INSTITUTUL DE CERCETĂRI JURIDICE ȘI POLITICE
Al ACADEMIEI DE ȘTIINȚE A MOLDOVEI

Cu titlu de manuscris

C.Z.U. 343 6 (043.2)

DRĂGAN Alin Teodorus

FRAUDA INFORMATICĂ: ANALIZA JURIDICO-PENALĂ A INFRACȚIUNII

TEZĂ DE DOCTOR ÎN DREPT

Specialitatea: 554.01 – Drept penal și execuțional penal

Conducător științific: **CUȘNIR Valeriu,**
profesor universitar,
doctor habilitat în drept

Autor:

CHIŞINĂU, 2017

DRĂGAN Alin Teodorus, 2017

CONȚINUTUL TEZEI

ADNOTĂRI (în limbile română, engleză, rusă).....4

LISTA ABREVIERILOR.....7

INTRODUCERE.....8

1. ANALIZA DOCTRINARĂ A FRAUDEI INFORMATICE.....15

1.1 Analiza materialelor ştiinţifice publicate la tema tezei în România şi Republica Moldova....15

1.2 Analiza materialelor ştiinţifice publicate la tema tezei în străinătate.....34

1.3 Concluzii la Capitolul 1.....41

2. FENOMENUL INFRACȚIONAL ÎN DOMENIUL INFORMATIC: DEFINIRE ȘI CARACTERIZARE.....43

2.1 Preliminarii privind fenomenul infracțional în spațiul informatic.....43

2.2 Modalități tipice şi făptuitori în cazul infracțiunilor informatice.....53

2.3 Concluzii la Capitolul 2.....83

3. SEDIUL NORMATIV-PREVENTIV DE INCRIMINARE A FRAUDEI INFORMATICE: REGLEMENTĂRI INTERNAȚIONALE ȘI NAȚIONALE…….85

3.1 Cadrul juridic internațional în materia incriminării fraudei informatice.....85

3.2 Incriminarea fraudei informatice în legislația altor state.....90

3.3 Reglementări antifraudă informatică și locul incriminării în legea penală a României și Republicii Moldova.....101

3.4 Concluzii la Capitolul 3.....125

4. INFRACȚIUNEA DE FRAUDĂ INFORMATICĂ ÎN LEGA PENALĂ A ROMÂNIEI ȘI REPUBLICII MOLDOVA 127

4.1 Conţinutul legal al infracţiunii.....127

4.2 Condiţii preexistente.....133

4.3 Structura şi conţinutul juridic al infracţiunii.....145

4.4 Forme agravante ale infracțiunii…….....155

4.5 Concluzii la Capitolul 4…….....158

CONCLUZII GENERALE ŞI RECOMANDĂRI.....160

BIBLIOGRAFIE.....165

DECLARAŢIA PRIVIND ASUMAREA RĂSPUNDERII.....178

CV AL AUTORULUI.....179

ADNOTARE

Drăgan Alin Teodorus, „Frauda informatică: analiza juridico-penală a infracțiunii”.

Teză de doctor în drept. Specialitatea: 554.01 – Drept penal și execuțional penal, Chișinău, 2017

Structura tezei: text de bază 177 pagini, adnotare (în limbile: română, engleză și rusă), lista abrevierilor, introducere, patru capitole divizate în secțiuni, concluzii generale și recomandări, bibliografia din 221 titluri, declarația privind asumarea răspunderii, cv-ul autorului. Rezultatele obținute sunt publicate în șase lucrări științifice.

Cuvinte-cheie: criminalitate informatică, infracţiune informatică, internet, sistem informatic, date informatice, securitate informatică, fraudă informatică, fals informatic.

Domeniul de studiu: Drept penal; prezenta teză vizează cercetarea științifică a infracțiunii de fraudă informatică, ca manifestare a criminalității din cyberspațiu, nepierzând din vedere faptul că infracțiunile informatice reprezintă punctul de întâlnire dintre dreptul penal și informatică.

Scopul și obiectivele lucrării: scopul tezei constă în abordarea complexă a infracțiunii de fraudă informatică prin prisma reglementărilor din România, Republica Moldova, altor state, dar și a cadrului juridic internațional în domeniu. Obiective: reliefarea fenomenului infracțional în domeniul informatic și caracterizarea acestuia; conturarea și tratarea modalităților tipice de comitere și a făptuitorilor în cazul infracțiunilor informatice; analiza juridico-penală infracțiunii de fraudă informatică potrivit legislaţiei penale a României şi Republicii Moldova; formularea recomandărilor ştiinţifice pentru perfecționarea legislaţiei penale pe segmentul problematicii investigate.

Noutatea și originalitatea științifică a rezultatelor obținute derivă din abordarea multiaspectuală și de pionerat a fenomenului fraudei informatice, reprezentarea modalităților tipice de comitere a infracțiunii și a făptuitorilor, caracterizarea sediului normativ-preventiv de incriminare a fraudei informatice, inclusiv prin prisma actelor internaționale și legislației altor state și fundamentarea riguroasă a elementelor constitutive și a celor agravante ale infracţiunii de fraudă informatică. Abordarea pluridisciplinară și cercetarea ştiinţifică monografică a fenomenului de fraudă informatică, însoțită de analiza și evaluarea prevederilor art.249 N.C.pen.român şi art. 260^6 C.pen. al Republicii Moldova, a viziunilor doctrinare în materie, susținute cu cazuistică pertinentă, sesizează un veritabil suport științifico-practic pentru soluţionarea unor probleme privind aplicarea normelor în cauză, dar și întru perfecționarea cadrului normativ în domeniu.

Problema științifică de importanţă majoră soluţionată prin cercetarea realizată constă în fundamentarea științifică a elementelor şi semnelor constitutive ale infracţiunii de fraudă informatică prin prisma legii penale şi practicii judiciare, având ca efecte favorizarea încadrării juridice și aplicarea corectă a legii, precum și perfecționarea cadrului normativ de sancționare, fapt de natură să contribuie la sporirea ansamblului preventiv și de combatere a infracțiunilor în sfera tehnologiilor informaționale.

Semnificația teoretică a lucrării. Valoarea teoretica a studiului se concretizează în efortul de a descrie, inventaria, analiza, interpreta și sistematiza materia epistemologică, normativă și praxiologică în domeniul fraudei informatice, dar și a criminalității informatice în ansamblul ei. Valențele teoretice ale lucrării sunt reliefate și de caracterul pluridisciplinar (informatic și juridic) al cercetării, or fenomenul fraudei informatice se săvârșește într-un mediu virtual.

Valoarea aplicativă a lucrării se regăseşte în explicarea în detaliu a tehnicilor şi a modului de operare a infractorilor cibernetici, în raport cu modalităţile normative ale fraudei informatice, fapt care contribuie la o cunoaştere a fenomenului şi în acelaşi timp la însuşirea metodelor de prevenţie a acestui tip de infracţiuni. Lucrarea poate servi drept un veritabil ghid de îndrumare, în special pentru cei ce aplică normele de drept - ofiţeri de urmărire penală, procurori şi judecători.

Implementarea rezultatelor științifice. Rezultatele studiului pot fi utilizate în studiile științifice referitoare la criminalitatea informatică, la soluționarea cauzelor penale referitoare la infracțiunea de fraudă informatică, precum și la implementarea viitoarelor inițiative legislative în domeniul infracțiunilor informatice.

ANNOTATION

at the doctoral dissertation: „Computer-related fraud: legal and criminal analysis and investigation of the criminal offence. Author: Alin Teodorus Drăgan. Chişinău, 2017

Dissertation structure: introduction, four chapters, general conclusions and recommendations, bibliography of 221 titles, 177 pages as basic text, annotation and list of abbreviations. The results obtained are published in six scientific works.

Key words: computer-related crime, internet, computer system, computer data, computer-related fraud, search of computers, investigation of computer-related offences.

Field of study. This dissertation targets the scientific research of the computer-related fraud in the broader context of crime in the cyberspace, not overlooking the fact that computer-related offences represent the meeting point between criminal law and computer science.

Purpose and objectives of the work: the purpose of the dissertation consists in the complex study of computer-related fraud, as an integral part of computer-related crime. Objectives: knowledge of the forms which the computer-related crime may take, and also of the operational modality and techniques of cyber criminals for the purpose of preventing similar criminal offences; the study of the evolution of the regulatory act in which the offence of computer-related fraud is criminalized; the comparative analysis of criminal legislation of Romania and of the Republic of Moldova in matters of criminalization of the offence of computer-related fraud; detailed presentation of the aspects of criminal procedure law and of forensic investigation specific to computer-related offences.

Scientific novelty and originality of the results acquired. This doctoral dissertation represents one of the first complex and well-systematised scientific researches of the offence of computer-related fraud from a legal and criminal point of view.

The scientific problem of major importance solved through this research consists in the scientific substantiation of the constitutive elements and signs of computer-related fraud from the standpoint of criminal law, judicial practice and investigation particularities, which leads to correct law enforcement and perfection of the sanctioning legal framework, which will allow the enhancement of the system that prevents and combats crimes in the field of computer-related technologies.

Theoretical significance of the work. Theoretical value of the study is focused on an effort to describe, inventory, analyze, interpret and systematize the epistemological, normative and praxiological information in the field of computer-related fraud, as well as of the cybercrime as a whole. The theoretical valences of the work are shaped as well by the multidisciplinary character (informational and legal) of the study, as the phenomenon of computer related-fraud is committed in a virtual space.

The work's application value lies in the fact that the detailed analysis of methods and techniques used by cyber criminals constitutes a veritable lesson for preventing the computer-related attacks in everyday life.

Implementation of the scientific results. The results of this study may be used in scientific studies referring to computer-related crime, in solving criminal cases related to the offence of computer-related fraud, and also for the documentation of future legislative initiatives in the field of computer-related offences.

АННОТАЦИЯ

Дрэган Алин Теодорус, «Информационное мошенничество: уголовно-правовой анализ преступления». Диссертация на соискание ученной степени доктора права по специальности: 554.01 - Уголовное право и исполнительное право. Кишинэу, 2017

Структура: Настоящее исследование состоит из: аннотации (на трех языках), список сокращений, введение, четыре главы, заключение в виде общих выводов и рекомендаций и библиографии из 221 источников. Объем текста научного исследования составляет 177 страниц. Результаты исследования опубликованы в 6 научных работах.

Ключевые слова: информационные (компьютерные) преступления, интернет, информационная (компьютерная) система, компьютерная информация, информационное (компьютерное) мошенничество, ввод компьютерной информации, изменение или удаление информационных данных, взлом компьютерной системы, юридическая квалификация информационных (компьютерных) преступлений.

Область исследования – уголовное право; исследование содержит общую характеристику преступлений в сфере компьютерной информации а также предметный уголовно-правовой анализ информационного мошенничества по законодательству Республики Молдова, Румынии и других стран.

Цель и задачи исследования: является комплексное исследование информационного мошенничества, как вида преступления в сфере компьютерной информации, включая уголовно-правовые нормы инкриминирования и их подробная характеристика. Задачи исследования: анализ литературных и нормативных источников посвященных информационным (компьютерным) преступлениям, исследование форм проявления информационных (компьютерных) преступлений, изучение способов совершения преступлений в сфере компьютерной информации, рассмотрение эволюции инкриминирования общественно опасных явлений в сфере компьютерной информации, сравнительно правовой анализ уголовно-правовых норм состава информационного (компьютерного) мошенничество по законодательству Республики Молдова, Румынии, и других государств, разработка предложений по совершенствованию действующего законодательства.

Научная новизна и оригинальность состоит в том, что данная диссертация, будучи комплексным и систематизированным исследованием информационного мошенничества, как преступления в сфере компьютерной информации, в том числе уголовно-правовой характеристики состава преступления и особенностей юридической квалификации данного рода деяний, является одним из первых исследований такого рода и масштаба.

Решенная научная проблема состоит в уголовно-правовом исследовании информационного мошенничества, всестороннем анализе и оценки инкриминирующих норм и элементов состава данного вида преступления, и на этой основе разработка предложений по совершенствованию законодательства и правоприменительной практики.

Теоретическая важность исследования заключается в подробном исследовании уголовно-правовых норм информационного мошенничества по законодательству Республики Молдова и Румынии, а также других стран, на основании множества теоретических и практических источников, и комплексного подхода к оценки признаков состава преступления, во взаимосвязи с соответствующими уголовно-правовыми нормами других стран, разработки положений для совершенствования соответствующих норм.

Прикладное значение этой работы состоит в том что сформулированные автором тезисы и выводы могут быть использованы в процессе законотворчества, а также в практической деятельности правовых органов.

Внедрение научных результатов. Отдельные теоретические и практические положения диссертации нашли свое утверждение на национальных и международных научно-практических конференциях. Результаты исследования могут быть использованы в учебном процессе на юридических факультетах вузов, в правоприменительной практики, а также в качестве научной основы для дальнейших исследований.

LISTA ABREVIERILOR

alin. – alineat

art. – articol

COSC – Consiliul Operativ de Securitate Cibernetică

C. pen. – Cod penal

C. pr. pen. – Cod procedură penală

CNP – cod numeric personal

Ed. – editura

CVC – cod de verificare a cardului

lit. – litera

DOS –Denial of Service

F.B.I. - Biroul Federal de Informații

M.I. – Ministerul de Interne

MIT- Massachussets Institute of Technology

M. Of. – Monitorul Oficial

NATO – Organizația Tratatului Atlanticului de Nord

p. – pagina

nr. – numărul

RM – Republica Moldova

rom. - română

SNSC – Sistemul Național de Securitate Cibernetică

S.U.A. – Statele Unite ale Americii

U.E. – Uniunea Europeană

URL - Uniform Resource Locator

vol. - volumul

VPN - virtual private network

INTRODUCERE

Actualitatea și importanţa problemei abordate. Provocările pe care epoca modernă le pune practicianului in domeniul juridic derivă din răspândirea deja exponențială a instrumentelor tehnologice și de capacitatea lor de a influența viața persoanelor.

Cu treizeci de ani in urmă nu existau incă calculatoare personale si cu douăzeci ani in urmă utilizarea World Wide Web era incă necunoscută multora. Azi calculatoarele personale, Internet-ul si World Wide Web au devenit puncte esențiale ale vieții noastre de zi cu zi.

Societatea de azi se bazează pe tehnologii noi pentru a se administra, a oferi servicii cetatenilor și a comunica. Aproape toate sectoarele societatii contemporane sunt, deja, organizate de sisteme informatice: de la serviciul sanitar la transporturile publice, de la traficul aerian la sistemul bancar, de la sistemul telecomunicațiilor la serviciul militar. Și economia globală este consolidată de noile tehnologii care oferă mari oportunități pe piața internațională. Multinaționalele, dar și întreprinderile mici si mijlocii, își desfașoară comerțul și afacerile lor mult mai ușor, fără bariere de spațiu. Noile tehnologii permit, într-adevăr, să se investească in activități noi, să se intre pe noi piețe și să se ofere produse și servicii intr-un mod nou, mai economic si eficient.

Realitatea "virtuală" ce s-a creat a deschis, de asemenea, noi spații pentru activitatile ludice și a generat competente profesionale specifice, revoluționând categoria serviciilor tradiționale și determinând introducerea de noi categorii de servicii.

Este unul din truismele infracţiunii faptul că infractorii întotdeauna sunt în pas cu ultima tehnologie – şi adesea mai repede decât publicul larg. Inventarea telefoanelor mobile, tabletelor, pager-urilor electronice, a computerelor și internetului au fost toate îmbrăţişate cu entuziasm de către infractori, care au fost rapizi în a le folosi valoarea ca instrument ori ca sursă de bani.

Formele de infracționalitate traditionala sunt, intr-adevar, modificate si "inovate" de noile tehnologii, ele putând fi realizate numai in cadrul unor noi sisteme de comunicare digitală. Astfel, a luat naștere o nouă formă de criminalitate, și anume criminalitatea informatică.

Actualitatea demersului științific este conferită de creșterea exponențială a infracțiunilor informatice o dată cu progresul tehnologiei, fapt confirmat și de datele statistice. Astfel, în România, Centrul Național de Răspuns la Incidente de Securitate Cibernetică care este o instituție publică aflată în coordonarea Ministerului pentru Societate informațională, în raportul privind alertele de securitate cibernetică procesate în anul 2015 a oferit următoarele date îngrijorătoare: pentru perioada de referință, respectiv 01.01.2015 – 31.12.2015, și anume: s-au colectat 68.206.856 de alerte de securitate cibernetică; 26% (2.3 mil.) din totalul I.P. –urilor unice alocate spațiului cibernetic național au fost implicate în cel puțin o alertă de securitate cibernetică: 78% (53. mil) din alertele colectate și procesate vizează sisteme informatice vulnerabile, în sensul că sunt nesecurizate sau configurate

necorespunzător; 17.088 de domenii ”.ro” au fost raportate ca fiind compromise, adică 6.5% din totalul domeniilor ”.ro” active [93].

Pentru a sublinia actualitatea tezei, putem menționa un fapt foarte recent de o gravitate deosebită care se încadrează în rândul criminalității informatice, și anume faptul că rezervele de valută și aur ale Bangladeshului care se aflau în custodia Băncii Federela de Rezerve din New York, erau pe cale să aibă aceeași soartă ca și sistemul bancar al Moldovei datorită acțiunilor unor hackeri. Aceștia au încercat să scoată un miliard de dolari din conturile Băncii Centrale din Bangladesh, dar s-au ales cu o sumă considerabil mai mică, dar totuși uriașă, de 81 milioane de dolari, din cauza unei greșeli de ortografie, mai precis la a cincea solicitare a lor de a li se vira banii în contul indicat au scris în loc de ”foundation” (așa cum era corect), ”fandation”. Acest fapt a stârnit suspiciuni și a dus la anularea virării următoarelor tranșe de bani [172].

Prin prezentarea amănunțită a fenomenului criminalității informatice, a originilor acestuia, a formelor pe care le îmbracă, precum și a modurilor în care sunt săvârșite infracțiunile informatice, prezenta teză se constituie într-un instrument util atât pentru teoreticieni dar și pentru practicieni, de contracarare a acestui flagel.

Scopul şi obiectivele tezei. Scopul tezei constă în abordarea complexă a infracțiunii de fraudă informatică prin prisma reglemântărilor din România, Republica Moldova, altor state, dar şi a cadrului juridic internaţional în domeniu, normelor similare de incriminare din alte state, totul privit fiind în contextul infracţionalităţii informatice în ansamblul ei, frauda informatică constituind doar o parte a unui ansamblu infracţional.

În vederea realizării acestui scop au fost trasate următoarele **obiective:**

- analiza lucrărilor ştiinţifice din doctrina penală autohtonă şi cea străină publicate la tematica problematicii investigate;
- reliefarea fenomenului infracțional în domeniul informatic și caracterizarea acestuia;
- conturarea și tratarea modalităților tipice de comitere și a făptuitorilor în cazul infracțiunilor informatice;
- abordarea sediului normativ-preventiv de incriminare a fraudei informatice: actelor internaționale de referință; normelor de incriminare a fraudei informatice din legislația altor state; reglementărilor antifraudă informatică și incriminarea faptei în legea penală a României și Republicii Moldova;
- analiza juridico-penală a conținutului legal, condițiilor preexistente, conținutului juridic și agravantelor infracțiunii de fraudă informatică potrivit legislaţiei penale a României şi Republicii Moldova;
- reevaluarea cadrului normativ-penal privind frauda informatică din legislaţia penală a României şi a Republicii Moldova;

- formularea recomandărilor ştiinţifice pentru îmbunătăţirea legislaţiei penale pe segmentul problematicii investigate.

Metodologia cercetării științifice. Bazele metodologice ale cercetării juridico-penale a infracțiunii de fraudă informatică au fost instituite dintr-o pluralitate de metode și procedee, atât teoretice dar și practice, de cunoaștere a acestui fenomen. Astfel, pentru efectuarea acestui studiu au fost folosite o gamă de metode analitice de cercetare științifică, inclusiv: - metoda analizei comparative, constând în sesizarea elemenelor identice sau diferite în ceea ce privește reglementarea infracțiunii de fraudă informatică în legislația României, Republicii Moldova și altor state; - metoda clasificării, care a permis clasificarea infracțiunilor informatice după anumite criterii; - metoda analizei istorice, constând în trecerea în revistă a apariției și evoluției infracțiunilor informatice; - metoda analizei logice, constând în folosirea raționamentelor logice pentru sintetizarea opiniilor doctrinare ale diverșilor autori.

