menţionate înseamnă punerea în pericol a securităţii globale.

Deşi criminalitatea informatică a apărut târziu pe scena mondială, prin tipologia infracţiunilor care o caracterizează, putem spune cu uşurinţă că prezenţa ei s-a făcut resimţită încă din cele mai vechi timpuri. Prevenirea şi combaterea criminalităţii informatice la nivel global nu reprezintă exclusiv o problemă a statelor membre ale acesteia pentru azi, ci pentru viitor. Generaţiile care se formează acum vor fi familiarizate pe deplin cu tehnologiile informaţionale, care le vor permite explorarea şi actualizarea lor permanentă. Uniunea Europeană se află la răscrucea infracţiunilor informatice între cele patru continente: american, asiatic,

[62] Acestea au fost incluse în cadrul Strategiei Naţionale de Apărare a Ţării pentru perioada 2015 – 2019, O Românie puternică în Europa şi în lume.

african şi mult mai îndepărtat, australian. Acest lucru o determină să accelereze pasul în lupta cu criminalitatea informatică, atât la nivel legislativ, cât şi la nivel tehnologic, prin găsirea unui echilibru între cele două nivele. Autorităţile de aplicare a legii trebuie să fie bine pregătite profesional, dar şi practic, pentru că, de regulă, infractorii utilizează sisteme ieftine dar care produc pagube uriaşe. Infracţiunile informatice nu prezintă nici un element constant în alcătuirea lor, ci de fiecare dată primează elementul de noutate. Nu aceasta şochează, ci modul în care tehnologia avansează: extrem de rapid, fără a conserva vreun element vechi. Statele lumii trebuie să conlucreze în vederea elaborării şi adoptării unei politici globale de securitate IT.

Astăzi, „criminalitatea de vitrină" lasă loc „criminalităţii de interior", mult mai sofisticată, ale cărei efecte se resimt din ce în ce mai puternic. Criminalitatea informatică nu produce efecte hic et nunc, ci acestea se resimt în timp. Să ne fie teamă de o experienţă digitală Hiroshima sau de un Cernobâl digital? Este important să ne analizăm situaţia actuală, posibilele ameninţări viitoare şi vulnerabilităţile pentru a dezbate dogmele de securitate în vederea elaborării noilor strategii şi deschiderii căilor de străbătut în domeniul cercetării.

După parcurgerea literaturii de specialitate în domeniul de referinţă pot afirma, fără a greşi, că infracţionalitatea informatică a ajuns să fie cea mai răspândită formă a criminalităţii organizate, Terra incognita a devenit Terra supracognita. În prezent, cercetătorii fenomenului au evidenţiat că secolul XXI se luptă cu o nouă formă a terorismului, cel informatic, mult mai puternică. Ţinând cont de tipologia terorismului, pot afirma că generaţia noastră trebuie să facă faţă unui terorism postmodern, ale cărui forme sunt mult mai complexe, dificil de monitorizat faţă de cel tradiţional. Făcând o paralelă cu postmodernismul, pot identifica trăsături ale criminalităţii informatice: amestecul de naivitate a utilizatorilor IT, valorificarea naivităţii, estomparea graniţelor tradiţionale ale infracţiunilor comune, utilizarea limbajului codificat al infractorilor. Vechile organizaţii teroriste cu un nucleu bine închegat şi cu responsabilităţi clar stabilite lasă loc terorismului postmodern.

Cu toate măsurile pe care le vom adopta, în plan legislativ, educativ, organizatoric, fenomenul nu poate fi oprit, ci doar controlat pentru a nu înregistrat un trend ascendent şi rapid faţă de capacităţile autorităţilor de aplicare a legii.

Pentru a dezvolta o strategie de luptă împotriva criminalităţii informatice trebuie să înţelegem atacatorii cibernetici, să cunoaştem interesele acestora, să estimăm pagubele pe care infracţiunile informatice le produc, dar mai ales să evaluăm măsurile legislative existente la momentul actual, la nivel global.

BIBLIOGRAFIE

I. LEGISLAŢIE

a) ACTE NORMATIVE NAŢIONALE

1. *Constituţia României,* modificată şi completată prin Legea de revizuire a Constituţiei României nr. 429/2003;
2. *Legea 255/2013 pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedura penală şi pentru modificarea şi completarea unor acte normative care cuprind dispoziţii procesual penale;*
3. *Legea 187/2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal*;
4. *Legea nr.1/2011 educaţiei naţionale;*
5. *Legea nr. 135/2010 privind Codul de procedură penală;*
6. *Legea nr. 286/2009 privind Codul penal;*
7. *Legea nr. 301/2007 pentru modificarea Legii nr. 196/2003 privind prevenirea şi combaterea pornografiei*;
8. *Legea nr. 64/2004 privind ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică adoptată la Budapesta la 23.11.2001*;
9. *Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice*;
10. *Legea nr. 496/2004 pentru modificarea şi completarea Legii nr. 196/2003 privind prevenirea şi combaterea pornografiei;*
11. *Legea nr. 302/2004 privind cooperarea judiciară internaţională în materie penală, cu modificările şi completările aduse prin Legea nr. 224/2006, Ordonanţa de Urgenţă nr. 103/2006 privind unele măsuri pentru facilitarea cooperării poliţieneşti internaţionale şi Legea nr. 222/2008;*
12. *Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de*

afaceri, prevenirea şi sancţionarea corupţiei;

13. *Legea nr. 196/2003 privind prevenirea şi combaterea pornografiei, cu modificările aduse prin Legea nr. 496/2004 şi Legea nr. 301/2007;*
14. *Legea nr. 39/2003 privind prevenirea şi combaterea criminalităţii organizate*;
15. *Legea nr. 365/2002 privind comerţul electronic*;
16. *Legea nr. 678/2001 privind prevenirea şi combaterea traficului de persoane*;
17. *Legea nr. 677/2001 privind protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date*;
18. *Legea nr. 92/1996 privind organizarea şi funcţionarea Serviciului de Telecomunicaţii Speciale*;
19. *Legea nr. 51/1991 privind siguranţa naţională a României*;
20. *Hotărârea Guvernului nr. 779/2015 pentru aprobarea Strategiei naţionale de ordine şi siguranţă publică 2015 – 2020;*
21. *Hotărârea Guvernului nr. 271/2013 privind aprobarea Strategiei de Securitate Cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului Naţional de Securitate Cibernetică*;
22. *Regulamentul nr. 6 din 11 octombrie 2006 al BNR privind emiterea şi utilizarea instrumentelor de plată electronică şi relaţiile dintre participanţii la tranzacţiile cu aceste instrumente;*
23. *Ordinul ministrului afacerilor interne nr. 132 din 24 iunie 2011 privind activităţile Ministerului Afacerilor Interne sub egida CEPOL.*

b) ACTE NORMATIVE EUROPENE

1. *German Criminal Code;*
2. *Code pénal de la République Française ;*
3. *Police and Justice Act 2006;*
4. *The Computer Misuse and Cybercrime Act 2003;*
5. *Criminal Code of the Republic of Lithuania.* Official Gazette. 2000, No. 89-

2741;

6. *Criminal Code of the Republic of Lithuania.* Official Gazette. 1961, No. 18-147;
7. *Convenţia Consiliului Europei privind criminalitatea informatică;*
8. *Data Protection Act 1998*;
9. *Legge 23 dicembre 1993 n. 547 - Modificazioni ed integrazioni alle norme det codice penale e del codice di procedura penale in tema di criminalita informatica*;
10. *Recomandarea nr. R(87)15 privind reglementarea utilizării datelor personale în munca de poliţie;*
11. *Recomandarea nr. R(95)13 privind problemele legale de dreptul procedural penal care au legătură cu tehnologia informaţiei;*
12. *Recomandarea nr. R(95)4 privind protecţia datelor personale în domeniul serviciilor de telecomunicaţii cu referire la serviciile de telefonie în mod deosebit;*
13. *Recomandarea nr. R(81)12 privind criminalitatea economică;*
14. *Recomandarea nr. R(85)10 privind normele de aplicare a Convenţiei Europene de Asistenţă Mutuală în Materie Infracţională, cu referire la comisiile rogatorii privind interceptarea comunicaţiilor;*
15. *Recomandarea nr. R(89)9 asupra criminalităţii în legătură cu utilizarea computerului;*
16. *Recomandarea nr. R(88)2 privind măsurile de combatere a pirateriei în domeniul drepturilor de autor şi al drepturilor conexe;*
17. *Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului;*
18. *Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului din 14 septembrie 2016 privind Poliția de frontieră și garda de coastă la*

nivel european şi de modificare a Regulamentului (UE) 2016/399 al Parlamentului European şi al Consiliului şi de abrogare a Regulamentului (CE) nr. 863/2007 al Parlamentului European şi al Consiliului, a Regulamentului (CE) nr. 2007/2004 al Consiliului şi a Deciziei 2005/267/CE a Consiliului;

19. *Regulamentul (UE) 2015/2219 al Parlamentului European şi al Consiliului din 25 noiembrie 2015privind Agenţia Uniunii Europene pentru Formare în Materie de Aplicare a Legii (CEPOL) şi de înlocuire şi de abrogare a Deciziei 2005/681/JAI a Consiliului;*
20. *Regulation of Investigatory Powers Act 2000*;
21. *Tratatul de la Lisabona de modificare a Tratatului privind Uniunea Europeană şi a Tratatului de instituire a Comunităţii Europene, semnat la Lisabona, la data de 13 decembrie 2007.*

c) ACTE NORMATIVE DIN DREPTUL COMPARAT

1. *Anti-Cyber Crime Law,* 8 Rabi1, 1428 / 26 March 2007;
2. Codul penal al Federaţiei Ruse;
3. Codul penal al Republicii Moldova;
4. *Swiss Criminal Code;*
5. *Draft African Union Convention on The Establishment of a Legal Framework Conducive to Cyber Security in Africa*;
6. *United Nations Convention against Transnational Organised Crime and its Protocoals.*