Noutatea și originalitatea științifică a rezultatelor obținute derivă din abordarea multiaspectuală și de pionerat a fenomenului fraudei informatice, reprezentarea modalităților tipice de comitere a infracțiunii și a făptuitorilor, caracterizarea sediului normativ-preventiv de incriminare a fraudei informatice, inclusiv prin prisma actelor internaționale și legislației altor state și fundamentarea riguroasă a elementelor constitutive și a celor agravante ale infracţiunii de fraudă informatică. Abordarea pluridisciplinară și cercetarea ştiinţifică monografică a fenomenului de fraudă informatică, însoțită de analiza și evaluarea prevederilor art.249 N.C.pen.român şi art. 260^6 C.pen. al Republicii Moldova, a viziunilor doctrinare în materie, susținute cu cazuistică pertinentă, sesizează un veritabil suport ştiinţifico-practic pentru soluţionarea unor probleme privind aplicarea normelor în cauză, dar și întru perfecționarea cadrului normativ în domeniu.

Noutatea demersului ştiinţific se concretizează şi în următoarele:

1. S-a argumentat ca fiind neîntemeiată soluţia legiuitorului moldovean de a limita cercul subiecţilor activi al fraudei informatice doar la persoanele fizice. În contextul progresului tehnico-ştiinţific, succeptibilitatea persoanelor juridice de a fi implicate în activităţi infracţionale legate de fraude informatice este una evidentă.

2. S-a fundamentat teza potrivit căreia la baza poziționării locului incriminator al fraudei informatice în legislaţiile penale stau două criterii: 1) obiectul juridic de atentare și 2) mijlocul de comitere a infracţiunii. Din noţiunea fraudei informatice, reiese în mod indubitabil că scopul final al infractorului nu este de a perturba sistemul informaţional, ci cel de a obţine anumite bunuri, beneficii sau drepturi asupra bunurilor. Prin urmare, anume aceasta este raţiunea legiuitorilor care incriminează frauda informatică ca infracţiune patrimonială. În această viziune legislativă relaţiile patrimoniale prevalează faţă de relaţiile ce condiţionează existenţa sistemului informaţional, fapt pentru care frauda informatică este incriminată în compartimentul ce se referă ocrotirea penală a patrimoniului (Cod

penal al României). Mijlocul de comitere a fraudei informatice este în măsură să perturbeze sau chiar să dăuneze în mod grav sistemul informaţional, afectându-se în acelaşi şi încrederea pe care persoanele o au în utilizarea acestora. În această abordare deja relaţiile sociale referitoare la protejarea sistemului informaţional prevalază faţă de relaţiile sociale din domeniul patrimonial, fapt pentru care infracţiunea este incriminată în acel compartiment al legii penale care se referă la protejarea relaţiilor sociale din domeniul informaticii (Cod penal al R. Moldova).

3. De *lege ferenda* propunem următoarea variantă a textului incriminator de la art. 260^6 C.pen. al Republicii Moldova:

Frauda informatică,

(1) Dobîndirea ilegală a bunurilor altei persoane, a avantajelor materiale sau de altă natură prin introducerea, modificarea sau ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic,

se pedepsesc cu amendă în mărime de la 550 la 850 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare până la 4 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 1000 la 3000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(2) Aceleaşi acţiuni săvârşite:

a) de un grup criminal organizat sau de o organizaţie criminală;

b) în proporţii mari

se pedepsesc cu închisoare de la 4 la 8 ani cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de până la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 3000 la 5000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(3) Acţiunile prevăzute la alin.(1)-(2) săvîrşite în proporţii deosebit de mari

se pedepsesc cu închisoare de la 7 la 12 ani cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de până la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 5000 la 10000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea persoanei juridice.

(4) Cauzarea de pagube materiale prin introducerea, modificarea sau ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic săvârşită în proporţii mari, dacă fapta nu este o însuşire,

se pedepsesc cu amendă în mărime de la 200 la 500 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare de până la 3 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 500 la 3000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(5) Acţiunile prevăzute la alin.(4) săvârşite în proporţii deosebit de mari,

se pedepsesc cu închisoare de la 3 la 6 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 3000 la 5000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

4. De *lege ferenda*, pentru o mai bună prevenire a fraudei informatice se propune introducerea în legislația penală a Republicii Moldova și a României a unei noi incriminări cu denumirea marginală de ***furt de identitate*** *(phishing)*, cu următoarea formulare legislativă: ***Acțiunea prin care făptuitorul obține în mod fraudulos identitatea altei persoane cu ajutorul sistemelor informatice sau de telecomunicație prin inducerea în eroare a utilizatorului sistemului informatic datorită creării unei stări de aparență menite a determina utilizatorul să furnizeze date personale în cadrul unei comunicări electronice.*** În C.pen. al României incriminarea ar urma să fie statuată în Titlul VII, Capitolul VI din Partea specială la art. 364^1, cu instituirea unei pedepse *de la 3 luni pînă la 2 ani sau cu amendă*. În C.pen. al Republicii Moldova incriminarea urmează să fie încorporată în Capitolul XI din Partea specială prin introducerea art. 260^7 și instituirea următoarei pedepse: *amendă în mărime de la 200 la 500 unităţi convenţionale sau muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau închisoare de pînă la 2 ani, cu amendă, aplicată persoanei juridice, în mărime de la 1000 la 3000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate*.

Problema ştiinţifică de importanţă majoră soluţionată prin cercetarea realizată constă în fundamentarea științifică a elementelor şi semnelor constitutive ale infracţiunii de fraudă informatică prin prisma legii penale şi practicii judiciare, având ca efecte favorizarea încadrării juridice și aplicarea corectă a legii, precum și perfecționarea cadrului normativ de sancționare, fapt de natură să contribuie la sporirea ansamblului preventiv și de combatere a infracțiunilor în sfera tehnologiilor informaționale.

Importanța teoretică a lucrării. Valoarea teoretica a studiului se concretizează în efortul de a descrie, inventaria, analiza, interpreta și sistematiza materia epistemologică, normativă și praxiologică în domeniul fraudei informatice, dar și a criminalității informatice în ansamblul ei. Totodată, în teză sunt concentrate viziunele doctrinare privind infracțiunea de fraudă informatică și stabilirea elementelor constitutive a variantei tip și agravantelor infracțiunii. Valențele teoretice ale lucrării sunt reliefate și de caracterul pluridisciplinar (informatic și juridic) al cercetării, or fenomenul fraudei informatice se săvârșește într-un mediu virtual.

Valoarea aplicativă a lucrării se regăsește în explicarea în detaliu a tehnicilor și a modului de operare a infractorilor cibernetici, în raport cu modalitățile normative ale fraudei informatice, fapt care contribuie la o cunoaștere a fenomenului și în același timp la însușirea metodelor de prevenție a acestui tip de infracțiuni. Teza oferă și soluții juridice adecvate pentru activitatea de interpretare și aplicare a normei de incriminare a fraudei informatice, prevăzute la art.249 N.C.pen.român și art. 260^6 C.pen. al Republicii Moldova. Lucrarea este utilă atât pentru teoreticienii dreptului, în special pentru instituțiile

care pregătesc cadre profesionale antrenate în combaterea acestui fenomen, dar se constituie și într-un autentic ghid de îndrumare, în special pentru practicieni ai dreptluui, cum sunt ofițerii de urmărire penală, procurorii și judecătorii, dar oferă cunoștințe utile și utilizatorului obișnuit al internetului sau al unui sistem informatic.

Aprobarea rezultatelor cercetării. Concluziile şi recomandările formulate au fost tratate în conţinutul mai multor articole ştiinţifice şi pot servi drept bază teoretico-metodologică pentru efectuarea unor cercetări ulterioare. Totodată, unele concepte, ideii, opinii ce au constituit rezultatul cercetării, au făcut obiectul unor publicaţii în formă de rapoarte și comunicări la conferințe ştiinţifice internaţionale, în speță:

- Conferința științifică internațională a doctoranzilor și tinerilor cercetători cu tema ”Tendințe contemporane în evoluția patrimoniului istoric și juridic al Rebublicii Moldova”, Chișinău, 12 aprilie, 2012;
- Conferința științifică internațională ”Consolidarea statului de drept al Republicii Moldova în contextul evoluției sistemului internațional și proceselor integraționiste”, Chișinău, 3 iunie, 2014.

Implementarea rezultatelor ştiinţifice. Rezultatele științifice pot fi aplicate în procesul de instruire a studenţilor, masteranzilor din cadrul facultăților de drept a instituţiilor de învățământ universitar, precum și în activitatea practică a organelor de drept.

Sumarul compartimentelor tezei. Ținând cont de standardele stabilite, prezenta teză de doctorat are următoarea structură: text de bază 177 pagini, adnotare (în limbile: română, engleză și rusă), listă a abrevierilor, introducere, patru capitole divizate în secțiuni, concluzii generale și recomandări, bibliografia din 221 titluri, declarația privind asumarea răspunderii, cv-ul autorului.

Primul capitol cu titlul ***ANALIZA DOCTRINARĂ A FRAUDEI INFORMATICE,*** este destinat, prioritar, analizei materialelor ştiinţifice relevante (tratate, monografii, cursuri, studii de drept, culegeri și spețe de practică judiciară etc.) publicate la tema tezei de doctorat atât în România, Republica Moldova, cât şi în alte state, aparținând diferitor sisteme de drept. Efortul principal s-a axat pe analiza și evaluarea lucrărilor autorilor: M. Dobrinoiu, Gh. Iu. Ioniță, C. Moise, I. Vasiu, L. Vasiu, I. A. Barbu, F. Encescu, O. Vară, G. Zlati, S. Brînnză, V. Stati, Gh. Alecu, A. Barbăneagră, P .W. Singer, M. Streeter, C. E. Ch. Eastomm, J. Taylor, J. Taylor, G. Kirwan, A. Power, J. Sammons, F. Donovan, K. Bernier, R. Moore, S. W. Brenner, F. Barresi, M. Nigretti etc. În cadrul ambelor secțiuni - 1.1 Analiza materialelor ştiinţifice publicate la tema tezei în România şi Republica Moldova și 1.2 - Analiza materialelor ştiinţifice publicate la tema tezei în străinătate, sunt puse în evidență definiții, caracrteristici, particularități și viziuni ale autorilor privind infracțiunile informatice la general și frauda informatică în particular.

Cel de-al doilea capitol al cercetării cu titlul ***FENOMENUL INFRACȚIONAL ÎN DOMENIUL INFORMATIC: DEFINIȚIE ȘI CARACTERIZARE***, cuprinde în primul rând

considerații generale privind amploarea pe care o are în zilele noastre fenomenul criminalității informatice și a pericolului pe care acesta îl prezintă asupra relațiilor sociale. În acest compartiment al lucrării au fost reliefat fenomenul infracțional în domeniul informatic și operată o amplă caracteristică a acestuia, precum și au fost conturate și tratate modalitățile tipice de comitere și tipologia făptuitorilor în cazul infracțiunilor informatice.

Capitolul trei al tezei întitulat ***SEDIUL NORMATIV-PREVENTIV DE INCRIMINARE A FRAUDEI INFORMATICE: REGLEMENTĂRI INTERNAȚIONALE ȘI NAȚIONALE***, este consacrat caracterizării fraudei informatice din perspectiva reglementărilor internaţionale care standardizează cadrul incriminator al legislaţiilor naţionale. Tot în acest cadru al lucrării a fost analizată frauda informatică din perspectiva practicilor de incriminare urmate de alte state, precum Federația Rusă, Ucraina, Belarus, Polonia, Franța, Germania, Belgia, Spania, Bulgaria – ce aparțin sistemului de drept romano-germanic și Marea Britanie și Canada – aparținând sistemului de drept anglo-saxon; elementelor de drept penal comparat prin prisma relevării componentelor de bază care particularizează normele de drept material existente în domeniu.

În cadrul acestui capitol se acordă o atenție deosebită Convenției Consiliului Europei privind criminalitatea informatică, ca și document care a inspirat legislația penală din România și din Republica Moldova în sensul armonizării normelor de incriminare conform prvederelor acesteia. Nu în ultimul rând au fost relevate reglementările dreptului naţional al Republicii Moldova şi României destinate prevenirii, inclusiv juridico-penale, a fraudei informatice.

Capitolul IV al tezei cu titlul ***INFRACȚIUNEA DE FRAUDĂ INFORMATICĂ ÎN LEGA PENALĂ A ROMÂNIEI ȘI REPUBLICII MOLDOVA***, este dedicat analizei juridico-penale a conținutului legal, condițiilor preexistente, conținutului juridic și agravantelor infracțiunii de fraudă informatică potrivit legislaţiei penale a României şi Republicii Moldova. În textul capitolului dat se reflectă o reevaluare a cadrului normativ-penal privind frauda informatică din legislaţia penală a României şi a Republicii Moldova și formularea recomandărilor ştiinţifice pentru îmbunătăţirea legislaţiei penale pe segmentul problematicii investigate. Studiul juridico-penal al infracţiunii este realizat în baza a două sedii normative incriminatorii: România şi Republica Moldova.

I. ANALIZA DOCTRINARĂ A FRAUDEI INFORMATICE

1.1. Analiza materialelor științifice publicate la tema tezei în România și Republica Moldova

Trăim în două lumi și ambele sunt foarte reale. Una este lumea fizică în care ne-am petrecut existența dintotdeauna și care ne este familiară nouă. Cealaltă este lumea virtuală în care ne creăm o identitate (sau uneori chiar mai multe) online. Aceste identități digitale au devenit parte intgrantă din viața noastră la fel cum identitatea noastră face parte din lumea fizică.

Lumea aceasta virtuală prezintă și ea numeroase riscuri, aceasta deoarece principalele avantaje ale rețelei internet și vulnerabilitățile sale au creat un cadru propice pentru activitățile criminale, determinând apariția unei noi forme de manifestare a criminalității, criminalitatea informatică. Principaliii factori care au contribuit la dezvoltarea acestui fenomen sunt: dependența de tehnologia informației și comunicațiilor, numărul utilizatorilor, disponibilitatea dispozitivelor și accesului, disponibilitatea informațiilor, lipsa mecanismelor de control, automatizarea, comunicații anonime, viteza proceselor de schimb de date, independența locației și prezenței la locul infracțiunii, dimensiunea internațională a transferului de date [70, p.771-777].

Conform raportului emis de către Kaspesky Lab pentru anul 2015, topul țărilor unde utilizatorii au cel mai mare risc de infectare online este condus de Rusia cu 48,9%, Kazakhstan – 46,27%, Azerbaidjan – 43,23%, Republica Moldova este prezentă în top 20, pe locul 15 cu 33,28% în timp ce România se află la categoria de risc moderat cu 23,4% [89].

În ciuda incertitudinii asupra cifrelor, ceea ce putem spune fără echivoc este faptul că infracţiunea informatică prezintă acum cea mai mare ameninţare potenţială cunoscută vreodată la adresa societăţii. Şi aceasta din cauza masivei achiziţionări globale de tehnologie la sfârşitul secolului al XX-lea de către firmele disperate să reducă din costuri şi să-şi stimuleze productivitatea.

Una dintre formele pe care o poate îmbrăca infracțiunea informatică o reprezintă în prezent frauda informatică. O primă constatare care poate fi făcută sub aspectul preocupărilor doctrinare asupra acestei teme, este că până în prezent, în literatura de specialitate din România și Republica Moldova nu au fost elaborate studii monografice, care ar fi destinate abordării exclusive a infracțiunii de fraudă informatică. De regulă, analiza problemelor privitoare la infracțiunea analizată poate fi regăsită în abordările doctrinare privind privind criminalitatea informatică, concretizate în ultimul timp în tot mai multe cărți de specialitate, precum și în cursurile de drept penal – parte specială, de regulă în capitolul rezervat studiului infracțiunilor informatice.

Studiul doctrinar al acestei infracțiuni este un demers interdisciplinar, deoarece înțelegerea acesteia în complexitatea ei, necesită atât cunoștințe juridice, dar și stăpânirea unui limbaj specific informaticii.

Printre primii autori care au analizat în mod monografic criminalitatea informatică se înscrie Maxim Dobrinoiu. În monografia sa intitulată **Infracțiuni din domeniul informatic**, autorul a început prin a descrie conceptul de calculator și apoi pe cel de internet, pentru o bună înțelegere a ceea ce înseamnă un sistem informatic. Cu privire la calculator, acesta îl descrie ca fiind un echipament capabil de a procesa informații și de a efectua calcule complexe la viteze ce depășesc posibilitățile creierului uman. Acesta procesează datele prin intermediul unor seturi de instrucțiuni denumite programe. Aceste programe sau aplicații sunt create de programatori și determină modul de comportare al calculatoarelor [40, p.1]. Aceasta, în timp ce intenetul este definit ca fiind o rețea globală compusă din mii de de rețele mai mici de calculatoare și milioane de calculatoare comerciale, educaționale, guvernamentale și personale [40, p.34], definiție care deși este succintă este foarte edificatoare.

Ulterior, după clarificarea acestor noțiuni de bază fără de care demersul științific nu poate fi realizat, M. Dobrinoiu definește criminalitatea informatică ca fiind orice acțiune ilegală în care un calculator constituie instrumentul sau obiectul delictului, altfel spus orice infracțiune al cărui mijloc sau scop este influențarea funcției unui calculator [40, p.62].

Analizând aspectele de drept comparat referitoare la criminalitatea informatică, același autor sesizează că divergențele care există între codurile penale ale statelor în ceea ce privește modul de reglementare al criminalității informatice se explică, pe de o parte, prin faptul că infracțiunile din domeniul activităților informatice nu au fost recunoscute pe plan mondial decât în ultimii ani și au avut evaluări divergente, iar pe de altă parte, prin nivelul scăzut de dezvoltare al unor state în domeniul criminalităților informatice și al sistemelor de telecomunicații, care nu a impus introducerea reglementărilor în această materie [40, p.77].

O altă preocupare a autorului o constituie clasificarea infratorilor digitali și prezentarea acestora, exemplificând cu categorii precum traficanții de informații și mercenarii, în viziunea autorului ei comițând infracțiuni de pe urma cărora realizează profituri financiare sau alte avantaje patrimoniale mari. Aceștia se ocupă cu spionajul economic și vând concurenței secretele firmelor ale căror rețele reușesc să le penetreze [40, p.310-311].

Totodată, în analiza infracțiunii de fraudă informatică, autorul atrage atenția că frauda informatică poate avea mai multe forme și adesea se poate confunda cu înșelăciunea tradițională, mijlocul de realizare fiind computerul [40, p.222].

Un alt reprezentant al doctrinei penale din România care s-a arătat preocupat de criminalitatea informatică este Gheorghe Iulian Ioniță prin lucrarea sa **Infracțiunile din sfera criminalității informatice**. Acesta prezintă o scurtă analiză a principalelor amenințări la adresa securității sistemelor informatice și rețelelor de comunicații, descriind în mod detaliat ce reprezintă, cum acționează și ce pericole prezintă virușii informatici, troienii, jurnalul de taste (keylogger), analizatoarele de trafic de

rețea (sniffer analysers), kitul de rădăcină (rootkit), instrumentele de scanare (scaninng tool), instrumentele de spargere a parolei (password cracker tool), rețelele bot (botnet) și refuzul serviciului (denial of service) [69, p.32-45].

Autorul prezintă primele încercări de definire a criminalității informatice, specificând faptul că la nivel internațional nu se manifestă încă un consens în ceea ce privește terminologia fenomenului. După o trecere în revistă a unor încercări de definire venite atât din partea unor organisme internaționale, precum Organizația pentru Cooperare și Dezvoltare Economică sau Comisia Comunităților Europene, acesta își asumă o definiție proprie considerând criminalitatea informatică ca ansamblul infracțiunilor comise, prin intermediul sau în legătură cu utilizarea sistemelor informatice sau rețelelor de comunicații, într-un interval temporar și spațial determinat. Sistemul informatce și rețelele de comunicații pot fi instrumentul, ținta sau locația acestor infracțiuni [69, p.50].

Autorul face o scurtă trecere în revistă a evoluției criminalității informatice, distingând patru, etape distincte, după cum urmează [69, p.54]:

- prima (specifică anilor 80), care a fost caracterizată de banalizarea informaticii, piratarea programelor, falsificarea cărților de credit etc.

- a doua (specifică sfârșitului anilor 80), a fost favorizată de apariția rețelelor locale și extinse, precum și a punților de legătură, și caracterizată de importante deturnări de fonduri și ”isprăvile” hacker-ilor care accesau calculatoarele NASA, CIA și oricare altă țintă care reprezenta un simbol politico – ideologic sau un element al puternicului complex militaro – industrial american;

- a treia (specifică anilor 90), care a coincis cu proliferarea sistemelor informatice și rețelelor de comunicații (internet-ului, în special) și a fost caracterizată de specializarea infractorilor, apariția unor veritabili profesioniști ai pirateriei, deturnărilor de fonduri, sabotajelor informatice;

- a patra (în prezent), favorizată de faptul că sistemele informatice au pătruns în toate sectoarele vieții sociale și le controlează pe cele mai importante dintre ele (transporturi, apărare etc.) și care este caracterizată de conturarea de noi și grave amenințări ca terorismul informatic, războiul informatic etc).