II. TRATATE, CURSURI, MONOGRAFII

1. Gheorghe ALECU, Alexei BARBĂNEAGRĂ, *Reglementarea penală şi investigarea criminalistică a infracţiunilor din domeniul informatic,* Ed. Pinguin Book, Bucureşti, 2006 ;
2. Tudor AMZA, Cosmin – Petronel AMZA, *Criminalitatea informatică,* Editura Lumina Lex, Bucureşti, 2003;

3. Ionuţ – Andrei BARBU, *Introducere în criminalitatea informatică*, Editura Sitech, Craiova, 2014;
4. Alexandru BOROI, *Drept penal. Partea generală*, Ediţia 2, Editura C. H. Beck, 2014, Bucureşti;
5. Costică VOICU, Alexandru BOROI, *Drept penal al afacerilor*, Ed. C. H. Beck, Bucureşti, 2008;
6. Mihai Petru CRAIOVAN, *Introducere în psihologia resurselor umane*, Editura Universitară, Bucureşti, 2006;
7. Vasile CREŢU, *Drept internaţional public*, Editura Fundaţiei România de Mâine, Bucureşti, 2008;
8. Michael CROSS, *Scene of the Cybercrime*, ed. a II-a, Editura Syngress Publishing Inc., Rockland, Massachusetts, 2008;
9. Damian MICLEA, *Cunoaşterea crimei organizate*, Editura Pygmalion, Ploieşti, 2001;
10. Ioan DASCĂLU, Ştefan PRUNĂ, Cristian-Eduard ŞTEFAN, Marin-Claudiu ŢUPULAN, Laurenţiu GIUREA; *Organizaţia criminală a drogurilor*, Editura Sitech, Craiova, 2008;
11. Maxim DOBRINOIU, *Infracţiuni în domeniul informatic*, Editura C. H. Beck, 2006, Bucureşti;
12. Vasile DOBRINOIU, Norel NEAGU, *Drept penal. Partea specială*, Editura Universul Juridic, 2014, Bucureşti;
13. Augustin FUEREA, *Manualul Uniunii Europene*, Editura Actami, 2001, Bucureşti;
14. Daniela GĂRĂIMAN, *Dreptul şi informatica*, Editura AU Beck, 2003, Bucureşti;
15. R. HOLLINGER, *Crime, deviance and the computer*, Dartmouth: Aledershot – Brookfield, 1997;
16. Mihai Adrian HOTCA, Maxim DOBRINOIU, *Infracţiuni prevăzute în legi speciale*, Editura C.H. Beck, 2008, Bucureşti;
17. H. Marshall JARRETT, Michael W BAILIE, *Prosecuting Computer*

Crimes; Office of Legal Education, 2010;

18. D. KIOUPI, *Criminal Law and the Internet*, Ant. N. Sakkoula Editions, 1999*;*
19. Luca IAMANDI, *Cooperarea poliţienească internaţională*, Editura Fundaţia universitară Dunărea de jos, Galaţi 2006;
20. Iosif LUCACI, Robert MARIN, *Criminalitatea informatică*, Editura Fed Prinţ S.A., 2003, Bucureşti;
21. Iosif LUCACI, Robert MARIN, *Investigarea fraudelor informatice*, Editura Ministerului de Interne, 2002, Bucureşti;
22. Mihaela MARINESCU, Marius POPA, *Mic dicţionar de termeni internaţionali intraţi în uzul limbii române,* Editura Vremea, Bucureşti, 2007;
23. Dumitru MAZILU, *Dreptul internaţional public*, Vol. II, Ediţia a V-a, Editura Lumina Lex, Bucureşti, 2010;
24. Damian MICLEA, *Cunoaşterea crimei organizate*, Editura Pygmalion, Ploieşti, 2001;
25. Damian MICLEA, *Combaterea crimei organizate*, vol. I, Editura Ministerului Administraţiei şi Internelor, Bucureşti, 2004;
26. H. MILONOPOULOU, *Criminal Justice – Special Section,* 2nd Edition, P. N. Sakkoula Editions, Athens 2006;
27. H. MILONOPOULOU, *Computers and Criminal Law*, N. Sakkoula Editions, 1991;
28. Constantin MITRACHE, *Drept penal român*, Editura Şansa, 2000, Bucureşti, p. 77;
29. Adrian CRISTEA MOISE, *Metodologia investigării criminalistice a infracţiunilor informatice*, Editura Universul Juridic, Bucureşti, 2011;
30. D. B. PARKER, *Fighting Computer Crime,* New York: Charles Scribner's Sons, 1983;
31. D. B. PARKER, *Crime by Computer*. New York: Charles Scribner's Sons, 1976;