Autorul atrage atenția în ceea ce privește procesul de legiferare că nu toate țările care au introdus infracțiuni privind frauda informatică incriminează toate formele de manipulare comise în cursul procesării datelor. În plus, unele legislații nu reclamă ca actele frauduloase să fie comise fără drept [69, p.131].

Gh. Ioniță prezintă diverse ghiduri și proceduri referitoare referitoare la investigarea infracțiunilor informatice, cum este și ghidul Institutului Național de Justiție din cadrul Ministerlui de Justiție al SUA, ghid care prevede următoarele principii generale și care poate fi luat drept etalon și în legislația altor state în ceea ce privește investigarea infracțiunilor informatice [69, p.170]:

- siguranța ofițerului și siguranța celorlalți, ar trebui să rămână preocuparea de bază a prim – respondentului, precizându-se că nimic din ghid nu intenționează să fie sau ar fi conceput ca având o mai mare importanță decât siguranța ofițerului și siguranța celorlalți;

- procesul colectăriii, asigurării și transportării dovezilor digitale nu ar trebui să modifice dovezile;

- dovezile digitale ar trebui examinate doar de cei care au fost instruiți profesional în acest scop;

- tot ce s-a făcut în timpul confiscării, transportării și depozitării dovezilor digitale ar trebui să fie pe deplin documentat, conservat și disponibil pentru studiul cazului.

Primul respondent, în manipularea dovezilor electronice, ar trebui să urmeze următorii pași [69, p.171]:

- recunoaște, identifică, confiscă și asigură toate dovezile digitale la fața locului;

- documentează întreaga scenă și locațiile specifice unde dovezile au fost găsite;

- colectează, etichetează și conservă dovezile digitale;

- împachetează și transportă dovezile digitale într-o manieră sigură.

Înainte de colectarea dovezilor la fața locului, primul respondent ar trebui să se asigure că:

- există o autorizare legală pentru confiscarea dovezilor;

- locul faptei a fost asigurat și documentat;

- sunt folosite echipamente de protecție a personalului.

În sfera preocupării autorului intră, pe bună dreptate, și măsurile privind cooperarea internațională pentru combaterea eficientă a criminalității informatice. Autorul accentuează faptul că autoritățile judiciare române cooperează cu instituțiile având atribuții similare din alte state, precum și cu organizații internaționale specializate în domeniu, în mod direct, în condițiile legii și cu respectarea obligațiilor decurgând din instrumentele juridice internaționale la care România este parte. Obiectul acestei cooperări (după caz) poate consta în asistența judiciară internațională în materie penală, extrădarea, identificarea, blocarea, sechestrarea și confiscarea produselor și instrumentelor infracțiunii, desfășurarea anchetelor comune, schimbul de informații, asistența tehnică sau de altă natură pentru culegerea și analiza informațiilor, formarea personalului de specialitate, precum și alte asemenea activități.

Anchetele comune se pot desfășura pe teritoriul României, în baza acordurilor bilaterale sau multilaterale încheiate de autoritățle competente, în vederea prevenirii și combaterii criminalității informatice, la solicitarea autorităților competente române sau ale altor state. Reprezentanții autorităților competente române pot participa la anchete comune desfășurate pe teritorii ale altor state, cu respectarea legislațiilor acestora [69, p.225].

În ceea ce privește metodologia cercetării infracțiunilor din sfera criminalității informatice, se observă existența unei congruențe între infracțiunile din sfera criminalității informatice și infracțiunile tradiționale. Fenomenul este provocat de faptul că sistemele informatice nu sunt doar ținta infractorilor ci și instrumentul prin care sunt comise alte infracțiuni sau, pur și simplu, acestea facilitează prin funcțiile lor comiterea mai ușoară sau mai sigură a infracțiunilor tradiționale (de drept comun, care puteau și pot fi comise și fără intervenția sistemelor informatice). Din acest motiv, multe dintre investigațiile unor infracțiuni tradiționale (indiferent de natura acestora) vor include sistemele informatice ce pot conține date despre motivația, identitatea, locația, conexiunile făptuitorilor/complicilor etc., și care pot ușura finalizarea respectivelor investigații [69, p.251].

Un alt autor român cu înclinație spre studierea criminalității informatice este Adrian Cristian Moise prin cartea sa **Metodologia investigării criminalistice a infracțiunilor informatice**. Acesta detaliază modul în care se desfășoară un atac asupra unui sistem informatic, precizând că în mod uzual se parcurg următorii pași [2, p.142]:

1. Cercetarea sistemului informatic în vederea obținerii de informații.

Primul pas în cadrul unui atac informatic îl reprezintă cercetarea sistemului informatic pentru a obține informații importante care pot fi utilizate în atac. Așadar este importanr să se obțină informații cum ar fi de exemplu: tipul hardware-ului utilizat, versiunea software, informații personale ale utilizatorilor care pot fi utilizate în următorul pas.

2. Pătrunderea în sistemul informatic.

Imediat ce sistemul informatic țintă a fost identificat, iar informațiile despre el au fost adunate, următorul pas este de a lansa atacuri în scopul pătrunderii în sistem.

3. Modificarea setărilor sistemului informatic.

Modificarea setărilor sistemului informatic reprezintă următorul pas după ce s-a pătruns în sistemul informatic. Acest pas permite atacatorului să reintre în sistemul informatic compromis mult mai ușor.

4. Comunicarea cu alte sisteme.

Odată ce rețeaua sau sistemul informatic au fost compromise, atunci utilizatorul le utilizează în scopul de a ataca alte rețele și computere. Aceleași instrumente care sunt utilizate în pasul nr. 1 sunt acum îndreptate spre alte sisteme.

5. Afectarea rețelelor și a dispozitivelor.

Acest pas include ștergerea sau modificarea fișierelor, furtul datelor valoroase, distrugerea comuterelor sau atacurile DOS (Denial of service attacks).

Autorul nu omite să indice și organele abilitate să efectueze expertizele criminalistice în domeniul informatic, arătând că în România acestea se efectuează de către următoarele institute: Institutul de Criminalistică din cadrul Inspectoratului general al Poliției Române, Institutul Național de

Expertiză Criminalistică din cadrul Ministerului Justiției și Institutul pentru Tehnologii Avansate din cadrul Serviciului Român de Informații[2, p.164] și că singurul organism competent din România în domeniul acreditării laboratoarelor de criminalistică este Asociația de Acreditare din România (RENAR). Totodată, primele două insitute menționate mai sus fac parte Rețeaua Europeană a Institutelor de Criminalistică (ENFS).

Cu referire la probele digitale sunt trecute în revistă o serie de standarde pentru examinarea științifică a acestora [2, p.176]:

- proba originală ar trebui conservată într-o stare cât mai apropiată posibil de starea în care a fost găsită;

- trebuie făcută o copie exactă cu originalul care să fie folosită în examinare astfel încât să nu se distrugă integritatea originalului;

- copiile de date pentru examinare trebuie făcute pe suporturi de date care nu au memorate în ele; suporturile de date trebuie să fie complet curate și verificate contra virușilor și defecțiuniloe;

- toate probele trebuie să fie marcate, etichetate și înregistrate și de asemenea trebuie să fie ținut un lanț al custodiei, iar fiecare pas al examinării criminalistice trebuie înregistrat în detaliu.

La fel, tot cu referire la potențiale probele digitale, se arată că acestea se găsesc în diverse tipuri de fișiere care sunt stocate fie pe hard-disc, fie pe alte dispozitive de stocare, cum ar fi [2, p.179]:

- fișiere create de utilizator: agende, fișiere audio-video, calendare, fișiere de baze și date, fișiere text și fișiere document, fișiere e-mail, fișiere imagine și fișiere de calcul;

- fișiere protejate de utilizator: fișiere comprimate, fișiere criptate, fișiere ascunse, fișiere protejate prin parolă, fișiere ascunse prin metoda stenografiei. Există componente de fișiere care pot avea valoare probatorie, care includ data și timpul creației, modificării, ștergerii, accesului, numele utilizatorului și caracteristicile fișierului;

- fișiere create de computer: fișiere backup, fișiere de configurare, fișiere ascunse, fișiere history, cookies, fișiere log, fișiere de sistem, fișiere temporare

În continuarea aceluiași demers științific sunt indicate și principiile de examinare a unui sistem informatic pentru a se obține probele digitale, după cum urmează [2, p.180]:

- conținut - examinările pot determina ce tipuri de fișiere de date se află într-un sistem informatic;

- comparație – examinările pot compara fișierele de date din sistemul informatic cu fișiere de date și documente cunoscute;

- tranzacția – examinările pot determina timpul și secvența în care fișierele de date au fost create;

- extragerea – fișierele de date pot fi extrase din sistemul informatic sau din dispozitivele de stocare a datelor;

- fișierele de date șterse – fișierele de date șterse pot fi recuperate din sistemul informatic sau din dispozitivele de stocare a datelor;

- conversia formatului - fișierele de date pot fi convertite dintr-un format în alt format;

- căutarea după cuvinte cheie – fișierele de date pot fi căutate după cuvinte sau expresii, iar toate aceste activități vor fi înregistrate;

- parole – parolele pot pot fi recuperate și utilizate pentru decriptarea fișierelor codate;

- codul sursă limitat – codul sursă poate fi analizat și comparat.

Autorul abordează și problema de mare actualitate a contrafacerii cardurilor bancare analizând cele două etape ale contrafacerii, și anume: obținerea detaliilor bancare ale unui cont de card, urmată de falsificarea propriu-zisă (rescrierea datelor frauduloase obținute pe alte carduri de plastic care conțin o bandă magnetică) [2, p.290].

Datorită exploziei telefoniei mobile, A.C. Moise atrage atenția și asupra infracțiunilor care pot fi săvârșite prin utilizarea acestor gadgeturi. Date fiind caracteristicilor lor,.telefoanele mobile sunt foarte utile în societatea informațională, fiind folosite atât în scopuri personale, cât și profesionale de către utilizatori. Mici și relativ ieftine, aceste pot fi utilizate nu numai pentru comunicația vocală, simple mesaje text, agende telefonice, calendare, dar și pentru multe alte funcții caracteristice calculatoarelor. Aceste funcții includ poște electronică, navigarea pe web, stocarea și modificarea documentelor și accesarea datelor de la distanță. Investigarea criminalistică a infracțiunilor informatice săvârșite prin intermediul telefoanelor mobile (mobile phone forensics) este o metodă științifică de recuperare a probelor digitale și de sunet în condițiile legale. Ea cuprinde următoarele etape: conservarea, achiziția,examinarea, analiza datelor și raportarea rezultatelor obținute [2, p.306].

Autorul remarcă un adevăr evident, și anume că datorită extinderii rețelelor de comunicații, în special rețeaua internet este imposibil pentru orice țară din lume să lupte singură împotriva acestui tip de infracțiune. Cooperarea internațională în investigarea infracțiunilor informatice trebuie să se desfășoare cu celeritate.. Investigarea unei infractiuni informatice în astfel de cazuri nu poate avea loc fără formularea unei cereri de asistență judiciară internațională [2, p.349].

O a doua carte de referință a autorului Adrian Cristian Moise o reprezintă **Dimensiunea criminologică a criminalității din cyberspațiu**. Conform acestuia criminologia, care este o știință cu individualitate proprie, destinată studierii cauzelor, stării și dinamicii fenomenului infracțional, a criminalului, în scopul perfecționării actului de justiție, a politicii de apărare socială împotriva crimei și de prevenire a acesteia, poate fi privită și ca o dimensiune a criminalității din cyberspațiu. Cyberspațiul a schimbat natura și domeniul criminailtății și victimizării. Prin urmare a apărut o nouă noțiune și disciplină, denumită Criminalitatea din din cyberspațiu (Cyber Criminology), aceasta fiind o disciplină care studiază cauzalitatea infracțiunilor care se comit în cyberspațiu, un spațiu virtual și impactul lor în spațiul fizic [3, p.16].

Autorul accentuează faptul că în lumea offline, anumite activități, cum ar fi comerțul și afacerile, difuzarea informațiilor sunt supuse la diverse mecanisme de control prin intermediul unor reglementări de stat sau internaționale, în timp ce în lumea online, aceleași activități sunt lăsate să se autoreglementeze. Pe internet, unde nu există nici o intervenție de la nici un fel de organ de guvernare, sancțiunile de autoreglementare nu pot fi suficiente pentru a preveni comportamente nedorite, cum ar fi criminalitatea în cyberspațiu. Punerea în aplicare a legii trebuie să fie susținută de sancțiuni pentru a fi eficientă, autoreglementarea nefiind în măsură să ofere acest lucru. Mai mult decât atât, faptul că internetul nu are o jurisdicție clară, reprezintă un alt obstacol important pentru ca autoreglementarea să fie eficientă. Jurisdicția, mecanismele de pedepsire și instituțiile care impun aceste mecanisme de sancționare nu sunt clare în lumea online, așa cum sunt în lumea offline [3, p.16-17].

În ceea ce privește autoreglementarea pe internet, autorul apreciază care ar obiectivele acesteia [3, p.21]:

- punerea în aplicare a legii; detectarea și eliminarea conținutului ilegal prin cooperarea voluntară a furnizorilor de servicii de internet care include: protecția copilului prin prevenirea realizării de profit de la difuzarea de materiale de pornografie infantilă și prevenirea distribuirii de materiale neo – naziste, de materiale care incită la ură;

- protecția copilului prin prevenirea expunerii copiilor la materiale nepotrivite, cum ar fi, de exemplu, materialele cu un conținut pornografic sau violent.

Se observă, ca un adevăr incontestabil faptul că internetul oferă oportunități fără precedent pentru exercitarea drepturilor omului și joacă un rol important în viața noastră de zi cu zi. În acest context este esențial ca toți actorii, atât cei publici, cât și cei privați să respecte și să protejeze drepturile omului pe internet De asemenea, trebuie întreprinse acțiuni pentru garantarea faptului că internetul funcționează și evoluează într-o manieră care permite exercitarea și respectarea drepturilor omului.

În sprijinul realizării acestei viziuni asupra unui internet care are la bază drepturile omului, au fost definite următoarele principii [3, p.9-10]:

- universalitate și egalitate – toți oamenii se nasc liberi și egali în drepturi și demnitate, acestea trebuind să fie exercitate, respectate și protejate în mediul online;

- drepturi și dreptate socială – internetul este un spațiu destinat promovării și protecției drepturilor omului, precum și progresului dreptății sociale;

- accesibilitate – orice persoană are dreptul de a accesa și utiliza un internet deschis și sigur;

- exprimare și asociere – orice persoană are dreptul de a căuta, primi și distribui liber informații pe internet, fără cenzură sau alte interferențe. Orice persoană are dreptul de a se asocia liber, pe și prin domeniul internetului, în scopuri sociale, culturale, politice sau în alte scopuri;

- viața privată și protecția datelor cu caracter personal – orice persoană are dreptul la viață privată în mediul online. Aceasta include dreptul de a nu fi obiectul supravegherii, dreptul de a folosi mecanisme de criptare și dreptul la anonimitate online;

- viața, libertatea și securitatea – drepturile la viață, libertate și securitate trebuie să fie respectate, protejate și exercitte în mediul online. Aceste drepturi nu trebuie să fie utilizate pentru încălcarea altor drepturi în mediul online;

- diversitate - diversitatea lingvistică și culturală trebuie promovată pe internet, iar inovarea în materie de tehnologie și politici trebuie încurajată pentru a facilita pluralitatea de exprimare;

- acces nediscriminatoriu – orice persoană are drepul la acces universal și deschis la conținutul existent pe internet, fără să existe prioritizări discriminatorii, filtrare sau control al traficului din rațiuni comerciale, politice sau de altă natură;

- standarde și reglementare – arhitectura internetului, sistemele de comunicare și formatele datelor și documentelor trebuie să aibă la baze standarde deschise, care aigură interoperabilitatea deplină, precum și incluziunea și egalitatea de șanse pentru toți;

- guvernare – drepturile omului și dreptatea socială trebuie să reprezinte bazele legale și normative pentru funcționarea și guvernarea internetului.

Adrian Cristian Moise accentuează pericolele care zac ascunse în lumea digitală, dar și faptul că în lumea digitală orice activitate lasă o urmă. Unele persoane cunosc modul cum trebuie acoperită o urmă sau cum sau cum pot să o șteargă. Utilizatorii de internet sunt responsabili pentru informațiile personale pe care le publică pe rețelele de socializare. Peste tot pe internet oamenii sunt încurajați să ofere informațiile personale, preferințele și obiceiurile lor și să dezvăluie locațiile personale. Unele firme intră în posesia unor cantități mari de date cu caracter personal de la clienții lor. Adesea, utilizatorii nu sunt informați de aceste firme cu privire la scopul și modul de utilizare a acestor date, chiar dacă aceștia au consimțit să le transmită. Astfel, prin utilizarea necorespunzătoare a datelor cu caracter personal, utilizatorii ei înșiși ar putea să fie amenințați de potențiale pericole în spațiul virtual. Un număr important de companii care își desfășoară activitatea pe internet, cum ar fi de exemplu, furnizorii de platforme de rețelele de socializare și de servicii profită de această situație. Asfel, aceste companii realizează profituri mari prin comercializarea și exploatarea datelor cu caracter personal, pe care utilizatorii fie le-au transmis în mod liber, sau au fost colectate fără știrea lor [3, p.35-36].

Autorul își apleacă atenția și asupra lumii virtuale, aceasta fiind definită ca un tip de comunitate virtuală care ia adesea forma unui mediu simulat, bazat pe computer, prin care utilizatorii pot interacționa unii cu alții și pot utiliza și crea obiecte, de cele mai multe ori în spații tridimensionale [3, p.63].

El clasifică lumile virtuale în funcție de caracteristicile lor specifice. Astfel, lumile virtuale se împart în două categorii generale: lumea virtuală bazată pe jocuri și lumea virtuală bazată pe

comunitate, acestea adesesea partajându-și caracteristicile uneia celeilalte. Una dintre cele mai importante evoluții în cadrul lumilor virtuale o reprezintă posibilitatea de a transforma câștigurile obținute în cadrul acestor spații online în bani din lumea virtuală. Prin urmare, activitățile din lumea virtuală s-au transformat în profituri în lumea reală [3, p.64].

Cercetând cauzalitatea fenomenului criminalității din cyberspațiu și a victimizării, autorul a încercat să o explice prin teoria tranziției spațiului. Această terorie se referă la circulația persoanelor dintr-un spațiu în alt spațiu (din spațiul fizic în cyberspațiu). Teoria susține ideea că că oamenii se comportă diferit atunci când se deplasează dintr-un spațiu în altul. Principiile de bază ale acestei teorii sunt următoarele [3, p.69-72]:

- persoanele care au un comportament reprimat în spațiul fizic au tendința de a comite infracțiunea în cyberspațiu, care altfel nu ar fi săvârșit-o în spațiul fizic din cauza statutului și a poziției lor;

- flexibilitatea și anonimitatea identității lor și lipsa unor factori de descurajare în cyberspațiu oferă infractorilor posibilitatea de a săvârși infracțiuni în cyberspațiu;

- comportamentul criminal al infractorilor în cyberspațiu este importat în spațiul fizic; acesta, de asemenea, putând din spațiul fizic, să fie exportat în cyberspațiu;

- acțiunile infractorilor din cyberspațiu și natura dinamică spațio-temporală a cyberspațiului oferă șansa infractorilor din cyberspațiu să nu fie descoperiți de organele judiciare;

- infractorii din diferite state naționale se pot asocia în cyberspațiu în scopul comiterii unor infrațiuni, după cum și asocierea infractorilor în spațiul fizic este potrivită pentru a săvârși infracțiuni în cyberspațiu;

- conflictul dintre normele și valorile spațiului fizic cu normele și valorile cyberspațiului determină săvârșirea infracțiunilor în cyberspațiu.

Un alt factor sesizat de autor este faptul că imitarea, mimetismul este una dintre cauzele proliferării infracțiunilor informatice Deși activitățile de recrutare pe internet reduc posibilitatea de imitare în lumea fizică, grupurile teroriste au utilizat internetul pentru a furniza informații și direcții necesare online pentru ca persoanele recrutate să imite activitățile teroriste desfășurate de membrii grupului. De cele mai multe ori vor publica aceste informații pe internet, la care orice membru sau potențial membru al grupului terorist poate avea acces [3, p.83].