32. Victor Valeriu PATRICIU, *Criptografia şi securitatea reţelelor de calculatoare*, Ed. Tehnică, Bucureşti, 1994;
33. C.P. PFLEEGER, *Security in Computing*, 2nd edition, Prentice – Hall, Englewood Cliffs, etc, 1997;
34. Teodor POPA, *Frauda informatică*, Ed. Universităţii din Oradea, Oradea, 2002;
35. Liviu G. POPA, *Managementul prevenirii şi combaterii criminalităţii informatice* (Teza de doctorat), Bucureşti, 2009;
36. Ştefan PRUNĂ, Cristian – Eduard ŞTEFAN, Marin – Claudiu ŢUPULAN, Laurenţiu GIUREA, Ioan – coordonator DASCĂLU, *Organizaţia criminală a drogurilor,* Editura SITECH, Craiova, 2008;
37. Ştefan PRUNĂ, Ioan-Cosmin MIHAI, *Criminalitatea informatică*, Editura SITECH, Craiova, 2009;
38. Ilie-Ştefan RĂDULESCU, *Să vorbim şi să scriem corect*, Editura Niculescu, Bucureşti, 2008;
39. Chris REED, John ANGEL, *Computer Law. The Law and the Regulation of Information Technology*, 6th Edition, Oxford University Press, 2007, New York;
40. Van REENEN, *EUROPOL – History, Towards The Regionalism of Policing: Lessons from Europe*, Prima Publishing House, London, 2003;
41. Marco ROSINI, *World Wide Warfare, Jus ad bellum and the Use of Cyber Force*, Max Planck Yearbook of United Nations Law, Volume 14, 2010;
42. Abram N SHULSKY, Gary J SCHMITT, *Războiul tăcut. Introducere în universal informaţiilor secrete*, Ed. Polirom, 2008;
43. Ion SUCEAVĂ, *Interpol la început de mileniu*, Editura Meronia, Bucureşti, 2007;
44. Cristian-Eduard ŞTEFAN, Marin-Claudiu ŢUPULAN, Constantin DRĂGHICI, Ion CHIPĂILĂ, Ligia Teodora PINTILIE, *Globalizarea traficului de copii*, Editura SITECH, Craiova, 2006;
45. Anamaria TRANCĂ, *Infracţiuni informatice*, Practică judiciară, Editura

Hamangiu, Bucureşti, 2011;
46. Anamaria TRANCĂ, Dumitru Cristian TRANCĂ, *Infracţiunile informatice în noul Cod penal*, Editura Universul Juridic, Bucureşti, 2014;
47. Vasile TRONECI, Ioan HURDUBAIE, *România în Interpol*, Editura Ministerului de Interne, Bucureşti, 1994;
48. Ioana VASIU, Lucian VASIU, *Prevenirea criminalităţii informatice*, Editura Hamangiu, Bucureşti, 2006;
49. Ioana VASIU, *Totul despre hackeri*, Editura Nemira, Bucureşti, 2001 ;
50. Ioana VASIU, *Criminalitatea informatică*, Editura Nemira, Bucureşti, 2001;
51. Ioana VASIU, Lucian VASIU, *Informatică juridică şi drept informatic*, Editura Albastră, Cluj-Napoca, 2002, p. 166;
52. Ioana VASIU, Lucian VASIU, *Afaceri electronice, aspecte legale, tehnice şi manageriale,* Editura Albastra, Cluj-Napoca, 2007, p. 101F;
53. K. VLACHOPOULOU, *Electronic Crime, Library of Law Editions,* 2007;
54. M.YAR *Cybercrime and Society,* Sage Publications, 2006;
55. Pierre WEISS, *Le systeme des Nations-Unies,* Editura Nathan, Paris, 2008.

III. STUDII ŞI ALTE LUCRĂRI

A. Româneşti

1. Maxim DOBRINOIU, *Provocarea legislativă a reţelelor Wi-Fi,* Revista Intelligence, Anul VI nr. 16, iulie 2009, p.1;
2. Gândire de calitate, Educaţie de calitate, CEPOL, 2012;
3. Radu MOINESCU, *Viruşii – risc şi ameninţare asupra sistemelor informatice,* Revista Intelligence nr. 23/2012, p. 5 – 7;
4. Planul strategic instituţional al Ministerului Afacerilor Interne 2014 – 2016;
5. Carmen POSTELNICU, Sorana MARMANDIU, *Perspective teoretice asupra ameninţărilor cu incidenţă în domeniul securităţii,* Revista Intelligence nr. 23/2012, p. 44;
6. Programe şcolare, Informatică, Clasa a IX-a, Ciclul inferior al liceului, Filiera teoretică, profil real, specializările: Matematică-informatică intensiv