O carte de referință în abordarea infracțiunilor informatice o reprezintă **Criminalitatea în cyberspațiu** care îi are drept autori pe Ioana Vasiu și Lucian Vasiu. Autorii trag un semnal de alarmă în privința atacurilor informatice, specificând că acestea ridică probleme noi și multiple și pot afecta toate nivelele societății. Atacurile informatice vizează și afectează persoane fizice din toate grupurile demografice (bărbații și femeile raportând crime într-o proporție aproape egală), firme mici și mijlocii, instanțe de judecată, operatori bursieri, corporații globale, organisme guvernamentale, întregi industrii

sau chiar țări întregi. Impactul atacurilor informatice depinde de victimă și poate consta în pagube financiare mari, încălcarea drepturilor de proprietate intelectuală, contaminarea sau copierea datelor informatice, blocarea accesului la date informatice, repudierea tranzacțiilor sau comunicațiilor electronice, încetinirea vitezei de procesare a datelor ș.a. [98, p.13-14]

Cei doi autori analizează cerințele operaționale și legale privind prevenirea criminalității informatice, începând prin a arăta că sistemele informatice joacă un rol vital în organizațiile moderne pentru că ele furnzează informația necesară și capacitățile de prelucrare și diseminare a acesteia, strict necesare pentru îndeplinirea cerințelor funcționale/operaționale, indiferent de context sau domeniul de activitate. Deoarece infracționalitatea informatică poate avea consecințe multiple, în unele cazuri foarte grave (putând afecta chiar economia sau securitatea națională), precum și pentru a asigura încrederea absolut necesară desfășurării activităților care implică sisteme informatice și pentru a respecta cerințele cerințele legale existente, managementul securității sistemelor informatice devine extrem de important [98, p.64].

Conform autorilor, securitatea în domeniul sistemelor informatice se referă, în primul rând la confidențialitate, integritate, disponibilitate, nuanțând conținutul acestor concepte [98, p.70].

Confidențialitatea este un atribut care se referă la datele informatice și vizează prevenirea accesului fără drept. Datele informatice pot avea o valoare economică importantă, ceea ce poate duce la atacuri informatice care vizează accesul la acestea, implicit încălcarea confidențialității lor. Încălcarea confidențialității datelor personale poate avea multiple consecințe nefaste pentru cei afectați. Datorită caracteristicilor sistemelor informatice, atacurile care vizează încălcarea confidențialității datelor informatice sunt, în unele situații, dificil de detectat sau contracarat.

Integritatea se referă la păstrarea corectă, nealterată și completă a datelor informatice. Integritatea datelor informatice are atât componente fizice, cât și logice și implică anumite condiții dezirabile, care sunt menținute în timp, referitoare la menținerea și păstrarea datelor în condiții corespunzătoare situației inițiale care reflectă fapte corecte.

Disponibilitatea datelor sau sistemelor informatice se referă la prevenirea acțiunilor care împiedică sau întârzie semnificativ accesul la date sau folosirea sistemelor informatice – printre asemenea acțiuni se numără criptarea sau ștergerea datelor sau atacurile care vizează refuzul serviciului (Denial of Service - DoS). Atacurile de acest tip consumă resursele unui sistem informatic, resurse destinate servirii utilizatorilor legitimi.

În continuarea demerslui lor științific se remarcă că amenințările la adresa securității sistemelor informatice reprezintă o preocupare majoră deoarece afectarea negativă a funcționării acestora se reflectă într-o varietate de moduri asupra organizației care deține sau folosește respectivele sisteme: scăderea productivității și a veniturilor; pierderea de date informatice ale organizației, clienților sau angajaților; afectarea negativă a reputației și pierderea sau scăderea încrederii clienților și partenerilor;

costuri legate de respectarea prevederilor legale privind reglementările după un atac; amenzi din partea autorităților și costuri legate de posibilele procese civile; scăderea prețului acțiunilor la bursă, în unele cazuri afectând chiar terțe părți [98, p.79].

Totodată, se face apoi o trecere în revistă a principalilor autori care pot cauza probleme de securitate sistemelor informatice, după cum urmează [98, p.86-87]:

- angajați – aceștia sunt învestiți cu încredere și au acces la sistemul informatic, în multe situații putând abuza de drepturile de acces; în plus, angajații pot comite erori de utilizare, inițializare sau configurare (din neatenție, lipsa unor cunoștințe tehnice suficiente etc.), care pot cauza probleme de securitate;

- consultanți/personalul de întreținere a sistemului – aceștia au adesea acces la sistemul informatic, putând efectua diverse operațiuni;

- furnizori/clienți – motivele lor economice nu sunt în unele cazuri aliniate cu cele ale organizației și, în unele situații pot efectua anumite acțiuni care pot prezenta riscuri de securitate;

- competitori – alți indivizi sau organizații care vor avea de câștigat de pe urma pierderilor organizației cauzate de atacuri asupra sistemului informatic;

- crackeri/hoți profesioniști – persoana care penetrează ilegal sistemele informatice și cauzează daune intenționat;

- experți în spionaj – persoane care sunt specializate în obținerea de informații de care vor beneficia alte organizații. Aceste persoane au un nivel înalt de cunoștințe tehnice, sunt bine plătite și pot adesea realiza acțiunile lor nedectați.

Pentru atacatorii enumerați mai sus, primul pas în penetrarea neautorizată a unui sistem informatic constă în culegerea informațiilor necesare despre sistemele vizate. După colectarea acestor informații, atacatorii încearcă să determine vulnerabilitățile existente, pentru aceasta putând folosi un număr de utilitare (spre exemplu, Nmap pentru a identifica porturile deschise și serviciile care rulează la aceste porturi). Prin vulnerabilități se înțelege orice orice fapt care prezintă o problemă din punct de vedere al securității sistemului de informații într-un anumit context. Vulnerabilitățile pot rezulta din erori de programare (software, bugs), parole ușor de ghicit sau spart sau configurări greșite ale sistemului. Vulnerabilitățile sunt portițele prin care se manifestă amenințările. Unele vulnerabilități permit acces imediat la un calculator sau trecerea de un firewall, altele pot furniza informațiii care să permită indirect accesul neautorizat.

O lucrare recent apărută în rândul cărților din România care abordează problematica criminalității informatice este **Introducerea în crimalitatea informatică** a lui Ionuț Andrei Barbu. Acesta remarcă o realitate codidiană și anume faptul că noua tehmologie oferită de informatică a pătruns în activitatea cotidiană, a bulversat modul nostru de viață obișnuit și ne-a făcut să privim cu mai multă încredere în viitor. Astăzi, pentru a putea cumpăra un bilet de tren sau un tichet în metrou,

trebuie să intri într-un dialog necesar cu automatul care face distribuirea prin accesarea unui cod, activitate care banalizează în totalitate vechiul mod de disribuție [113, p.10].

Acest fapt nu poate să ducă decât la dependența noatră de sistemele informatice deoarece acestea ne oferă posibilitatea de a ne administra în toate domeniile; distribuția electricității gestionarea resurselor, transporturi eriene, alocații familiale, securitate socială, fiscalitate, gestiune bancară și tranzacții financiare, viramente de salarii, controale aeroportuare, cărți de identitate, pașapoarte, permise de cconducere, etc. De aceea, conștientizând importanța pătrunderii noilor tehnologii în viața cotidiană, trebuie să ne luăm măsuri de protejare a sistemelor informatice, noua tehnologie fiind la fel de vulnerabilă pe cât de necesară [113, p.12].

Totodată, în accepțiunea autorului, fenomenul criminalității informatice este compus, într-o accepțiune mai restrânsă din faptele care sunt îndreptate strict asupra sistemelor informatice sau a datelor pe care acestea le conțin, în timp ce în sens mai larg aici pot fi incluse comportamentele care s-ar circumscrie noțiunii de criminalitate legată de calculator [113, p.14].

Autorul sesizează în mod corect faptul că criminalitatea informatică include, pe lângă actele infracționale clasice (fraudă, contrafaceri, prostituție, înșelăciune) și fapte proprii domeniului cibernetic (piraterie, software, furtul de carduri sau falsificarea instrumentelor de plată electronice, virusarea rețelelor, terorismul electronic, hărțuire prin e-mail etc.) [113, p.16].

Ionuț Andrei Barbu avertizează asupra amplorii fenomenului, afirmând că încă din momentul în care răspândirea prelucrării automate a datelor a devenit o certitudine, s-a prevăzut că delictul cel mai frecvent care va fi întâlnit în statisticile privind criminalitatea va deveni criminalitatea prin computer [113, p.18].

Autorul trage un semnal de alarmă și asupra faptului că un atac informatic poate interveni în orice moment, mai ales atunci când rețeaua este conectată la internet. Autorii fraudelor informatice acționează de regulă noaptea târziu, ei evitând orele de zi, cu toate că traficul intens le-ar putea masca activitatea. Procedează așa deoarece mulți dintre aceștia au servicii, merg la școală sau alte activități care nu le permit să desfășoare activități criminale în fața calculatorului. Mulți dintre autorii fraudelor informatice accesează rețelele - țintă în momentele cele mai propice când, datorită traficului redus, rapiditatea penetrării unei rețele atinge viteza maximă, adică în jurul orei 4 dimineața [113, p.33].

S-a încercat chiar realizarea unui portret – robot al celor care încalcă legea săvârșind infracțiuni de natură informatică, considerându-se că acestea încadrează în tipul criminalității gulerelor albe. Un profil clasic al făptuitorilor acestor infracțiuni poate fi rezumat astfel; bărbat cu vârsta cuprinsă între 14 și 44 de ani, având un statut social bun, fără antecedente penale, inteligent și motivat [113, p.34].

Ionuț Andrei Barbu afirmă că alăturarea noțiunilor de drept penal și informatică nu trebuie să surprindă. Calculatorul este un instrument fragil și greu de controlat care poate fi manipulat destul de ușor. Fragilititatea instrumentului informatic îl determină pe legiuitor să încerce să asigure cea mai

bună protecție în scopul de a evita fraudele ce pot lua forme diverse: piratare informatică, crearea de conturi bancare fictive, contrafacere, distrugerea de sisteme prin intermediul unui virus – deci nu e deloc surprinzător că dreptul penal își găsește aplicarea în acest domeniu pentru a sancționa diferitele ativități frauduloase care aduc atingere în special drepturilor persoanelor [113, p.39].

Problematica infracțiunilor informatice s-a aflat în ultimul timp și în centrul preocupărilor tezelor de doctorat din România, putând exemplifica cu teza de doctorat **Criminalitatea informatică** a lui Florin Encescu, susținută în anul 2010.

Autorul sesizează în mod corect faptul că infracționalitatea informatică, este nu numai un domeniu de maximă actualitate în materie penală, dar mai ales un domeniu ce oferă largi și numeroase perspective cercetării viitoare, datorită fenomenalei dinamici tehnologice și diversificării, dar și sporirii gradului de rafinament al activităților antisociale, într-o lume electronică în care existența virtuală devine tot mai mult o a doua natură umană [203, p.7].

Referindu-se la prevenirea și combaterea acestui tip de infracțiuni, autorul remarcă că cele mai multe țări nu iau o poziție coerentă, unitară privind modul în care legea poate fi aplicată pe internet. În acest sens, măsurile trebuie să fie luate pentru a promova abilitarea forțelor la nivel internațional. Este încă o mare nevoie, subliniază el, de noi norme internaționale pentru a face mai ușoară investigarea și urmărirea în justiție a autorilor infracțiunilor săvârșite pe internet. Cercetarea infracțiunilor va continua să fie reglementată de jurisdicția binațională: principiul că un act trebuie să fie pedepsit în ambele țări va continua să se aplice pentru investigațiile penale internaționale, iar autoritățile de anchetă nu vor fi autorizate să efectueze investigații la rețele de calculatoare în afara jurisdicției lor naționale proprii [203, p.8].

O altă teză de doctorat din România, de dată mai recentă și anume din 2014, este și cea a lui Octavian Vară care poartă denumirea de **Criminalitate informatică**, precum cea anterior analizată.

În viziunea autorului, dacă în statele din afara Uniunii Europene guvernele ar putea abuza de spațiul virtual pentru supravegherea și controlul propriilor lor cetățeni, Uniunea poate contracara această situație prin promovarea libertății online și asigurarea respectării drepturilor fundamentale în mediul cibernetic. În același timp însă a sosit timpul ca Uniunea Europeană să-și intensifice eforturile în vederea elaborării unei strategii de securitate cibernetică a mediului virtual, care să prezinte viziunea sa în acest domeniu, clarificând rolurile și responsabilitățile statelor membre [196].

În final, este de remarcat George Zlati care este un alt doctrinar cu înclinație spre analizarea infracțiunilor informatice, acesta prezentând împreună cu un colectiv de autori în **Noul Cod penal. Partea specială. Analize sinteze și explicații** o interesantă relație a fraudei informatice cu alte infracțiuni.

În relația cu infracțiunea de fals informatic, acesta nu este de acord cu opinia conform căreia între falsul informatic și frauda informatică există un concurs de calificări, frauda informatică având un

caracter special față de falsul informatic. Acesta afirmă că în mod cert din Raportul explicativ al Convenției privind criminalitatea informatică rațiunea este diferită în ceea ce le privește, domeniul de activitate fiind, de asemenea, diferit. Este, așadar, posibilă reținerea unui concurs ideal de infracțiuni în anumite ipoteze particulare [168, p.280].

În relația cu infracțiunea de acces ilegal la un sistem informatic (art. 360 C. pen.) se apreciază că accesul la un sistem informatic fiind infracțiune mijloc, iar frauda informatică – infracțiunea scop, ne vom afla în prezența unui concurs ideal de infracțiuni. Nu putem discuta despre o absorbție naturală sau legală în acest context, deoarece infracțiunea de acces neautorizat la un sistem informatic poate fi catalogată inclusiv ca o infracțiune obstacol ce protejează inclusiv aspecte ce nu sunt avute în vedere de frauda informatică – de exemplu, confidențialitatea datelor informatice [168, p.281].

În ceea ce privește relația cu infracțiunea de înșelăciune, autorul consideră că între aceste două infracțiuni există un concurs de calificări incompatibile. Discutăm, practic, în viziunea acestuia despre aceeași valoare socială – patrimoniul – protejată de ambele texte de incriminare, fiind excesiv a sancționa agentul de două ori pentru lezarea aceleiași valori sociale. Tot el consideră însă că trebuie făcută o nuanțare. Astfel, cazul fraudei informatice, paguba trebuie să producă un efect direct al interacțiunii logice cu sistemul informatic vizat, fără a exista o altă conduită ulterioară prejudiciabilă a persoanei vătămate. În mod regretabil, în practica judiciară au existat situații în care s-a reținut un concurs între infracțiunea de înșelăciune și cea de fals și fraudă informatică atunci când agentul a introdus licitații fictive pe internet, în scopul obținerii unui folos material injust, indiderent dacă se reține frauda informatică ori infracțiunea de înșelăciune, este exclus ca acestea să fie reținute împreună. Au existat și în practica judiciară în care s-a reținut exclusiv infracțiunea de fraudă informatică. Acceptăm de multe ori că între cele două infracțiuni există o diferențiere de finețe. Cu toate acestea, este inacceptabil să fie reținute în concurs cu privire la aceeași faptă, același prejudiciu, același subiect pasiv și aceeași împrejurare [168, p.280-281].

În relația cu infracțiunea de alterare a integrității datelor datelor informatice (art. 362 C. pen.) se consideră că nu se poate afirma faptul că frauda informatică are un caracter special față de art. 362 C. pen, deoarece această din urmă infracțiune are o modalitate de comitere - prin deteriorarea datelor informatice – ce nu se regăsește în tipicitatea fraudelor informatice. Cu toate acestea, în viziunea autorului, ne vom afla în prezența unui concurs de calificări redundante atunci când modalitățile de comitere de la art. 362 C. pen. sunt exact cele avute în vedere de art. 249 C. pen. Practic, frauda informatică nu poate fi săvârșită fără comiterea modalităților de la infracțiunea de alterare a integrității datelor informatice. Așadar, în această ipoteză se va reține frauda informatică ce protejează inclusiv valoarea socială avută în vedere de art. 362 C. pen. Va exista un concurs de infracțiuni doar când agentul realizează, pe lângă modalitățile avute în vedere de frauda informatică, și o deteriorare a datelor informatice [64].

În ceea ce privește Republica Moldova, criminalitatea informatică a intrat în sfera preocupărilor autorilor Gheorghe Alecu și Alexei Barbăneagră prin cartea acestora intitulată **Reglementarea penală și investigarea criminalistică a infracțiunilor din domeniul informatic**.

Cei doi autori fac o paralelă între criminalitatea informatică reală și criminalitatea informatică aparentă, arătând că diferența reprezintă cifra neagră a acestui gen de crimă și ea cuprinde toate acele fapte sancționate de legiuitor, dar care, din anumite motive, rămân nedescoperite de către organele abilitate ale justiției penale. Dacă în cadrul criminalității generale se apreciază că cifra neagră reprezintă un important segment de fapte penale nedescoperite, în cadrul criminalității informatice, procentul acesteia tinde tinde să fie în jur de 90%. Din totalul fraudelor detectate, 58% sunt descoperite din greșeală sau din întâmplare – ceea ce indică faptul că sistemele de control din cadrul companiilor sunt neadecvate, ele neputând sesiza și detecta fraudele în foarte multe cazuri [65, p.20].

Referindu-se la subiectul activ al infracțiunii informatice, se afirmă că dezvoltarea fără precedent a tehnologiei informației a dus la crearea unui nou grup, cu specificitate aparte, cel al calculatoriștilor. Din cauza perioadei scurte în care s-a format, grupul de calculatoriști este constituit în proporție de 90% din indivizi tineri, dacă nu foarte inteligenți, atunci foarte capabili de a lucra cu entități abstracte, grupul dovedind că poate acționa mult mai unitar decât altele [65, p.178].

În ceea ce privește subiectul pasiv al infracțiunilor informatice, Gheorghe Alecu și Alexei Barbăneagră consideră că cooperarea victimei este un factor esențial în eliminarea criminalității informatice. Reticiența de a anunța organele abilitate să efectueze cercetarea constituie o problemă gravă în lupta contra acestei criminalități. În multe cazuri, numai o informație din partea victimei permite investigarea faptei comise, urmărirea și arestarea infractorului. Denunțarea infracțiunilor informatice în fața autorităților competente și, în general, a publicului, ar putea să aibă avantaje pentru organismele informatice în ceea ce privește prevenirea acestor fapte. S-ar putea ajunge prin urmare, la o mai bună evaluare a imperfecțiunilor și a riscurilor în unitatea în care lucrează victima sau în alte organizații de același tip și, în consecință la o ameliorare a calității măsurilor de securitate informatică și de detectare a infracțiunilor informatice. În mod sigur aceasta ar putea ameliora atât competența, cât și experiența organelor însărcinate cu cercetarea și judecarea infracțiunilor informatice".

Preocupându-se și de măsurile de securitate în sistemele informatice, autorii remarcă că orice organizație, companie, instituție deține date și informații sensibile, pe care trebuie să le protejeze: numere ale cărților de credit ale clienților, parole de acces, secrete de cercetare - dezvoltare și înregistrări financiare. Aceste date și informații au devenit rapid un fel de "bijuterii ale coroanei" în inima oricărei organizații, informații care trebuie ținute departe de ochiul unei persoane neautorizate, văzute doar de cei care au acces autorizat [65, p.188].

Ca o măsură măsură de securitate în vederea scurgerii de informații, se recomandă de către cei doi autori ca utilizatoririlor individuali dintr-o companie să li se asigure accesul la datele de care au

strictă nevoie sau care sunt de folosință generală și interzicerea folosirii acelor date care le exced responsabilitatea. O atenție deosebită trebuie acordată managementului activității de securitate și selectării personalului care va lucra cu fluxul de informații, stabilirii unor reguli clare și asigurarea respectării acestora. Accesul la informații trebuie restricționat la datele strict necesare îndeplinirii sarcinilor de serviciu, iar materialele sensibile vor fi împărțite în secțiuni, astfel încât nici un angajat să nu cunoască documentele respective în întregime [65, p.189-190].

Pentru implementarea concretă a acestor măsuri, utilizatorii trebuie să ia la cunoștință despre reguli referitoare la ceea ce le este permis, și mai ales, la ceea ce nu le este permis în interiorul sistemului informatic, după cum urmează [65, p.192];

- să nu folosească nici un echipament de calcul fără permisiune;
- să nu încerce să acceseze informații decât dacă au cunoștință că sunt autorizați în acest sens;
- să nu folosească echipamentele de calcul în scopuri personale;
- să știe ce trebuie făcut în situația în care un virus este descoperit în sistem;
- să nu modifice datele stocate decât în cazul în care sunt autorizați în acest sens;
- să fie foarte atenți la informațiile copiate de pe internet sau alte surse în vederea identificării programelor tip virus sau cal troian;
- să-și păstreze în mod confidențial datele de identificare (user-name) și acces (parolă) și să nu permită nimănui să nu le folosească;
- să nu lase un calculator în funcționare nesupravegheat, fără să folosească opțiunile de securitate care solicită introducerea unei parole pentru a obține accesul la stația de lucru;
- să nu folosească datele de identificare și de aces ale altor persoane;
- să ia în considerare faptul că toate activitățile realizate în sistem, prin folosirea elementelor personale de identificare și acces, vor cădea în responsabilitatea sa.

Tot în Republica Moldova, o altă carte de referință în domeniu o constituie **Pasul II în ciberspațiu: Securitatea informațională**, semnată de un colectiv de autori: Nicolae Ploteanu, Sergiu Maftea, Rodica Griniuc, Angela Coțofană.

Conform opiniei autorilor, prin pericol pentru securitatea informațională se are în vedere intenția, acțiunea (inacțiunea) manifestată real sau potențial, sau factorul cu caracter ecologic, tehnic sau de alt gen, a cărui realizare sau dezvoltare contravine intereselor de bază a persoanei, societății și statului în domeniul infracțional [149, p.13].

Ei clasifică sursele pericolelor securității informative a Republicii Moldova în surse externe și surse interne.

Principalele surse externe ar fi următoarele [149, p.16]:

- ciber – criminalitatea transnațională, activitatea structurilor criminale, a unor grupuri sau persoane, orientată spre obținerea accesului nesancționat la resurse de rețea și informație;

- activitatea ilegală a organizațiilor teroriste și extremiste internaționale, interesul acestora față de posedarea și utilizarea ”armei informaționale;

- activitatea structurilor internaționale, politice, economice, militare, de spionaj și a serviciilor speciale, orientată spre efectuarea controlului asupra spațiului cibernetic global și obținerea nesancționată a informației;

- avansarea tehnologică a marilor puteri mondiale, întețirea concurenței mondiale pentru deținerea celor mai importante tehnologii și resurse;

- elaborarea de către un șir de state a conceptului de ”război informațional”, care presupune crearea unor mijloace eficiente de influență asupra mediului informațional al altor state, distrugerea infrastructurii informaționale sau defectarea funcționării normale a sistemelor informaționale și de comunicații, obținerea accesului nesancționat la resurse informaționale sau impunerea unor informații false.

Principalele surse interne ale pericolelor sunt următoarele:

- imperfecțiunea bazei normative ce reglementează organizarea și funcționarea sistemului complex, unic de protecție a informației în Republica Moldova, inclusiv subsistemele de protecție tehnică criptografică a informației;

- activitatea ilegală a unor grupuri de persoane orientate spre obținerea nesancționată a accesului la informație și efectuarea controlului asupra funcționării sistemelor informaționale și de telecomunicații;

- coordonarea insuficientă a activității, delimitarea neclară a autorităților organelor administrației publice ce țin de elaborarea și elaborarea politicii unice de stat în vederea asigurării securității informaționale a Republicii Moldova;

- utilizarea forțată, cauzată de rămânerea în urmă a industriei autohtone, a mijlocelor de program și aparat importate, la crearea și elaborarea sistemelor informaționale și de telecomunicații;

- nivelul inadecvat de automatizare a autorităților administrației publice, a domeniului de credit și a celui financiar, industrial, agriculturii, educației, sănătății, domeniului de deservire a cetățenilor, precum și nivelul insuficient de instruire pentru a lucra la calculator și a nivelului general de educație;

- finanțarea bugetară necorespunzătoare a activităților ce țin de securitatea informațională în Republica Moldova.

Autorii avertizează asupra faptului că uneori, un eveniment care are loc pe un computer sau o rețea este parte a unei serii de pași ce intenționează să producă un acces neautorizat. Acest eveniment este apoi considerat ca parte a unui atac. Un atac are mai multe evenimente. În primul rând e format din mai mulți pași pe care atacatorul îi face. Printre acești pași regăsim o acțiune îndreptată spre o țintă, cât și utilizarea unei unelte pentru a exploata o vulnerabilitate. În al doilea rând, un atac intenționează să obțină un rezultat neautorizat privit din perspectiva utilizatorului sau administratorului

sistemului în cauză. În final, un atac reprezintă o serie de etape voluntare pe care atacatorul le realizează, acest lucru diferențiind un atac de secvență de acțiuni normale [149, p.46].

O lucrare de referință în domeniul dreptului penal din Republica Moldova o reprezintă monumentalul tratat de **Drept penal. Partea specială** a autorilor Sergiu Brînză și Vitalie Stati. Deși această carte nu se constituie într-o monografie dedicată criminalității informatice, după cum arată și titlul acesteia, prin modul exhaustiv în care sunt abordate și analizate inclusiv infracțiunile informatice, ea reprezintă o lucrare etalon în domeniu.

Potrivit autorilor dacă deceniul trecut a fost marcat de apariția și perfecționarea calcalculatoarelor personale, ușor accesibile și la prețuri din ce în ce mai scăzute, deceniul actual este caracterizat de conectivitatea tot mai pronunțată, adică de fuziunea dintre calculatoare și telecomunicații; cele mai multe calculatoare sunt folosite azi în interconectare, în rețele locale (LAN) și în rețele de arie largă (WAN), ceea ce conferă informaticii și telecomunicațiilor un rol determinant în asigurarea legăturilor științifice, de afaceri, bancare sau de natură umană între persoane și instituții. Trăim într-o lume în care sute de milioane de calculatoare, deservind utilizatori foarte diverși, sunt interconectate într-o infrastructură informatică globală. Specialiștii caută și găsesc, cu o viteză de-a dreptul incredibilă, soluții tehnice pentru dezvoltarea capacității de comunicație a calculatoarelor și pentru sporirea calității serviciilor de rețea oferite [170, p.253].

Conform acestora, crearea tehnicii de calcul cu o potențialitate enormă, implementarea ei amplă în activitatea economică, socială și managerială, alături de sporirea considerabilă a valorii informației – toate acestea dictează necesitatea reglementării juridice a proceselor care au loc în sfera informatizării [170, p.253].

În opinia celor doi autori informația stocată nu are nici o valoare în sine. Valoarea ei devine evidentă în momentul în care o folosești, sau mai rău, o pierzi prin nefolosirea rapidă și eficientă. De aici efortul permanent de reorganizare a producției și distribuției de informație, precum și a simbolurilor utilizate pentru a o comunica. Deci, informațiile trebuie protejate și când sunt lansate în rețele pentru a se restructura în modele din ce în ce mai largi, în arhitecturi de cunoștințe. Datorită spațiului în care se poartă și legislației precare, războiul infracțional în acest caz implică riscuri mici și posibile câștiguri mari [173, p.253].

1.2. Analiza materialelor ştiinţifice publicate la tema tezei în străinătate

În străinătatate, dar prepomderent în S.U.A. au fost publicate numeroase cărţi dedicate analizei fenomenului de criminalitate informatică.

Un astfel de caz este, de exemplu, lucrarea **Computer Crime, Investigation, and the Law** scrisă de Chuck Eastomm şi Jeff Taylor, în care se face şi o interesantă prezentare a istoricului infracţiunilor informatice în America.

Astfel, 1981 nu a fost doar anul primei arestări pentru o infracţiune informatică, ci a fost un an pivotal şi în istoria viruşilor informatici. Primii viruşi cunoscuţi pe scară largă găsiţi „în sălbăticie" (adică în spaţiul public) au fost Apple I, II şi III, descoperiţi în anul 1981. Aceşti viruşi aveau drept ţintă sistemul de operare Apple II şi s-au răspândit iniţial în sistemele Universităţii A&M din Texas prin intermediul jocurilor de calculator piratate. Acest incident este deosebit de interesant deoarece a implicat, de fapt, două infracţiuni: prima a fost lansarea propriu-zisă a virusului informatic, iar a doua a fost faptul că multe victime ale virusului au devenit victime prin propria lor activitate infracţională – furt de date prin piraterie de programe informatice [19, p.39].

În 1983, ajungem la un alt punct de reper în acest domeniu În acest caz, un grup de adolescenţi, care se autodenumeau grupul 414, cu referinţă la codul zonei în care locuiau (Milwaukee), au fost arestaţi de FBI şi acuzaţi de multiple incidente de pătrundere în calculatoare. Printre calculatoarele în care pătrunseseră erau şi cele ale Centrului de Cancer Sloan Kettering şi ale Laboratoarelor Naţionale Los Alamos. Unuia dintre cei acuzaţi i s-a acordat imunitate împotriva trimiterii în judecată în schimbul cooperării cu autorităţile, iar ceilalţi au primit cinci ani de supraveghere strictă. Acest caz este fascinant din câteva motive. Primul şi cel mai important este faptul că acesta este una dintre primele arestări pentru hacking. În perioada aceea de început, legile privitoare la infracţiunile informatice erau încă inadecvate şi, sincer vorbind, multora dintre instituţiile însărcinate cu supravegherea respectării legii le lipseau cunoştinţele necesare pentru investigarea infracţiunilor informatice. În al doilea rând, acest caz este notabil din cauza ţintelor înalte care au fost atacate de hackeri. În vremea aceea, era ceva obişnuit ca administratorii de reţea să acorde destul de puţină atenţie, sau chiar deloc, măsurilor de securitate. Avuseseră loc atât de puţine incidente de hacking încât chiar şi cei din comunitatea tehnologiei informaţiei nu erau pe deplin conştienţi de potenţialele pericole. În ultimul rând, este vrednică de remarcat sentinţa relativ uşoară. Aceşti indivizi au pătruns în calculatoare de mare importanţă şi au riscat să producă stricăciuni uriaşe datelor şi totuşi sistemul justiţiei infracţionale a tratat acest caz ca o poznă tinerească inofensivă. Din nefericire, aşa au fost tratate de obicei infracţiunile informatice la începuturi. Tribunalele tratau infracţiunile informatice cu uşurinţă. Poate fi doar o speculaţie, dar pare a fi rezonabil să presupunem că asemenea sentinţe uşoare

n-au făcut altceva decât să încurajeze şi alte infracţiuni de acelaşi fel sau, în cel mai bun caz, au făcut foarte puţin înspre a le descuraja [19, p.40].

Anul 1989 a fost un an de răscruce pentru infracţiunile informatice, conform aceloraşi autori. Acesta a fost anul primului incident de spionaj cibernetic recunoscut pe scară largă. Cinci indivizi din Germania Federală au fost arestaţi pentru pătrunderea ilegală în sisteme informatice ale guvernului şi ale unor universităţi şi pentru furtul unor date şi programe. Trei din cei cinci vindeau datele şi programele software guvernului sovietic. În timp ce au existat fără îndoială incidente de spionaj cibernetic înaintea acestuia, acest incident a fost primul care a devenit cunoscut publicului. Spionajul, inclusiv cel cibernetic, este dificil de documentat. Unul dintre motive este acela că doar eşecurile dramatice ajung să fie cunoscute în mod public. Spionajul reuşit nu ajunge niciodată la public. Este de asemenea problematic faptul că politica serviciilor secrete este întotdeauna aceea de a refuza să confirme sau să infirme orice presupus incident, în timp ce susţinătorii teoriei conspiraţiei tind să arunce vina pentru orice pe vreun complot guvernamental infam. Încercarea de a afla adevărul dintre cele două extreme este cât se poate de dificilă. Totuşi, este rezonabil să presupunem că folosirea sistemelor informatice pentru scopuri de spionaj a precedat anul 1989 şi continuă, fără îndoială, şi astăzi [19, p.42-43].

Ei punctează faptul că anii ’90 au adus, printre altele, exemple de terorism cibernetic fără echivoc. În 1998, gherilele etnice tamileze au invadat ambasadele Sri Lankăi cu 800 de emailuri pe zi timp de două săptămâni. Mesajul era: „Noi suntem Tigrii cei negrii ai Internetului şi facem aceasta pentru a vă întrerupe comunicaţiile.” Serviciile secrete l-au caracterizat ca fiind primul atac cunoscut al unor terorişti împotriva sistemelor informatice ale unei ţări. Evident, se pot purta discuţii despre care a fost primul atac terorist cibernetic real, dar acest incident îndeplineşte, în mod cert, toate cerinţele. Mai întâi, a fost un atac pur cibernetic. În al doilea rând, a fost în mod clar realizat în scopuri politice. Şi în ultimul rând, a fost parte dintr-un conflict aflat în plină desfăşurare [19, p.47-48].

Anul 2003 ne-a adus un alt capitol interesant în istoria infracţiunilor informatice. Acesta a fost anul în care Microsoft a început să anunţe „recompense” ca un mod de a facilita capturarea hackerilor, a creatorilor de viruşi şi a altor feluriţi infractori informatici. Până acum nu există indicii că vânarea recompenselor cibernetice ar fi fost o întreprindere de succes, dar a fost un mod interesant de a combate infracţiunile informatice. Rămâne de văzut dacă „vânătorii de recompense cibernetice” liber-profesionişti vor fi de folos în depistarea infractorilor informatici, într-un mod foarte asemănător celui în care vânătorii de recompense ai Vestului Sălbatic au ajutat la capturarea proscrişilor timpului lor [19, p.52].

Având în vedere că apariția și proliferarea infracțiunilor informatice nu ar fi fost posibilă fără apariția internetului, autorii Peter.Warren. Singer și Michael Streeter în lucrarea **Cyber crime and warfare** prezintă o interesantă istorie a apariției și dezvoltării acestuia.

Istoria internetului este mai lungă decât cred mulţi. Nu mai târziu decât în anul 1962, informaticianul american J.C.R. Licklider venise cu ideea de a lega între ele mai multe calculatoare pentru a forma o reţea. În decursul unui deceniu, au fost dezvoltate o varietate de reţele însărcinate cu comutarea pachetelor de mesaje, dintre care cea mai importantă a fost numită ARPANET, prescurtarea în limba engleză pentru Reţeaua Agenţiei Proiectelor de Cercetare Avansată. ARPA era o agenţie a Departamentului Apărării Statelor Unite, iar aceasta nu a fost nici prima, nici ultima dată în istorie când un proiect militar a condus la realizări deosebit de benefice pentru societate..În acea periodă, ARPA avea la dispoziţie doar un număr limitat de calculatoare puternice de cercetare, iar acestea erau răspândite prin ţară, îngreunând accesul cercetătorilor. Logic, legarea lor urma să accelereze cercetarea. ARPANET şi-a început viaţa în 1969, iniţial conectând doar calculatoare din Statele Unite, dar în prima parte a anilor ’70 s-a conectat şi Norvegia, iar mai apoi Regatul Unit. În 1983 armata S.U.A. a ieşit din proiect pentru a-şi constitui separat propria sa reţea de comunicaţii. Între timp, diverşi informaticieni, printre care Vinton Cerf şi Bob Kahn, lucrau la protocoale pentru a armoniza diferitele reţele care începuseră să se dezvolte paralel cu ARPANET-ul. Este greu să se dea data precisă a naşterii internetului, deoarece a fost un proces de durată, dar pe la începutul anilor ’90 ajunsese deja larg răspândit. Odată cu apariţia Reţelei Informatice Internaţionale în 1991 (adoptarea de către consumatori pe scară largă a Reţelei a început în 1995), o parte semnificativă a populaţiei lumii era expusă celei mai mari reţele din istorie. În acelaşi timp, răspândirea şi utilizarea populară a Internetului şi Reţelei – în special în forma unei cereri explosive de email-uri – reprezenta o oportunitate gigantică pentru creatorii viruşilor de calculator [154, p.26-27].

Autorii fac distincție între internet și Reţeaua Informatică Internaţională (engl. World Wide Web). Reţeaua Informatică Internaţională a fost inventată de omul de ştiinţă britanic Tim Berners-Lee la începutul anilor 90 şi este, în esenţă, un sistem care ne permite să vedem de pe calculatorul nostru documente „hipertext” asociate sau „pagini”. Reţeaua nu este acelaşi lucru cu internetul. Reţeaua poate fi privită drept o aplicaţie sau un serviciu care funcţionează pe internet, care este ea însăşi un sistem internaţional de reţele de calculator conectate. Contribuţia cheie a lui Berners-Lee a fost să descopere cum sistemul hipertext deja cunoscut poate fi făcut să funcţioneze pe internet [154, p.29].

Lucrarea **Cybercrime. The Psichology of Online Offenders** scrisă de Grainne Kirwan și Andrew Power analizând printre altele și conflictele de jurisdicție incearcă să găsească un răspuns la întrebarea dacă există cumva un spaţiu virtual sau spaţiu cibernetic unde sistemele legale tradiţionale nu au jurisdicţie şi unde o nouă ordine poate fi construită de către locuitorii acelui spaţiu. Ideea spaţiului cibernetic ca loc unde poţi merge şi unde noi legi s-ar putea aplica este sprijinită de faptul că trebuie să iei o decizie pentru a merge acolo, manifestată prin accesarea un calculator şi introducerea unei parole. În acest sens există o graniţă pe care o treci pentru a ajunge „acolo”. S-a sugerat că s-ar putea ca spaţiul cibernetic să semnalizeze ultimele zile ale unui sistem de guvernare care se bazează pe

statele suverane individuale ca autorităţi legislative primordiale, un sistem care ne-a servit, adesea spre mai bine şi uneori spre mai rău, în ultima jumătate de mileniu [75, p.32].

Autorii apreciază că atunci când se ia în considerare crearea unui cadru de lege pentru internet, sunt lecţii de învăţat de la dreptul internaţional. O caracteristică a dreptului internaţional este apariţia conceptului de soft law ca o soluţie mai eficientă decât. hard law în numeroase situaţii multistatale. Hard law este definit ca fiind regulile şi regulamentele care alcătuiesc sistemele legale în sensul tradiţional, iar soft law ca fiind format din reguli informale ce nu au un caracter obligatoriu dar, datorită normelor cutumiare sau standardelor de comportament, au efect practic [75, p.36].

O altă lucrare în domeniu cercetat este **The Basics of Digital Evidence**, autor John Sammons. Autorul subliniază că examinarea calculatoarelor şi a probelor ce rezultă din această operațiune constituie procedee veritabile practicate de organele poliţiei pe întreg teritoriul Statelor Unite în vederea demascării și tragerii la răspundere a cyber infractorilor.

El remarcă că pentru a contracara noile progrese ale criminalisticii în domeniul investigării infracțiunilor informatice, instrumente şi tehnici anticriminalistice apar în număr semnificativ de mare. Există multe definiţii ale termenului anticriminalistică, cum ar fi: orice demers de a manipula, şterge sau obscuriza date digitale sau de a face examinarea lor dificilă, de lungă durată sau aproape imposibilă. Există chiar şi un site de internet dedicat acestui subiect şi cei ce susţin site-ul nu sunt câtuşi de puţin subtili cu privire la obiectivele lor. Anti-Forensics.com este o comunitate dedicată cercetării şi punerii în comun a unor metode, instrumente şi informaţii care pot fi folosite pentru a crea frustrare în cadrul investigaţiilor criminalistice informatice pentru examinatorii criminalişti. Descrierea continuă cu precizarea scopului acestui site, arătându-se că un scop major al unor programe de anticriminalistică, precum şi punctul focal al Anti-Forensics.com, este să facă analiza şi examinarea probelor digitale cât mai dificilă, confuză şi îndelungată cu putinţă [116, p.81-82].

Utilizarea tehnicilor anticriminalistice nu se limitează la terorişti şi pedofili. Ele au fost puse în uz şi de către personalul executiv al marilor corporaţii, care folosesc aceste instrumente şi tehnici pentru a ascunde sau a distruge emailuri, evidenţe financiare incriminatorii ş.a.m.d. Chiar şi unele aplicaţii uzuale precum browser- ele de Internet au caracteristici care ar putea fi folosite pentru a obstrucţiona o examinare criminalistică – ştergerea istoriei navigărilor pe internet, de exemplu. Cele mai multe browsere de nouă genereaţie vin cu un mod numit „private browsing” (rom. „navigare privată”), care nu înregistrează lucruri precum site-urile web vizitate şi istoricul căutărilor [116, p.82].