informatică, Filiera vocaţională, profil militar, specializarea: Matematică-informatică intensiv informatică, Bucureşti, 2009;
7. Raportul privind criminalitatea informatică, Norton Symantec, 2012;
8. Raportul OCTA pentru anul 2011;
9. Revista Română de Studii de Intelligence, Nr. 4, Bucureşti, Decembrie 2010;
10. Revista Română de Studii de Intelligence, Nr. 8, Bucureşti, Decembrie 2012;
11. Raluca SIMION, *Cybercrime and its challenges between reality and fiction. Where do we actually stand?,* Rivista di Criminologia, Vittimologia e Sicurezza – Vol. III - N. 3, Vol. IV –N. 1 – Settembre 2009-Aprile 2010;
12. Strategia Naţională de Apărare 2010;
13. Strategia Naţională de Apărare a Ţării pentru perioada 2015 – 2019;
14. Helen ŞIPOŞ, *Abordări ale activităţii de prevenire a criminalităţii în cadrul CEPOL*, Buletinul de Informare şi Documentare al Ministerului Administraţiei şi Internelor - Secretariatul General, nr. 2/2009 ;
15. Terorismul. Istoric, forme, combatere. Culegere de studii. Editura Omega, Bucureşti, 2001;
16. Unde-i lege, nu-i tocmeală!, manual de educaţie judiciară, realizat în conformitate cu noul Cod Penal intrat în vigoare la 1 februarie 2014, Direcţia Generală de Poliţie a Municipiului Bucureşti, Inspectoratul Şcolar al Municipiului Bucureşti;
17. Ioana VASIU, *Modalităţi de comitere a infracţiunilor informatice. Programe distructive,* Revista de Drept Penal, nr. 3 din 1997.

B. Străine

1. Stephen AGUILAR-MILLAN, Joan E. FOLTZ, John JACKSON, Amy OBERG, *The Globalization of Crime,* The Futurist, November-December 2008;
2. I. ANGELI, *The Convention of the Council of Europe for the Fight against Crime in Cyberspace*, Poiniko Dikaio 2001;

3. Annual Report 2012, Strengthening Police Cooperation Through Learning, CEPOL, 2013;
4. Myrna AZZOPARDI, *The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Brief Introduction on its Treatment of Jus Ad Bellum Norms*, Elsa Malta Law Review, Edition III, 2013;
5. John BAIDEN, Cybercrimes, 27 June 2011;
6. Glenn D. BAKER, *Trespassers Will be Prosecuted: Computer Crime in the 1990s*,12 COMPU1~ LJ. 61, p.62;
7. J. M. BALKIN, N. KOZLOVSKI, 2007 "Introduction". in: Balkin et al. eds., 2007. Cybercrime. Digital Cops in a Networked Environment. New York/London: New York UP, pp. 1- 10;
8. S.W. BRENNER, 2002 "Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships". North Carolina Journal of Law & Technology, 4, pp. 1- 50.
9. S.W. BRENNER, 2007 *"The Council of Europe's Convention on Cybercrime"*. In: Balkin et al. eds., 2007, *"Cybercrime. Digital Cops in a Networked Environment"*. New York/London: New York UP, pp. 207- 20;
10. S.W. BRENNER, 2008 *"Fantasy Crime: The Role of Criminal Law in Virtual Worlds"*, in the Vanderbilt Journal of Entertainment and Technology Law, 11(1), pp. 1- 97.
11. Roderic BROADHURST, Yao-Chung CHANG, *Cybercrime in Asia: trends and challenges*, Draft 5.1.2012 – Asian Handbook of Criminology;
12. I. CARR and S. K. WILLIAMS *Draft Cybercrime Convention, Criminalization and the Council of Europe (Draft) Convention on Cybercrime*, Computer Law & Security Report 2002;
13. Charter of the Commonwealth, Signed by Her Majesty Queen Elizabeth II, Head of the Commonwealth, Commonwealth Day 2013;
14. Mohamed CHAWKI, *A Critical Look at the Regulation of Cybercrime, LL.B (1998), BA (1998), LL.M (2000), DU (2003);*
15. Contributing to European Police Cooperation Through Learning, CEPOL,

2010;

16. Prabhash DALEI, Tannya BRAHME, *Cyber Crime and Cyber Law in India: An Analysis, International Journal of Humanities and Applied Sciences (IJHAS)* Vol. 2, No. 4, 2013;
17. Okonigene Robert EHIMEN; Adekanle BOLA, *Cybercrime in Nigeria*, Business Intelligence Journal - January, 2010 Vol.3 No.1;
18. EU Kids Online: Final Report, Sonia Livingstone and Leslie Haddon Coordinator;
19. Eurojust 2009, 2010, 2011 2012 Annual Reports;
20. Eurojust News, Issue No.7 – October 2012;
21. European Police Science and Research Bulletin, 2017;
22. M. GERCKE, *Understanding Cybercrime. A Guide for Developing Countries*, Draft April 2009;
23. M. D. GOODMAN, *Why the police don't care about computer crime,* 10 Harvard Journal of Law and Technology 465, Summer, 1997;
24. International Crime Threat Assessment, *Global Context of International Crime, Implications of Changing World*, Chapter I, Clinton Foundation, 2005;
25. International Journal of Computer & Organization Trends – Volume1Issue2- 2011;
26. Y. JEWKES & M. YAR, eds. 2010, *Handbook of Internet Crime*, Cullompton: Willan Publishing;
27. M. KAIAFA-GBANDI, *Criminal Law and Abuses of Information Technology*, Armen 2007;
28. K. CAMPBELL, L. A. GORDON, M.P. LOEB şi L. ZHOU, *The economic cost of publicly announced information security breaches: empirical evidence from the stock market, Journal of Computer Security* 11, 2003, p. 431-448
29. Bert-Jaap KOOPS, *Cybercrime Legislation in the Netherlands,* in: Pauline C. Reich(ed.), Cybercrime and Security, Vol. 2005/4, Dobbs Ferry, NY:

Oceana Publications;

30. Edward, K. LESTRADE, O St.J, LLB, MA, SJD, Attorney at Law Lestrade Law Associates LLC, *The Cybercrime Phenomenon and Latvian Cybercrime Law*;
31. Lisbon Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon on 20 November 2010;
32. P. J. MCFADDEN (1997), Guarding computer data. Journal of Accountancy, 184(1), 77–79;
33. Saroj MEHTA, Vikram SINGH, *A Study of Awareness about Cyberlaws in the Indian Society*, International Journal of Computing and Business Research, Volume 4 Issue 1 January 2013;
34. Gerhard O. MUELLER, *Transnational Crime: Definitions and Concepts, Transnational Organised Crime*, Review 4 (3-4), pp.13 -21;
35. National Plan to Combat Cybercrime, Australian Government Attorney General's Department;
36. National Security Council, *International Crime Threat Assessment*;
37. R. L. PARRY (2009, 9 July 2009). *North Korea "launches massive cyber attack on Seoul".* The Times;
38. Prospective Analysis on Trends in Cybercrime from 2011 to 2020;
39. J. Keziya RANI, S. Prem KUMAR; U. Ram MOHAN, C. Uma SHANKAR, *Laptop Theft Analysis for Digital Investigations*, International Journal of Computer& Organization Trends – Volume 1 Issue 2- 2011;
40. Van REENEN, *EUROPOL – History, Towards The Regionalism of Policing: Lessons from Europe*, Prima Publishing House, London, 2003;
41. Neil ROBINSON, Emma DISLEY, Dimitris POTOGLOU, Anais REDING, Deidre CULLEY, Maryse PENNY, Maarten BOTTERMAN, Gwendolyn CARPENTER; Colin BLACKMAN, Millard JEREMY, *Feasibility Study for a European Cybercrime Centre*, Final Report, February 2012;
42. B. SANDYWELL, 2010, *"On the globalisation of crime: the Internet and*

new criminality". În: Y. Jewkes & M. Yar. eds. 2010, Cullompton: Willan Publishing, pp. 38- 66;

43. Darius SAULIŪNAS, *Legislation on Cybercrime in Lithuania: Development and Legal Gaps in Comparison with The Convention on Cybercrime*, Jurisprudence 2010, 4(122), p. 203–219;
44. Stein SCHJOLBERG, *Computer-Related Offences*, A presentation at the Octopus Interface 2004 - Conference on the Challenge of Cybercrime, 15-17 September 2004, Council of Europe, Strasbourg, France;
45. Miha ŠEPEC, *Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related Frau*, International Journal of Cyber Criminology, 2012;
46. E. J. SINROD, W.P. Reilley, Cyber-Crimes: *A practical approach to the application of federal computer crime laws,* 16 Santa Clara Computer & High Technology Law Journal 177, 188, 2000;
47. Michael A. SUSSMANN, *The critical challenges from international high-tech and computer-related crime at the millenium*, Duke Journal of Comparative&International Law, Volume 9,1999;
48. Gregor URBAS, *An Overview of Cybercrime Legislation and Cases in Singapore,* Asian Law Institute, Working Paper Series No. 001, December 2008;
49. The Council of Europe 800 Million Europeans, Council of Europe: January 2012;
50. *The Cyber Index International Security Trends and Realities UNIDIR*, United Nations Institute for Disarmament Research, Geneva, Switzerland, New York and Geneva, 2013.
51. The National Strategy to Secure Cyberspace, February, 2003;
52. D THOMAS, B LOADER, *Cybercrime in the Information Age*, ediţia 2000, în *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge, pp. 6-7;
53. Training Competency Framework on Cybercrime;

54. S. David WALL, *Cybercrime: New Wine, No Bottles? in P. Davis and V. Jupp, Invisible Crimes: Their Victims and their Regulation*, London: Macmillan;
55. Michael E WHITMAN, *In defense of the realm, understanding the threats to information security,* International Journal of Information Management 24 (2004) 43–57;
56. C. C. WOOD, (1999). *Information security policies made easy*. Sausalito, CA: Baseline Software Inc.
57. 2012/2013 The South African Cyber Threat Barometer;
58. 2012 Norton Cybercrime Report.

IV. SURSE ON-LINE

1. https://ro.wikipedia.org/wiki/Jacques-Yves_Cousteau, site consultat la data de 2 ianuarie 2016, ora 12:08.
2. http://www.edteck.com/dbq/more/analyzing.htm, site consultat la data de 1 ianuarie 2016, ora 17:51.
3. https://en.wikipedia.org/wiki/Alan_Turing, site consultat la data de 1 ianuarie 2016, ora 19:30.
4. http://www.academiaromana.ro/pro_pri/pag_com01socinf_tem.htm, site consultat la data de 1 ianuarie 2016, ora 17:53.
5. http://migrantsatsea.files.wordpress.com/2011/05/octa_2011-1.pdf, site consultat la data de 1 ianuarie 2016, ora 19:34.
6. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding -cybercrime -guide.pdf, site consultat la data de 1 ianuarie 2016, ora 19:39.
7. https://www.ncjrs.gov/pdffiles1/nij/231832.pdf, site consultat la data de 1 ianuarie 2016, ora 18:00.
8. http://www.slideshare.net/socialmediadna/cybercrime-in-the-netherlands-2009, site consultat la data de 1 ianuarie 2016, ora 18:02.
9. http://www.crime-research.org/articles/Critical/, site consultat la data de 1 ianuarie 2016, ora 20:20

10. http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf, site consultat la data de 1 ianuarie 2016, ora 18:12.
11. http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech465.pdf, site consultat la data de 1 ianuarie 2016, ora 18:13.
12. http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech465.pdf, site consultat la data de 1 ianuarie 2016, ora 18:13.
13. http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf, site consultat la data de 1 ianuarie 2016, ora 18:14.
14. http://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf, site consultat la data de 1 ianuarie 2016, ora 18:22.
15. http://www.gobookee.net/get_book.php?u=aHR0cDovL3d3dy5jeWJlcmNyaW1lam91cm5hbC5jb20vSGlldGFuZW5ib29rcmV2aWV3SnVseTIwMDkucGRmCkJvb2sgUmV2aWV3IG9mIEN5YmVyY3JpbWU6IFRoZSBUcmFuc2Zvcm1hdGlvbiBvZiBDcmltZSBpbiB0aGUgLi4u., site consultat la data de 1 ianuarie 2016, ora 18:23.
16. http://www.rand.org/content/dam/rand/pubs/technical_reports/2012/RAND_TR1218.pdf., site consultat la data de 1 ianuarie 2016, ora 18:25.
17. http://link.springer.com/article/10.1007%2Fs11416-006-0015-z#page-1, site consultat la data de 1 ianuarie 2016, ora 20:30.
18. http://fas.org/irp/threat/pub45270index.html, site consultat la data de 1 ianuarie 2016, ora 21:35.
19. www.academiaromana.ro/pro_pri/doc/st_e03a.doc, site consultat la data de 1 ianuarie 2016, ora 21:36.
20. http://www.gobookee.net/get_book.php?u=aHR0cDovL3d3dy5jZXJ0Lm9yZy9hcmNoaXZlL3BkZi9jeWJlcmNyaW1lLWJ1c2luZXNzLnBkZgpPcmdhbml6ZWQgQ3JpbWUgYW5kIEN5YmVyIC1DcmltZTogSW1wbGljYXRpb25zIGZvciBCdXNpbmVzcw, site consultat la data de 1 ianuarie 2016, ora 21:38.
21. http://www.baesystemsdetica.com, site consultat la data de 1 ianuarie 2016, ora 21:52.

22. http://www.gobookee.net/get_book.php?u=aHR0cDovL3d3dy5oYW55YW5nLmFjLmtyL2hvbWVfbmV3cy9INUVBRkEvMDAwMi8xMDEvMjAxMi8yOS0zLnBkZgpJbnNpZ2h0IHRvIEN5YmVyY3JpbWUgLSDtlZzslpHrjIDtlZnqtZA, site consultat la data de 1ianuarie 2016, ora 21:55.
23. http://www.witsa.org/papers/McConnell-cybercrime.pdf, site consultat la data de 2 februarie 2016, ora 12:24.
24. https://newskeeper.ro/articol?id=ECFE2D0BC4FC7E3A5FA718B14C8DA838&data=2013-03-26, site consultat la data de 02.01.2016, ora 12:36.
25. http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02, site consultat la data de 2 ianuarie 2016, ora 12:43.
26. http://www.eurojust.europa.eu/press_annual.htm, site consultat la data de 2 ianuarie 2016, ora 12:44.
27. http://www.ziare.com/articole/atacuri+informatice+banci, site consultat la data de 2 ianuarie 2016, ora 12:51.
28. http://legeaz.net/spete-penal-iccj-2006/decizia-4399-2006, site consultat la 23 decembrie 2015, ora 17.49.
29. http://legeaz.net/spete-penal-iccj-2010/decizia-4096-2010, site consultat la data de 23 decembrie 2015, ora 17.52.
30. http://www.internetworldstats.com/stats.htm, site consultat la data de 31 decembrie 2017, ora 20:02.
31. http://www.itu.int/wsis/basic/about.html, site consultat la data de 2 ianuarie 2016, ora 14:17.
32. http://www.mtic.gov.md/colaborarea_europeana_rom/, site consultat la data de 2 ianuarie 2016, ora 14:19.
33. http://eur-lex.europa.eu/Notice.do?val=307229:cs&lang=ro&list=307229:cs,&pos=1&page=1&nbl=1&pgs=10&hwords=&checktexte=checkbox&visu=#texte site consultat la data de 2 ianuarie 2016, ora 14:20.
34. http://europa.eu/legislation_summaries/information_society, site consultat la data de 2 ianuarie 2016, ora 14: 22.