Felicia Donovan și Kristin Bernier în lucrarea lot **Cyber Crimes Fighters: Tales from the Trenches** prezintă mai multe moduri de operare ale hackerilor, între care unele mai noi, realizate prin intermediul telefoniei celulare. Astfel, se afirnă că suntem permanent fascinaţi de ritmul rapid de dezvoltare a tehnologiei. Din nefericire, şi persoanele rău-intenţionate sunt fascinate. Nu le-a luat mult până să-şi dea seama că, dacă nu te-au putut păcăli pe internet, te-ar putea păcăli prin telefon. Astfel a

început conceptul de *vishing* sau *phishing de voce*. Vishing-ul este foarte asemănător phishing-ului, doar că foloseşte telefoanele drept mediu de transmitere a mesajelor. Vishing-ul nu se deosebeşte cu nimic de phishing în privinţa faptului că este o metodă inteligent deghizată de a obţine informaţii de identificare personală. Manevrele obişnuite vor implica notificarea că s-a pătruns în contul tău bancar sau că acesta a fost suspendat, dezactivat sau închis şi ţi se dă un număr pentru a suna şi a corecta situaţia. Când suni la acel număr, este derulat un mesaj de bun venit care sună autentic, iar apoi eşti îndemnat să îţi dai numărul de cont şi parola sau pin-ul. Mesajele de vishing pot fi trimise atât vocal cât şi sub formă de text, dar toate au acelaşi scop – să ne facă să divulgăm informaţiile legate de cont. Nu trebuie însă să ne lăsăm înșelații! De reținut și de subliniat că: nici o instituţie legitimă nu ne va întreba despre parola sau PIN-ul nostru la telefon [54, p.183]!

În lucrarea sa **Cybercrime - investigating high-technology computer crime**, Robert Moore a abordat, printre altele, și modul în carei hacking-ului a început să fie pus în evidență în mass – media, astfel încât lumea a început să devină conștientă de puterea potenţială pe care o putea avea un hacker, precum şi cu privire la publicitatea ce putea fi generată de asemenea fapte.

Astfel, de-a lungul celei de a doua jumătăţi a anilor 80 şi în primii ani ai anilor 90, oameni din întreaga lume au aflat despre escapadele unui tânăr numit Kevin Mitnick. Ca adolescent în anii ’80, Mitnick avea în mod constant probleme cu autorităţile din cauza activităţilor sale inadecvate în ceea ce priveşte computerele. Însă, în primii ani de după 1990 numele lui Mitnick a devenit foarte bine cunoscut atunci când a fost depistat tocmai din cealaltă parte a ţării de către un inginer în calculatoare al cărui computer Mitnick îl accesase ilegal. Mitnick îl văzuse pe inginerul cu pricina la televizor discutând despre o nouă tehnică de convertire a telefonului celular într-un receptor digital. Dorind să aibă aceste informaţii, Mitnick a pătruns în computerul inginerului şi a luat planurile asociate tehnicii. Inginerul, descoperind că se pătrunsese în computerul său, s-a dedicat în totalitate prinderii lui Mitnick. Acesta a fost forţat să plece de acasă şi a trăit ca fugar pentru o vreme.

Kevin Mitnick a ajuns să fie privit ca un infractor periculos şi deţine distincţia de a fi fost primul infractor computerist care a apărut pe lista celor căutaţi de FBI. Mai mult decât atât, cartea **Takedown (Punerea la podea)** consemnează urmărirea şi capturarea cyber infractorului Mitnick. Se consideră în general că escapadele lui Mitnick au adus chestiunea hacking-ului în prim-planul atenţiei naţiunii americane. Mai mult, activităţilor sale li se dă creditul de a fi speriat guvernul şi a-l fi făcut să creadă că hacking-ul poate fi periculos. Când Mitnick a fost în cele din urmă capturat, sentinţa lui a fost mai severă decât multe diverse sentinţe de omucidere din acea vreme. De ce o pedeapsă atât de severă pentru un delict nonviolent? Se spune că de-a lungul carierei sale infracţionale, Mitnick a reuşit să obţină accesul la unele din cele mai păzite sisteme de computere din ţară printr-o combinaţie de măiestrie în programarea computerelor şi abilităţi de inginerie socială. Ingineria socială se referă la abilitatea de a folosi competenţe de comunicare scrisă şi vorbită pentru a-i convinge cu şiretenie pe

oameni să furnizeze informaţii necesare – în cazul lui Mitnick, informaţii necesare pentru a obţine acces la diferite computere [164, p.22-23].

Mitnick avea o astfel de reputaţie legată de operarea aparaturii tehnice încât se spune că mulţi administratori de penitenciare i-au refuzat accesul la echipamente electronice. De exemplu, Mitnick a fost pus o dată în regim de carceră deoarece oficialilor închisorii le era teamă că încearcă să-şi transforme radioul portabil într-un dispozitiv de interceptare a convorbirilor. Se spune că se credea că plănuise să plaseze dispozitivul de ascultare în biroul gardianului. Lui Mitnick i s-a refuzat, se zice, şi accesul la convorbiri telefonice nesupravegheate din cauza fricii că putea intra prin tastare pe telefon în computerele Departamentului de Apărare, ceea ce se zvonea că fusese în stare să facă de câteva ori de-a lungul carierei sale (deşi acest fapt nu a fost niciodată confirmat de vreo sursă oficială) [164, p.23].

Povestea lui Kevin Mitnick prezintă un interes special datorită impactului pe care l-a avut arestarea sa asupra altor membrii ai comunităţii de hackeri. Ca rezultat al încarcerării sale, Mitnick a devenit, pe bună dreptate, hackerul cel mai popular din lume. Au răsărit pe Internet numeroase site-uri în toate limbile care aduceau argumente în favoarea elibererării lui Mitnick. Strigătul lor comun era „Eliberaţi-l pe Kevin". Au exista numeroase articole pe internet care discutau campania „Eliberaţi-l pe Kevin" şi s-a realizat un documentar de către compania care publică revista *2600*. După eliberarea lui Mitnick, acestuia nu i s-a permis să atingă vreun computer, dar putea acorda asistenţa sa de expert în cazurile care implicau o infracţiune legată de computer, folosind o altă persoană pentru tastarea pe computer. Se spune că de când a fost arestat şi a petrecut timp în închisoare Mitnick nu a mai comis nicio infracţiune, renunţând la viaţa lui de infractor informatic. De fapt, şi-a înfiinţat propria companie de securitate a computerului (în a cărei pagină web s-a intrat incidental prin hacking în ziua lansării sale) şi a scris două cărţi. Una din ele detaliază felul în care companiile îi pot împiedica pe cei care vor să obţină acces la date prin inginerie socială, iar cealaltă carte examinează incidente de hacking care au implicat activităţi de inginerie socială aplicată de alţi hackeri [164, p.23-24].

Un alt nume cu rezonanță în studierea criminalității informatice este și Susan W. Brenner, prin lucrarea acesteia, **Cybercrime. Criminal threats from cyberspace.** Analizând și frauda, aceasta apreciază că frauda este un tip de furt. Aşa cum a remarcat o instanţă de judecată, cineva comite furt când ia o proprietate personală a altcuiva şi o duce cu sine cu intenţia de a fura proprietatea". Furtul constă în luarea proprietăţii cuiva fără permisiunea acestuia şi cu intenţia de a priva permanent victima de posesiunea şi de uzul acelei proprietăţi. Frauda este o variaţiune relativ nouă a furtului. Infracţiunea de fraudă a fost creată pentru a cuprinde situaţia în care victima dă de bună voie proprietatea infractorului – fraudator. Dacă proprietarul îşi dă prin consens proprietatea cuiva, cu intenţia ca acea persoană să o păstreze, acesta nu este furt; trebuie să fie altceva. Cu secole în urmă, dreptul comun englezesc a dezvoltat infracţiunea de fraudă, care constă în a convinge pe cineva să își dea proprietatea sa prezentând pretenţii false, precum a-i spune unei persoane că în schimbul proprietăţii va primi titlu

de proprietate asupra Podului Brooklyn, spre exemplu. Frauda este cunoscută şi ca furt prin şiretlic [175, p.42].

În același timp ea reliefează și dificultățile de care se lovesc uneori anchetatorii atunci când infracţiunile cibernetice implică victime într-o ţară şi făptaşi în altă ţară, aceasta deoarece funcţionarii publici însărcinaţi cu supravegherea aplicării legii nu se pot baza pe procedurile pe care le folosesc de obicei pentru a găsi dovezi şi/sau a prinde făptaşii indigeni. Un mandat de arestare sau de percheziţie american nu are nicio altă valoare în altă ţară, în acelaşi fel în care un mandat francez nu are niciun efect legal în Statele Unite. Problema strângerii dovezilor şi a prinderii făptaşilor într-o altă ţară nu este specifică doar infracţiunilor cibernetice. De-a lungul istoriei, infractorii au fugit din jurisdicţia unde şi-au comis infracţiunile în efortul de a evita trimiterea în judecată şi primirea pedepsei. Ce este diferit în privinţa infracţiunilor cibernetice este frecvenţa cu care apare acest scenariu. Înainte era ceva neobişnuit, dar acum devine tot mai mult normal. Din păcate, legea nu a fost în pas cu această modă. Infracţiunile transfrontaliere creează două tipuri de provocări funcţionarilor însărcinaţi cu supravegherea aplicării legii. Una dintre acestea este strângerea dovezilor de peste graniţă, iar cea de a a doua este obţinerea custodiei suspectului din străinătate [175, p.141].

În fine, Franco Barresi și Michele Nigretti în cartea **Fenomeno hacking: analisi sociocriminnalistica dell intrtrusione informatica** precizează faptul că hackerii se consideră ca fiind un fel de eroi ai vremurilor noastre, cu obiectivul de bază de a elibera orice informație și comunicare de imprejmuirile rigide ale controlului si ale pieței, pentru posibilitatea ca oricine să aibă acces in mod liber liber la informație iar dreptul de a fi informat și de a informa să poată fi exercitat în orice moment [56, p.99].

Totodată, acești autori punctează asupra faptului că orice hacker care se respectă cunoaște sistemele și aplicațiile Microsoft, inclusiv numeroasele vulnerabilități ale acestora, dar lucrează cu GNU/Linux și cu free software, adică cu software gratuit [56, p.100], ca o formă de protest împotriva corporațiilor și a practicilor acestora de a îngrădi accesul la informație prin taxarea pentru achiziționarea aplicațiilor.

1.3. Concluzii la Capitolul 1

Pe marginea materialelor științifice reflectate în Capitolul I, secţiunile 1.1 şi 1.2 cu referire la analiza doctrinară a fraudei informatice putem desprinde următoarele *concluzii:*

1. În rândul cercetătorilor care s-au preocupat activ de abordarea și tratamentul infracțiunilor informatice, în speță a fraudei informatice, de elaborarea tezelor teoretice și problematicii legate de conţinutul normativ al infracțiunilor în cauză se enumeră: M. Dobrinoiu, Gh. Iu. Ioniță, C. Moise, I. Vasiu, L. Vasiu, I. A. Barbu, F. Encescu, O. Vară, G. Zlati, S. Brînză, V. Stati, Gh. Alecu, A. Barbăneagră, Айков Д.А., Зыков Д.С., Карабаналов С.С.,Тропина Т.Н.,Черных А.В., P .W. Singer, M. Streeter, C. E. Ch. Eastomm, J. Taylor, J. Taylor, G. Kirwan, A. Power, J. Sammons, F. Donovan, K. Bernier, R. Moore, S. W. Brenner, F. Barresi, M. Nigretti etc.

Este de menţionat că lucrările acestor autori consacraţi reprezintă baza teoretică a investigaţiei. Prezenta teză de doctorat vine să completeze studiile întreprinse anterior în domeniu, evidenţiindu-se unele tendinţe şi aspecte noi de dezvoltare a ştiinţei în domeniul de referinţă, specifice pentru etapa actuală de dezvoltare a societăţii.

2. Examinarea şi studierea aprofundată a problemei fraudei informatice ca parte integrantă a infracționalității informatice ne îndreptăţeşte să afirmăm că, în prezent, acest fenomen a fost cercetat direct sau tangenţial în conţinutul diferitor lucrări de specialitate expuse mai sus. Totodată, infractorii din domeniu, mai ales cei transnaţionali, sunt deosebit de ingenioşi, astfel încât, pe de o parte, ei îşi adaptează noile metode de comitere a infracţiunilor la realităţile timpului, iar, pe de altă parte, înseşi modalităţile faptice de activitate infracţională suportă şi ele o restructurare perpetuă. Prin urmare, dată fiind mobilitatea vădită ce caracterizează acest tip de criminalitate înseşi cercetările ştiinţifice în materie trebuie să aibă un caracter continuu.

3. În acelaşi timp, se face absolut necesară o reevaluare a conţinutului politicilor penale de prevenire şi de combatere a infracțiunilor informatice, inclusiv a fraudei informatice, prin prisma normativului penal în vederea relevării unor propuneri de *lege ferenda* care ar ţine pas noilor curente de gândire juridică şi politici promovate la nivel penal.

4. Prin urmare, scopul cercetării înfățișate în teza de doctorat constă în efectuarea, pe baza cercetărilor teoretice şi a materialelor empirice, a unei investigaţii complexe privind infracțiunea de fraudă informatică prin prisma cadrului juridic internațional aferent, normelor de incriminare a fraudei informatice din alte state, reglemăntărilor juridico-penale din România și Republica Moldova. Pe aceiaşi cale s-a urmărit formularea propunerilor de ameliorare a calităţii cadrului normativ-penal în materie şi a unor măsuri eficiente de reprimare a acestui flagel infracţional.

Atingerea scopului propus presupune realizarea următoarelor *obiective*:

- analiza lucrărilor ştiinţifice din doctrina penală autohtonă şi cea străină publicate la tematica problemei investigate;
- reliefarea fenomenului infracțional în domeniul informatic și caracterizarea acestuia;
- conturarea și tratarea modalităților tipice de comitere și făptuitorilor în cazul infracțiunilor informatice;
- abordarea sediului normativ-preventiv de incriminare a fraudei informatice: actelor internaționale de referință; normelor de incriminare a fraudei informatice din legislația altor state; reglementărilor antifraudă informatică și incriminarea faptei în legea penală a României și Republicii Moldova;
- analiza juridico-penală a conținutului legal, condițiilor preexistente, conținutului juridic și agravantelor infracțiunii de fraudă informatică potrivit legislaţiei penale a României şi Republicii Moldova;
- reevaluarea cadrului normativ-penal privind frauda informatică din legislaţia penală a României şi a Republicii Moldova;
- formularea recomandărilor ştiinţifice pentru îmbunătăţirea legislaţiei penale pe segmentul problematicii investigate.

2. FENOMENUL INFRACȚIONAL ÎN DOMENIUL INFORMATIC: DEFINIRE ȘI CARACTERIZARE

2.1. Preliminarii privind fenomenul infracțional în spațiul informatic

Infracțiunile informatice constituie noua provocare pentru sistemele de drept penal din lumea intreagă. Acest tip de infracționalitate apare din ce in ce mai pregnant in statisticile oficiale, in multe din aceste cazuri fiind asociat unor grupări criminale cu caracter organizat.

Dacă, inițial, infracționalitatea informatică a reprezentat o atitudine teribilistă de sfidare a securității rețelelelor informatice, treptat ea a devenit un instrument în săvârșirea celor mai grave infracțiuni, dând naștere unei veritabile piețe negre ale informațiilor piratate, ale furtului de identitate și ale violării dreptului de proprietate intelectuală, ale fraudării cardurilor bancare. Criminalitatea informatică are la bază, deopotrivă evoluția tehnologică fulminantă, în expansiune continuă, și trăsături umane vechi de când lumea: lăcomia, dorința de putere, de faimă, atașamentul de valori materiale (bani, bunuri), de lux, orgoliul etc. [13, p.250, 265].

Imaginea hacker-ului izolat de acum un deceniu, preocupat numai de a demonstra vulnerabilitațile sistemelor de operare este deja depașită, asta in timp ce goana după profit a devenit principala motivație a criminalilor informatici. Toate aceste lucruri se desfășoară în contextul globalizării, la care o contribuție indiscutabilă și-a adus-o insăși dezvoltarea fără precedent a tehnologiei informației, proliferarea calculatoarelor personale și a noilor dispozitive de comunicare tot mai inteligente precum și accesul tot mai facil la internet.

Există trei factori care concură la săvârșirea unei infracțiuni: o țintă adecvată, un infractor motivat și absența organelor de aplicare a legii. Toți acești factori, se regăsesc, de asemenea, și în cazul infracțiunilor informatice.

Astăzi nu doar instrumentele aferente ocupaţiei de infractor s-au schimbat – ci şi ţinta imediată. Pe vremuri banii erau „stocaţi” în formă de bancnote şi monede şi aceste entităţi fizice erau ceea ce căutau infractorii. Astăzi cantitatea de bani accesibili în formă de bancnote este mică în comparaţie cu banii care sunt stocaţi în modalitatea cea nouă – și anume cea electronică. Banii noştri sunt nişte simple cifre într-o bază de date. Pentru a obţine aceşti bani avem nevoie de informaţii – nume, adresă şi parole şi aşa mai departe – şi acesta este motivul pentru care una dintre preocupările principale ale infractorilor cibernetici este să pună mâna pe informaţiile noastre personale. Acestea servesc infractorilor drept poartă de intrare pentru a pune mâna pe banii noştri.

Modul în care ne păstrăm informaţiile personale se schimbă, de asemenea. Odată erau păstrate în fişete (safeuri), mai apoi pe calculatorul nostru de acasă. Acum este la fel de probabil să fie ţinute pe un telefon mobil sau alt dispozitiv portabil.

În mod inevitabil, infractorii s-au prins de această nouă modă şi sunt acum viruşi adresaţi în mod specific telefoanelor mobile şi dispozitivelor conexe. Este probabil ca această modă să ia amploare.

Consumatorii au adoptat telefonul inteligent ca pe o parte indispensabilă a vieţii lor; iar pentru un număr tot mai mare de persoane, este portalul preferat pentru internet. O modă dintre cele mai recente este încurajarea oamenilor de a-şi folosi telefoanele pentru a face plăţi online sau în magazine. Există o varietate de moduri de a face aceasta. Dar ideea centrală este că informaţii importante despre consumator – inclusiv parole şi detalii ale conturilor bancare – sunt cel mai probabil stocate pe acest aparat. Aceasta îi face pe posesori potenţial vulnerabili atacurilor cu programe informatice maliţioase.

În viață aproape orice poate fi utilizat într-un mod abuziv atunci când nimerește în mâinile unor oameni nepotriviți, iar internetul nu constituie sub nici o formă o excepție. În realitate, anonimitatea aparentă de care beneficiază utilizatorii atunci când navighează pe web și când folosește alte servicii internet lasă breșă unor utilizări improprii, imorale și ilegale.

Internetul este o rețea de calculatoare care comunică între ele pe bază de Transport Control Protocol Internet Protocol (TCP/IP). Aceasta este o rețea internațională de calculatoare interconectate, care permite oamenilor să comunice cu un altul în cyberspațiu și să acceseze mari cantități de informații din jurul lumiii [32, p.3].

Controlul internetului este dificil de realizat din cauza naturii sale și infrastructurii fizice, rețeaua fiind utilizată în principal de utilizatori privați care folosesc domenii diferite (spre exemplu, numele de domenii sunt administrate în S.U.A. de Internet Corporation for Assignet Names and Numbers – ICAN)..

Accesul la internet se realizează în baza unui abonament încheiat de o persoană fizică sau juridică; acesteia atribuindu-se o adresă IP corespunzând unui număr care facilitează identificarea fiecărui calculator care se află conectat la internet.

Internetul a creat o dimensiune virtuală unde comportamentul este cu mult mai liber și mai necontrolat decât în lumea reală.

Întrucât facilitează comunicarea și diifuzarea de informații la scară planetară, internetul favorizează comiterea de infracțiuni și apare ca fiind vectorul unei noi forme de criminalitate, în privința căreia aplicarea dreptului penal se străduiește să identifice autorii, având în vedere dimensiunea sa internațională [113, p.39].

Pana acum dreptul s-a ocupat de bunuri corporale deoarece lumea reala era inconjurata de obiecte tangibile: azi, in schimb, este in curs un adevărat proces de „dematerializare” prin raspandirea progresivă și de neoprit a programelor pentru calculator, circuitelor electronice, semiconductoarelor, datelor, informatiilor, frecventelor radio, numelor de domeniu si protocoalelor de transmisie [129, p.2].

Numărul mare de indivizi care accesează bazele de date a sporit vulnerabilitatea sistemelor, iar ocaziile de a face uz în mod abuziv sau de a le folosi în scopuri criminale nu au întârziat să apară, această activitate răsfrângându-se foarte accentuat în plan economic, precum și în planul securității umane, atingând uneori nivelul de terorism informatic [21, p.192-193].

Încă de la apariția sistemelor informatice și rețelelor de comuncații au fost căutate vulnerbilitățile acestora, fie în scopul îmbunătățirii performanțelor și siguranței în exploatare fie în scopul compromiterii lor [66, p.13].

De-a lungul timpului s-a demonstrat că internetul este un sistem vulnerabil, iar acest lucru combinat cu avantajele oferite de el (stocarea, procesarea si transmiterea de cantități imense de date, accesibilitate, usurința in utilizare, independența de distanță, posibilitatea unor aplicații in domeniul afacerilor) au creat un cadru favorabil pentru activități criminale determinand apariția unui nou fenomen infracțional - criminalitatea informatică.

Spațiul cibernetic nu trebuie confundat cu internetul real (ca rețea), ci trebuie privit ca însumând aspectele psihologice și sociale pe care i le conferă, prin utilizare, psihicul uman individual și societatea în ansamblu. Acesta cuprinde, prin urmare, identitățile și obiectele care există în rețelele de computere folosite de indivizii umani în diverse scopuri [44, p.166].

Infractorii cibernetici eludează limitările fizice care guvernează infracțiunile din lumea reală, aceasta deoarece nu este necesară proximitatea fizică între victimă și făptuitor. Infracțiunea cibernetică este o infracțiune fără limitări, victima și făptuitorul putând fi în orașe, state sau chiar țări diferite.

Spaţiul cibernetic, ca viaţa de altfel, se află într-o continuă dezvoltare. Combinaţia hibridă de tehnologie şi fiinţe umane care folosesc tehnologia este în perpetuă schimbare, modificându-se implacabil totul de la mărimea şi întinderea spaţiului cibernetic la regulile tehnice şi politice care urmăresc să îl ghideze. Aşa cum s-a exprimat un expert, „geografia spaţiului cibernetic este mult mai mutabilă decât cea a altor medii. Munţii şi oceanele sunt greu de mutat, dar porţiuni din spaţiul cibernetic pot fi activate sau inactivate printr-o simplă apăsare de buton” [153, p.14].

Un element important al infracţiunii cibernetice este acela că – în general, dar nu întotdeauna – faptele infracţionale sunt înfăptuite din depărtare, existând deci o distanţă între infractor şi victimă. Aşadar, de exemplu, cineva care disemineză un virus de calculator – o infracţiune cibernetică clasică – ar putea face aceasta de pe plaja mărginită de palmieri a unei insuliţe îndepărtate, la multe sute de kilometri distanţă de cea mai apropiată potenţială victimă a sa [153, p.2].

Tot ce are nevoie un infractor cibernetic este un computer conectat la internet. Astfel, un infractor cibernetic poate, spre exemplu, să extragă fonduri dintr-un cont bancar american și să le mute in conturi din zone mai profitabile din punct de vedere fiscal din alte țari, cu puțin efort si mai puțină vizibilitate.

Infracțiunea cibernetică este automatizată, iar cu ajutorul automatizării infractorii pot comite mii de infracțiuni cu maximă rapiditate și minim de efort. Prin automatizarea proceselor infractorii pot pune la cale escrocherii care se bazează pe un număr mare de infracțiuni, dar care generează o pierdere relativ mică pentru fiecare victimă. Astfel ei pot obține un profit destul de însemnat și cu riscuri mai reduse deoarece cu cât mai scăzuta este fiecare pierdere,cu atât este mai mare probabilitatea ca victima să nu raporteze infracțiunea.

Un singur individ în cazul acestor tipuri de infracțiuni poate victimiza un număr extrem de mare de persoane, fapt care este mai puțin intâlnit in lumea reală. Deși este săvârșită de un procent mic al populației unei societăți, acest mic grup poate comite infracțiuni la o scară care depășește cu mult ceea ce ar putea realize ei în lumea reală, unde de regulă unui infractor îi corespunde o victimă, deci este un raport biunivoc.

Drept urmare, numărul infracțiunilor cibernetice va depăsi simțitor numărul infracțiunilor din lumea reală, fapt care va eroda abilitatea organelor însărcinate cu aplicarea legii de a reacționa eficient la infracțiunile individuale, aceasta cu atât mai mult cu cât infracțiunea cibernetică nu înlocuiește infracțiunea din lumea reală, ci se va adăuga acestor infracțiuni, care se vor întâmpla cu frecvența obișnuită.

Încălcarea legii este, din nefericire, o parte atotprezentă a societăţii moderne, iar lupta care are loc în fiecare societate între cei care comit infracţiunea şi cei care caută să prevină, să detecteze sau să pedepsească activitatea infracţională este într-o continuă schimbare, atât în ceea ce priveşte rata de succes cât şi natura activităţilor. Oamenii petrec tot mai mult timp online, folosind o varietate de programe şi dispozitive pentru a păstra legătura unii cu alţii şi a efectua diferite activităţi atât pentru locul de muncă cât şi pentru relaxare. Această creştere continuă a timpului petrecut online şi a tipurilor de activităţi efectuate online, de la comunicare la tranzacţii financiare şi distracţie, este ceea ce a condus la cele mai recente forme ale acestei lupte [75, p.28-29].

Entitățile care suportă consecințele infracțiunilor informatice pot fi cele mai diverse –statul și instituțiile statale, societățile comerciale, instituții bancare, oameni de afaceri etc. Astfel, victime ale infracțiunilor informatice pot fi atât persoanele fizice cât și persoanele juridice, iar cercetările efectuate relevă că marea majoritate a victimelor provin din sectorul bancar și din cel al asigurărilor [102, p.341-342].

În doctrină este propusă următoarea clasificare a victimelor infracțiunilor informatice [3, p.236-237]:

- persoanele care utilizează rețeaua internet de puțin timp – persoanele care utilizează rețeaua internet de puțin timp nu conștientizează faptul că sistemele lor informatice pot să fie afectate de viruși prin simpla deschidere a unui attachement de e-mail sau prin accesarea unui site web care conține programe malițioase; de asemenea persoanele care utlizează rețeaua internet de puțin timp

demonstrează lipsa lor de experiență în mediul online prin comunicarea cu ușurință cu diferite persoane necunoscute de ele;

- persoanele naive care utilizează internetul – persoanele foarte tinere și cele vârstnice reprezintă țintele preferate ale infractorilor. Persoanele tinere au o concepție deformată asupra lumii, având în vedere mediul protejat în care s-au dezvvoltat. În spațiul virtual tinerii nu conștientizează faptul că există persoane care pot să le producă un prejudiciu, transformându-i în victime. Persoanele vârstnice nu sunt familiarizate cu utilizarea tehnologiei informațieișisi comunicațiilor, această situație creând posibilitatea ca acestea să devină victime sigure ale infractorilor în cyberspațiu. De cele mai multe ori când persoanele în vârstă cad victime ale comportamentului criminal din cyberspațiu, acestea ar putea ezita să raporteze infracțiunea comisă în mediul online organelor de punere în aplicare a legii, datorită sentimentului de rușine pe care acestea îl încearcă, în urma victimizării lor în cyberspațiu;

- persoanele defavorizate sau cu dizabilități – persoanele cu dizabilități fizice și psihice pot să devină ținte ale infractorilor din cyberspațiu, iar cu scopul de a identifica potențialele victime, infractorii din cyberspațiu caută aceste persoane în bazele de date online și se alătură grupurilor de discuții ce sunt create pentru susținerea acestor persoane cu dizabilități. Grupurile de discuții reprezintă un mijloc de interacțiune socială și o sursă de prietenie pentru persoanele cu dizabilități;

- persoanele disperate, singure sau cu alte nevoi emoționale – persoanele disperate reprezintă victime sigure pentru infractorii din cyberspațiu. Astfel, aceste persoane ar putea căuta dragostea în mediul online în zone greșite, cum ar fi de exemplu; diferite site-uri web matrimoniale nesigure, ar putea solicita cu disperare ajutorul prin intermediul grupurilor religioase de pe internet, ori ar putea avea nevoie mare de bani sau de alte nevoi urgente emoționale sau fizice.

Infractorii informatici devin oameni bogați ai zilelor noastre. Unele firme sau organizații nu sesizează pierderile cauzate de atacurile informatice, fie pentru a nu da curaj și altora să încerce, fiind deja un precedent, fie de teama de a nu fi trase la răspundere pentru că nu au luat cele mai bune măsuri de asigurare a securității, fie pentru a nu face publicitate negativă aplicațiilor folosite. Cu calculatorul s-au înfăptuit cele mai multe „crime perfecte” [139, p.299].

Până acum, infracțiunea cibernetică nu a schimbat înclinația oamenilor spre omor, tâlhărie sau viol in lumea reală, ba mai mult se poate vorbi în prezent de o congruență între infracțiunile informatice și infracțiunile așa numite tradiționale.

Sunt infracţiunile cibernetice pur şi simplu nişte variante mai electronice ale vechilor infracţiuni din „lumea reală” sau sunt infracţiuni noi? Este o întrebare bună şi răspunsul este – în cele mai multe cazuri – primul. Furtul de identitate este o infracţiune cibernetică, aflată exact în centrul acestor tip de infracţiuni, implicând folosirea detaliilor personale ale altcuiva pentru a dobândi accesul în locuri nepermise – asumarea identităţii unei alte persoane în scopul dobândirii accesului la banii sau la alte valori ale sale. Aceasta însă nu este ceva nou, de vreme ce infractorii au folosit asemenea tehnici

încă de la începuturi. Cu toate acestea, practica modernă de a pune atât de multe informaţii personale şi financiare pe calculatoare, pe dispozitive de stocare de date şi online a transformat furtul de identitate într-o infracţiune mult mai uşoară şi, prin urmare, mai profitabilă. Este mult mai sigură şi pentru infractor, deoarece îşi poate asuma identitatea cuiva aflat în cealaltă parte a lumii, reducând şansele de a fi prins la aproape zero.

În lumea reală există persoane care pătrund în case și pot lua tot ce găsesc valoros. În lumea virtuală există indivizi care pătrund în sistemele informatice și fură toate datele valoroase. La fel cum în lumea reală există oaspeți nepoftiți și persoane care simt plăcere atunci când își însușesc sau distrug proprietatea altora, lumea calculatoarelor nu putea fi lipsită de acest fenomen. Este cu adevărat detestabilă perfidia acestor atacuri. Căci dacă se poate observa imediat lipsa cutiei cu bijuterii, o penetrare a serviciului de contabilitate poate fi depistată după câteva luni, atunci când toți clienții au renunțat la serviciile firmei deoarece datele furate și ajunse la concurență au ajutat-o pe aceasta să le facă oferte mai bune.

În general, putem afirma că infracţiunile cibernetice sunt în mare parte forme tradiţionale de infracţiuni care utilizează instrumente moderne. La urma urmelor, la un anumit moment în trecut, hoţii la drumul mare au trecut de la folosirea cuţitelor la arme de foc, astfel că nu ar trebui să ne surprindă dacă, în secolul al XXI-lea, unii dintre ei îşi actualizează metodele folosind calculatoarele. Esenţa infracţiunilor rămâne aceeaşi: oameni răi care ne vor banii, indivizi care vor să-şi facă victime, sau societăţi şi companii care vor să fure secretele concurenţilor lor.

Viteza cu care este comisă o infracțiune informatică, volumul datelor sau sumele implicate, distanța în raport cu locul comiterii infracțiunii sunt elementele care o diferențiază în comparație cu criminalitatea tradițională. Specific infracțiunilor informatice sunt următoarele caracteristici esențiale care se transformă în avantaje reale conferite făptuitorilor [127, p.12]:

- caracterul transfrontalier - acest fenomen nu ia în considerare granițele convențional stabilite;
- anonimitatea - făptuitorul nu trebuie să fie prezent la locul faptei;
- credibilitatea - făptuitorul creează aparența unei afaceri legale și corecte;
-rapiditatea - conferită de transmiterea aproape instantanee a datelor prin sistemele informatice;
- costurile foarte reduse în comparație cu beneficiile ce pot fi obținute.

Îmbrăţişând întâi calculatoarele, iar mai apoi internetul, lumea a adoptat o tehnologie bazată pe codul calculatorului, acesta fiind un limbaj care poate fi adaptat sau rescris de către alții pentru activități suspecte.

La început, nu s-a realizat faptul că se lucra cu o tehnologie imperfectă; pur şi simplu, nu s-a luat în considerare posibilitatea de a face ceva rău utilizând codul calculatorului. Astfel, de la bun început, lumea calculatorului şi a internetului s-a bazat pe imperfecţiuni, defecte şi uneori pe procese

prost înţelese. Am putea chiar numi acest fapt „păcatul originar” al internetului. În cele din urmă, nu doar cercetătorii în domeniul informaticii au ajuns să exploateze aceste defecte, ci şi infractorii.

Deja era însă prea târziu. Până la începutul secolului al XXI-lea lumea modernă a devenit înspăimântător de dependentă de uzull calculatorului şi de internet. De la maşini la utilităţi publice, de la centralele atomice la clădirile în care locuim şi muncim, toate se bazează pe lumea digitală pentru a funcţiona. Din nefericire, permiţând pătrunderea imperfecţiunii în sistem de la început, creatorii acestei lumi au permis de asemenea şi pătrunderea infractorilor, teroriştilor şi a statelor paria (care nu se conformează convenţiilor internaţionale). Aceste grupuri au învăţat să exploateze slăbiciunile tehnologice care stau la baza vieţii noastre zilnice, în moduri despre care suntem în mare parte neştiutori. Infracţiunea cibernetică este astăzi o ameninţare la însăşi modul nostru de viaţă.

Acest lucru este provocat de faptul că sistemele informatice nu constituie doar ținta unor infracțiuni ci și instrumentul prin care sunt săvârșite alte infracțiuni, sau doar înlesnesc prin funcțiile lor săvârșirea mai facilă a infracțiunilor tradiționale.

În acest context, multe dintre investigațiile unor infracțiuni tradiționale (indiferent de natura acestora) vor include sistemele informatice ce pot conține date despre motivația, identitatea, locația, conexiunile autorilor sau complicilor, și care pot ușura finalizarea respectivelor investigații [66, p.10].

Rezultă din toate acestea o suprasarcină pentru organele legii, coroborat cu faptul că resursele pe care le au la dispoziție sunt minimal adecvate pentru a lupta cu infracțiunile din lumea reală, dar totodată total inadecvate pentru a lupta împotriva infracțiunilor cibernetice. O altă piedică o constituie faptul că deși organele abilitate depistează infracțiuni cibernetice, tendința este ca acestea să nu fie clasificate într-o categorie separată. Astfel, spre exemplu, frauda online este adeseori inclusă în categoria generală a fraudei, motiv pentru care lipsește documentația adecvată.

Modelul polițienesc clasic, bazat pe principiul că organele insărcinate cu aplicarea legii trebuie să reacționeze adecvat la o infracțiune, are mult mai puțină eficiență impotriva infracțiunii online deoarece reacția poliției incepe de obicei cu mult după ce infractiunea cibernetică a fost finalizată cu succes.

Urmele lăsate, asa cum sunt ele, nu mai sunt deci proaspete. O altă mare problemă constă în aceea că, acțiunile infracționale au loc intr-un mediu electronic, iar dovezile sunt fragile și volatile. Până in momentul in care poliția ajunge să reacționeze, s-ar putea ca unele dovezi sau chiar toate dovezile să fie distruse.

Deoarece infractorii cibernetici nu sunt prezenți in mod fizic la “locul” crimei, prezumția că ca ei ar fi putut fi observați in timp ce se pregăteau, comiteau infracțiunea sau fugeau de la locul faptei nu este valabilă. În fapt, este posibil ca ofițerii de investigații să nu poată determina locația din care fâptașul a comis infracțiunea sau cine este acesta. Spre deosebire de corespondenții lor din lumea reală, infractorii cibernetici ramân adesea anonimi [175, p.171].

Internetul fiind un spațiu aflat in continuă schimbare, investigațiile privind infracțiunile informatice trebuie să se desfașoare cu maximă celeritate pentru a se putea obține probe relevante [134, p.14].

Totodată, este adevărat că în domeniul informaticii, comportamentele infracționale nu se supun nici unui determinism social; delicvenții pot avea foarte bine 10 ani sau 60 de ani, să fie novici sau profesioniști. Autorii infracțiunilor informatice sunt adesea, oameni obișnuiți, dar pot fi și persoane cu aptitudini și talente excepționale. Având un minimum de calificare și stimulat de sfidarea tehnică, dorință de câștig, celebritate sau răzbunare, ori având motive ideologice, acesta poate deveni chiar periculos [113, p.33].

În ceea ce privește caracteristica infractorilor cibernetici, distingem anumite trăsături comune celor care recurg la comiterea de acte antisociale [48, p.53]: instabilitate emoțional-afectivă, inadaptabilitate socială, insatisfacție materială sau afectivă, comportament duplicitar și dialect infracțional.

Cunoașterea structurii psihice a infractorului este necesară întrucât numai astfel se poate determina eficiența măsurilor ce trebuie dispuse față de acesta [182, p.63].

Nici un stat care are acces la internet nu este ferit de aspectele nocive produse de infractorii informatici și este de presupus că o dată cu creșterea exponențială a conexiunilor de internet, acest tip de amenințare va cunoaște și el un trend ascendent. Spre deosebire de informația imprimată pe hartie, informația in formă electronică poate fi potențial furată de la distanță și este mult mai ușor să fie interceptată și modificată [99, p.153].

Există totuși și un aspect pozitiv in creșterea numărului infractorilor care utilizează tehnologia, și anume implicarea computerelor in realizarea infracțiunilor a dus la o abundență de dovezi digitale care pot fi folosite pentru a acuza și condamna infractorii. În această epocă modernă este dificil să ne imaginăm o infracțiune care sa nu aibă și o dimensiune digitală. Infractorii, violenți sau deopotrivă stilați, se folosesc de tehnologia existentă pentru a-și facilita atingerea scopului infracțiunii sau pentru a evita incriminarea, generând astfel noi provocări pentru avocați, judecatori, procurori si criminaliști. Teroriștii folosesc internetul pentru a comunica, a recruta, a spăla banii și comite furturi de pe cardurile bancare,a solicita informații și distribui material propagandistice.

În consecință, Serviciul vamal al S. U. A., ca rezultat al extinderii traficului de droguri, pornografiei infantile, spălării banilor și a altor mărfuri ilegale tranzacționate cu ajutorul internetului, a ajuns să verifice fiecare computer din S. U. A. conectat prin internet [52, p.3] . Bazele de date se află pretutindeni si pot fi accesate foarte facil in orice investigatie. Este foarte probabil dealtfel ca cineva implicat intr-o infractiune să fi folosit un computer, un dispozitiv electronic mobil sau să fi accesat internetul. Din acest motiv, orice investigație organizată trebuie să ia in calcul informațiile relevante stocate in sistemele computerelor folosite de către suspecți.

Internetul permite nu numai manipularea informației dar este și o unealtă privilegiată pentru a răspunde zvonurilor sau oricărei forme de intoxicare sau campanie de destabilizare. De asemenea, sunt facilitate activitățile de spionaj și de informare, deoarece au devenit ușor de interceptat informațiile transferate pe internet [80, p.22].

Problemele asociate infracțiunilor informatice au ajuns să fie tot mai mult discutate in fiecare țară a lumii - chiar și in țări care nu sunt cunoscute pentru un nivel inalt de dezvoltare și competențe tehnologice deosebite. Natura mondială a acestui tip de criminalitate a ridicat probleme referitoare la aspecte precum jurisdicția.

În unele cazuri este astăzi foarte dificil să se determine cine are autoritatea de a investiga o infracțiune informatică. Spre exemplu, o persoană care traiește in Rusia are posibilitatea de a transmite o imagine pornografică infantilă in Statele Unite. În această situatie cine are jurisdicția? Rusia? Poate că sub incidența legii rusesti, tânăra din imagine a avut varsta legală pentru a-și da consimțământul. A fost atunci comisă vreo infracțiune in ochii functionarului public rus insărcinat cu respectarea legii? Sau au Statele Unite jurisdicția? Transmiterea imaginilor cu minori este ilegală, dar persoana in cauză nu a atins niciodată pamântul Americii. Poate să fie luată in considerare folosirea liniilor telefonice americane atunci cand se examinează dacă există jurisdicție pentru o investigație? Toate acestea sunt intrebări importante la care nu se poate răspunde ușor [164, p.6-7].