35. http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=2000&nu_doc=890, site consultat la data de 2 ianuarie 2016, ora 17:40.
36. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l14560_ro.htm, site consultat la data de 2 ianuarie 2016, ora 17:40.
37. http://www.juridice.ro/37875/cybex-certificat-european-criminalitate-probe-electronice.html, site consultat la data de 2 ianuarie 2016, ora 17:43.
38. http://www.coe.int/t/dghl/standardsetting/cdpc/2Recommendations.asp, site consultat la data de 2 ianuarie 2016, ora 17: 45.
39. http://www.coe.int/, site consultat la data de 2 ianuarie 2016, ora 17:47.
40. http://www.interpol.int/News-and-media/News-media-releases/2013/N20130925, site consultat la data de 2 ianuarie 2016, ora 17:48.
41. http://www.agerpres.ro/media/index.php/international/item/230222-Forta-de-Raspuns-a-NATO-un-deceniu-in-slujba-Aliantei.html, site consultat la data de 2 ianuarie 2016, ora 17:50.
42. http://www.dsclex.ro/legislatie/2010/decembrie2010/mo2010_860.htm, site consultat la data de 2 ianuarie 2016, ora 17:51.
43. http://webnet.oecd.org/OECDACTS/Instruments/ListByCommitteeView.aspx, site consultat la data de 2 ianuarie 2016, ora 17:52.
44. http://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information.aspx, site consultat la data de 2 ianuarie 2016, ora 17:53.
45. http://aimp.apec.org/Documents/2009/TEL/TEL40-SPSG/09_tel40_spsg_015.pdf, site consultat la data de 2 ianuarie 2016, ora 17:54.
46. http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68we05.htm, site consultat la data de 2 ianuarie 2016, ora 18:22.
47. http://www.cybercrimelaw.net/Austria.html, site consultat la data de 2

ianuarie 2016, ora 18:24.

48. http://www.cybercrimelaw.net/Belgium.html, site consultat la data de 2 ianuarie 2016, ora 18:32.
49. http://www.cybercrimelaw.net/Bulgaria.html, site consultat la data de 2 ianuarie 2016, ora 18:33.
50. http://www.cybercrimelaw.net/Italy.html, site consultat la data de 1 ianuarie 2016, ora 17.42.
51. http://www.legislation.gov.uk/ukpga/1998/29/section/1, site consultat la data de 1 ianuarie 2016, ora 17:31.
52. http://lex.justice.md/index.php?action=view&view=doc&id=331268, site consultat la data de 1 ianuarie 2016, ora 17:34.
53. http://www.law.cornell.edu/uscode/text/18/1030, site consultat la data de 2 ianuarie 2016, ora 18:41.
54. https://www.Europol.europa.eu/sites/default/files/publications/en_Europolreview2011_0.pdf, site consultat la data de 3 ianuarie 2016, ora 19:17.
55. http://www.cybercrimelaw.net/South-Africa.html, site consultat la data de 3 ianuarie 2016, ora 19:24.
56. http://www.comlaw.gov.au/Details/C2013C00006/Html/Text#_Toc344981292, site consultat la data de 3 ianuarie 2016, ora 19:25.
57. http://www.legalserviceindia.com/cyber/cyber.htm, site consultat la data de 3 ianuarie 2016, ora 19:26.
58. http://www.cybercrimelaw.net/Canada.html, site consultat la data de 3 ianuarie 2016, ora 19:27.
59. http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf, site consultat la data de 3 ianuarie 2016, ora 19:30.
60. http://www.politiaromana.ro/crima_organizata.htm, site consultat la data de 12 ianuarie 2016, ora 20.55.
61. http://eur-lex.europa.eu/legal content/RO/TXT/PDF/?uri=CELEX:32016R0794&qid=1515137669814&from=EN, site consultat la data de 5 ianuarie 2018, ora 18.08.

62. https://www.interpol.int/News-and-media/News/2017/N2017-087, site consultat la data de 6 ianuarie 2018, ora 22.22.
63. www.rolii.ro, site consultat la data de 2 martie 2018, ora 12.30.
64. http://securityaffairs.co/wordpress/70046/cyber-crime/raiffeisen-cyber-heist.html, site consultat la data de 11 martie 2018, ora 22:49.