Dificultatea rezultă din faptul că internetul se confruntă cu o eterogenitate de sisteme juridice la scară globală; ceea ce este incriminat într-una dintre țări nefiind neapărat și în alta. Acest fapt constituie un impediment în cooperarea judiciară internațională, fără de care o reprimare eficientă a fenomenului nu are sorți de reușită.

Există insă un nivel crescut de dezbatere si de discuții intre liderii mondiali pe masură ce tot mai multe entități internationale ajung să conștientizeze pericolele criminalității informatice.

In ceea ce privește definiția infracțiunii informatice, nu există o definiție standard in acest moment, operându-se mai multe accepțiuni și tratamente.

Conform unei opinii, formulată de Eoghan Casey, o *infracțiune informatică* ar fi *o infracțiune care implică un computer în următoarele moduri* [52, p.40]:

- computerul ca instrument al infracțiunii - în acest caz computerul este folosit ca un mijloc de angajare în activitatea infracțională. Un exemplu din această categorie ar fi o persoană care folosește computerul pentru a sustrage fonduri din contul unei companii;

- computerul ca focalizare a infracțiunii. Aici, computerul este folosit ca țintă urmărită de activitatea criminală și nu este neaparat folosit în comiterea actului. Cel mai bun exemplu în acest caz îl constituie individul care intră prin efracție într-un magazin de computere,după orele de program, cu intenția de a fura computere și echipamente conexe;

- computerul ca loc de stocare a dovezilor. Aici, persoana implicată in actul infracțional nu a furat computerul și nici nu l-a folosit ca mijloc de a comite vreo infracțiune, dar a stocat dovezi pe computer, cum ar fi păstrarea evidențelor asupra infracțiunilor comise pe hard-disk.

În această ordine de idei infracțiunea vizează sistemul informatic sub următoarele aspecte:

- sistemul informatic țintă a infractorilor – situația în care infractorii doar accesează sistemele informatice sau își însușesc ilegal (conținutul) informațiile stocate pe acestea: spre exemplu informațiile personale, clienții, planurile de marketing, aproape tot ce prezintă valoare comercială și este stocat pe discul dur (HDD);

- sistemul informatic instrument al infracțiunilor – situația în care infractorii accesează sistemele informatice fiind interesați de procesul prin care pot comite o altă infracțiune și nu de informațiie stocate pe acesta, spre exemplu folosirea unei parole pentru accesarea unui cont și transferarea respectivelor fonduri;

- sistemul informatic facilitează comiterea discretă a altor infracțiuni – situație în care infractorii utilizează sistemele informatice pentru comiterea mai ușoară a infracțiunilor care care ar putea fi comise și fără ajutorul acestora, spre exemplu; spălarea de banilor, pedofilia etc.;

- sistemul informatic furnizează în mod direct comiterea infracțiunilor – situația în care infractorii se folosesc direct de sistemele informatice pentru comiterea altor infracțiuni, spre exemplu: piratarea programelor, contrafacerea componentelor etc[167, p.28].

Este de remarcat că unele organizații, cum ar fi Departamentul de Justiție al S.U.A. și Consiliul Europei folosesc termenul de cybercrime (infracțiune cibernetică) cu referire tot la fenomenul de criminalitate informatică. Astfel, prin infracțiune cibernetică s-ar intelege orice infracțiune care implică un computer si o rețea informatică.

În ceea ce privește *clasificarea infracțiunilor informatice*, acestea pot fi grupate în [65, p.50]:

A. *Infracțiuni împotriva confidențialității, integrității și disponibilității datelor și sistemelor informatic*e:

- accesarea ilegală;
- interceptarea ilegală;
- afectarea integrității datelor;
- afectarea integrității sistemului;

B. *Infracțiuni informatice*:

- falsificarea informatică;
- frauda informatică;
- furtul de identitate;
- abuzurile asupra dispozitevelor;

C. *Infracțiuni referitoare la conținut*:

- interacțiunea cu material pornografic (în țările unde este incriminat ca infracțiune);

- pornografia infantilă;

- actele de natură violentă, rasistă sau xenofobă;

-actele care privesc convingerile religioase (în țările unde este incriminată ca infracțiune);

- jocurile de noroc ilegale online;

- atacurile cu mesaje nesolicitate tip spam;

D. *Infracțiuni referitoare la atingerile aduse drepturilor de proprietate intelectuală*:

- încălcarea drepturilor de autor și a drepturilor conexe;

- încălcarea drepturilor de proprietate industrială;

E. *Infracțiuni complexe*:

- terorismul informatic;

- războiul informatic:

Există o mare varietate a clasificării infracțiunilor informatice și nu există un consens în această privință, iar clasificarea de mai sus are drept bază prevederile Consiliului Europei privind criminalitatea informatică din 23/11/2001, clasificare pe care o vom susține și noi.

2.2. Modalități tipice și făptuitori în cazul infracțiunilor informatice

În trecut, atunci cand apăruse termenul **hacker**, era ceva obișnuit ca oamenilor să le răsară in minte imaginea unui adolescent pipernicit, cu aspect de tocilar stând in fața computerului său și jucând jocuri video. Astăzi, ar fi insă problematic și incorect ca oamenii să creadă că doar adolescenții se angajează in comportamente ca cele ale hackerilor. Adevarul este că sunt mulți care se implică in hacking in mod regulat, si de multe ori acești făptași, mai inaintați in varstă și nu adolescenții, săvârșesc fapte daunătoare computerelor și rețelelor.

De-a lungul timpului **hacking-ul –** o primă modalitate tipică de comitere a infracțiunilor informatice, inclusiv a fradei informatice - a parcurs patru etape [55, p.13]: prima generație (anii 1970) ce a fost condusă de nevoia de cunoaștere, a doua generație (începutul anilor 1980) a fost condusă de curiozitate și de nevoia de cunoaștere, iar mai târziu (1985-1990), hacking-ul a devenit o tendință; a treia generație (anii 1990) a devenitt o activitate obișnuită, condusă de curiozitate, stabilind rețele și schimbând informații; a patra generație (începând cu anul 2000 și până în prezent) condusă de dorințe și bani, în această etapă hacking-ul întâlnindu-se cu activitatea politică și cu activitatea criminală.

Originea termenului poate fi trasată până la Massachussets Institute of Technology (MIT) – Institutul de Tehnologie din Massachussets, acesta fiind unul dintre primele instituții din Statele Unite care a oferit cursuri de informatică și programare a computerului. Se crede că termenul a fost folosit pentru prima dată de către membrii Laboratorului de Inteligență Artificială de la MIT.

Aceste persoane nu erau infractori, fiiind o echipă de cercetare extrem de bine pregatită și devotată muncii ei. Aceasta nu inseamnă ca aceste persoane nu au violat regulile universității, ei incălcând in mod constant procedurile universității privitoare la numărul orelor in care un computer putea fi folosit. Membrii grupului au inceput să se autonumească hackeri deoarece erau capabili să ia programe de computer și să le facă să execute acțiuni pe care cei care au conceput programul software nu le-au intenționat [164, p.18]. Se crede că termenul s-a dezvoltat ca un fel de farsă, în special datorită emoției frenetice ce-i încerca atunci cand „tocau" (verbul *to hack* in limba engleza are sensul originar de a toca, a ciopârți, a sparge, a știrbi) tastaturile ore in sir.

Primii hackeri au folosit intruziunile într-o modalitate care era benefică din punct de vedere social, respectiv ca o practică care să-i ajute să priceapă cum funcționează sistemul informatic, astfel că la începutul anilor 60-70, hackingul era pentru mulți studenți echivalentul funcțional al unui studiu aprofundat privind calculatorul.

Ce este un hacker? La prima vedere pare o întrebare foarte ușoară, cu un răspuns simplu și clar, de genul indivizi diabolici, pe care-i vezi la tv sau despre care citești în ziare, acuzați că au spart sistemul informatic al unei bănci, au reprogramat sateliți militari, au lansat viruși informatici ș.a.m.d [100, p.5].

Deși tot mai multă literatură tratează natura malefică a hackerilor, hackerii originari au fost niște intelectuali interesați în a determina cât de departe puteau fi duse programele de calculator. Ei au fost entuziaștii erei calculatoarelor cu o nevoie permanentă de a învăța cât mai mult despre profunzimile tehnologiilor înalte. Când previziunile lor despre mersul tehnologiei informatice s-au adeverit, unii dintre ei au devenit bogați. Termenul de haker a rămas relativ obscur până ce infracțiunile comise prin computer au ajuns să castige mai multă publicitate în mass-media.

În general, hakerii par să fie conștienți de faptul că accesarea neautorizată a unui sistem informatic reprezintă o activitate ilegală. Totuși, hackerii nu sunt conștiensi de implicațiile financiare ale atacurilor lor. Ei nu consideră că pătrunderea neautorizată într-un sistem informatic în scopul de a studia modul cum sistemul informatic funcționează și de a testa limitele acestuia reprezintă o acțiune ilegală. Aceștia sunt de părere că marile companii producătoare de softwaee nu pot fi considerate victime, deoarece acestea încearcă să manipuleze cunoștințe științifice și beneficiază de informații care ar trebui să fie accesibile liber și în mod gratuit [3, p.272].

Hackerii au fost întotdeauna un grup marginalizat de societate. În școli hackerii sunt văzuți ca tocilari (engl. „geeks"), singuratici (engl. „loners") sau nesociabili. Fiind parte a unei culturi subterane, de cele mai multe ori se fac analogii între grupurile de hackeri și organizații criminale.

Hackerii au următoarele motivații [161, p.15-19]:

- curiozitatea intelectuală – hackerii doresc să învețe cum funcționează rețelele și sistemele informatice și de asemenea, să dobânsească noi cunoștințe referitoare la securitatea informatică;

- pasiunea pentru tehnologie când motivația hackerilor se bazează pe exploatarea sistemelor informatice, însă fără a avea ca scop afectarea acestora;

- amuzamentul – hackerii care accesează neautorizat sisteme informatice pentru amuzament nu urmăresc obținerea unor avantaje financiare, ci doar simpla pătrundere neautorizată în sistemul informatic al unei persoane;

- îmbunătățirea sistemelor informatice – mulți hackeri doresc să contribuie la îmbunătățirea performanțelor sistemelor informatice. De asemenea, aceștia doresc să crească și nivelul de securitate al sistemelor și rețelelor informatice;

- lupta pentru libertate – mulți hackeri consideră activitatea de hacking ca fiind un instrument de luptă împotriva problemelor politice și sociale. Hacking-ul este folosit în special împotriva eventualelor încălcări asupra principiilor care guvernează lunea online și împotriva atacurilor săvârșite în lumea fizică pe care hackerii o consideră coruptă. Hackerii doresc să apere dreptul la informare al oricărei persoane, determinând informația să circule liber și să fie accesibilă pentru oricine;

- spiritul de revoltă – hackerii prin acest tip de motivație doresc să-și demonstreze superioritatea lor față de autoritpțile publice prin pătrunderea neautorizată în sistemele și rețelele informatice ale acestora;

- atragerea atenției și faima – unii hackeri simt nevoia să facă cunoscute succesele obținute în activitatea lor, în scopul de a deveni celebri și de a atrage atenția mass-mediei;

- furia și frustrarea – furia și frustrarea îi poate determina adesea pe hackeri să săvârșească anumite fapte, pe care în mod normal nu le-ar săvârși, din cauza acestor tulburări emoționale;

- motive politice – unii hackeri încearcă să implice comunitatea hackerilor în politică;

- evadarea din mediul familial și din societate – pentru a scăpa de un mediu familial conflictual, de o viață de izolare și singurătate și pentru a se detașa de realitățile sociale, hackerii își găsesc un refugiu în pasiunea lor pentru computere;

- motive profesionale – există hackeri care desfășoară activități de hacking nu numai din motive legate de pasiune, ci și ca urmare a unor motive profesionale, cum ar fi, de exemplu spionul industrial, agentul guvernamental etc.;

- profiturile financiare – majoritatea hackerilor au ca motivație infracțională obținerea de câștiguri financiare.

Aproape fără excepție, majoritatea ignorantă îi consideră pe hackeri persoane extrem de periculoase care provoacă pagube extrem de mari în cel mai scurt timp posibil și unui număr cât mai mare de persoane [139, p.306].

Hackerul este o persoană care pătrunde într-un calculator, o reţea de comunicaţii sau o bază de date. Aceasta foloseşte internetul şi programele de calculator pentru a găsi punctele slabe ale sistemului de apărare al victimelor sale şi îşi face cale de intrare. Odată pătrunsă, ea poate folosi alte

programe pentru a trimite înapoi informaţii-cheie sau pentru a distruge ori a dezactiva sistemele, în funcţie de motivaţia pe care o are.

Dar hackerii nu folosesc doar tehnologia; ei adesea se bazează pe abilităţi umane pentru a depista parole sau alte informaţii folositoare care să le permită pătrunderea într-un sistem. În mod tipic, ei contactează personalul organizaţiei ţintă şi obţin informaţii care ar putea fi folositoare în depistarea parolelor şi codurilor, probabil pretinzând că sunt angajaţii unei companii client, prietenii sau rudele unui angajat sau furnizori.

Acestui tip de subterfugiu i s-a dat numele destul de pompos de „inginerie socială". De exemplu, infractorul ar putea studia site-ul web şi documentele publice ale unei companii pentru a obţine numele managerilor şi apoi să sune la companie pretinzând a fi noul tehnician IT. Acesta ar putea spune persoanei care răspunde la telefon că trebuie să-şi aducă la zi calculatorul de la distanţă, dar că şi-a pierdut parola şi să ceară apoi foarte politicos parola de la interlocutor.

Din punctul de vedere al securităţii, ingineria socială poate fi contracarată numai prin educarea salariaților sau utilizatorilor unui sistem. Este important ca toţi utilizatorii să fie avizaţi cu privire la tacticile ingineriei sociale şi să evite să le cadă în plasă.

Hackerii tradiţionali spun că scopul lor primordial este să desfacă ceva pentru a afla cum funcţionează şi pentru a vedea dacă îl pot îmbunătăţi sau adapta scopurilor lor.

Tot ei sunt de părere că mass-media și populația nu înțeleg fenomenul de hacking. Conform părerii hackerilor, oamenii au o imagine deformată față de ei, iar adeseori oamenii nutresc un sentiment de ură față de aceștia. Hackerii nu se consideră o amenințare pentru economia și bunăstarea unei țări, ci mai degrabă aceștia se consideră ca fiind o resursă datorită abilităților și cunoștințelor lor în domeniul securității sistemelor și rețelelor informatice. Totodată, ei nu se consideră infractori, ci mai degrabă apărători ai drepturilor omului, fiind de părere că adevărații infractori sunt persoanele care blochează accesul la informații și la cunoaștere, mediul online trebuind să fie caracterizat și prin accesibilitate.

Hackingul este o sarcină complexă care necesită un nivel înalt de cunoştinţe tehnice. De obicei nu se rentează să se depună efort pentru pătrunderea într-un calculator dintr-o locuinţă privată. Hackingul cel adevărat este folosit în mod tipic asupra calculatoarelor pe care este probabil să existe datele personale ale mai multor oameni, precum cele din şcoli, bănci, spitale, baze de date ale corporaţiilor etc

Ideea cea mai importantă de înţeles în legătură cu hackingul este că acesta nu este o sarcină uşoară. Deşi multe filme au făcut să pară că un hacker poate obţine acces în sisteme informatice deosebit de sigure în câteva minute, lucrul acesta pur şi simplu nu este adevărat. Hackingul este foarte asemănător spargerii: cu cât ţinta este mai sigură, cu atât va fi necesară mai multă îndemânare şi timp pentru infiltrare. Şi ca în cazul spargerii, infiltrarea în sistemele sigure necesită un grad înalt de

îndemânare şi cunoaşterea în profunzime a mai multor domenii. De exemplu, un spărgător iscusit va trebui să înţeleagă lăcătuşeria şi sistemele de alarmă; în mod similar, un hacker iscusit va necesita o înţelegere desăvârşită a sistemelor de operare, a reţelelor informatice şi a contramăsurilor de siguranţă [19, p.11].

Conform unei opinii, avem o clasificare a hacking-ului în hacking din afara si hacking dinăuntru [175, p.50].

Hacking-ul din afară este foarte asemănător din punct de vedere conceptual cu încălcarea proprietății din lumea fizică, acest lucru concretizându-se in accesul neautorizat al unei persoane la un calculator. Astfel, în acest tip de hacking, o persoană din afară accesează in mod intenționat un calculator sau un sistem computerizat fără a fi autorizat să facă aceasta.

Hacker-ul trebuie să știe că nu este autorizat să acceseze sistemul, dar acest lucru nu constituie in general o problemă, deoarece este extraordinar de dificil, dacă nu imposibil, să se facă hacking in mod accidental.

În mod similar celor care explorează o proprietate in lumea fizică, acești călcători virtuali ai proprietății violează cel puțin dreptul exclusiv al proprietarului de a hotărî cine are acces la proprietatea sa. Chiar dacă demersul lor ar fi doar unul inofensiv și motivat doar de curiozitate, ceea ce nu prea este valabil astăzi, aceștia pot cauza daune suplimentare proprietarului modificând sau ștergând din neglijență datele din sistemele asupra cărora acționează prin hacking.

Hacking-ul dinăuntru se petrece atunci când o persoană autorizată să acceseze o parte a unui sistem computerizat depășește sfera acelei autorizări și practic intră fraudulos în alte părți ale sistemului. Dacă hacking-ul din afară este definit drept dobândirea de acces neautorizat la un sistem computerizat, hacking-ul dinăuntru este conceput a fi depășirea accesului autorizat la un astfel de sistem.

Personalul sistemului are dreptul să urmărească bunul mers al programelor, al prelucrăriii fișierelor, al asigurării protecției, situație în care dacă nu sunt loiali sistemului, pot constitui pericolul cel mai mare. Această categorie nu apelează la tehnici prea performante deoarece desfășurându-și activitatea în interiorul sistemului pot înfăptui acte criminale cu mijloace mult mai simple [139, p.298].

Cele trei categori de bază ale atacatorilor din interior sunt: angajaţii nemulţumiţi, cei motivaţi financiar (hoţii) şi utilizatori care cauzează daune în mod neintenţionat.

Angajaţii nemulţumiţi pot crea probleme prin publicarea de informaţii pe reţeaua web pentru competitori sau alţi angajaţi (de exemplu, salariul tuturor angajaţilor). Angajaţii nemulţumiţi ar putea, de asemenea, să instaleze o bombă logică care va provoca daune sistemului informatic în cazul în care ei ar înceta să mai lucreze în companie.

Atacatorii din interior motivaţi financiar vor abuza de activele companiei sau vor manipula sistemul cu scopul de a fura.

Există atât ameninţări din interior intenţionate cât şi neintenţionate. Exemplele de ameninţări involuntare includ utilizatorii care şterg fişiere neintenţionat cauzând pierderea muncii respective sau afişează în mod accidental documente secrete pe sisteme publice cauzând ceea ce este cunoscut drept scurgere de informaţii.

În domeniul informaticii se întâmplă frecvent să li se dea încredere a priori angajaților subalterni, cărora li se conferă mari responsabilități, fără a fi supuși unei supravegheri și fără să li se ceară explicații cu privire la aceste responsabilități. Este foarte important ca în contractul de angajare sau în fișa postului să fie introdusă o clauză de asigurare a siguranței informațiilor și obligația de respectare a confidențialității [113, p.38].

Din moment ce riscul apare ca o consecință a activităților răuvoitoare sau subsersive sau din erori neintenționate, se poate estima că factorul uman constituie un adevărat călcâi al lui Ahile al sistemelor informatice.

Tipologia infractorilor. Infractorii cibernetici nu reprezintă doar o schimbare de nume în ceea ce privește abordarea infracțiunilor tradiționale într-o formă nouă. Infractorii digitali, ca dealtfel și faptele comise de aceștia, reprezintă o transformare fundamentală în felul nostru de a aborda problema crimei și a criminalității [181, p.58].

Noile categorii de infracțiuni care formează acum un nou tip de criminalitate, sunt comise tot de oameni, tot cu vinovăție, și au în vedere, de regulă, realizarea unor beneficii patrimoniale [139, p.301].

Autorii si cercetătorii clasifică hackerii intr-o varietate de grupuri, însă in această lucrare ne vom insuși clasificarea lui R. Moore și vor fi imparțiți in șase categorii: hackerii cu pălărie neagră, hackerii cu pălărie albă, hackerii cu pălărie gri, copilași copiatori (script kiddies), hactiviști, teroriștii informatici și spionii cibernetici.

Hackerul cu pălărie neagră este tipul de infractor cel mai temut de opinia publică. Este genul de individ care violează securitatea computerelor pentru nimic altceva decât câștigul personal sau din malițiozitate. Această formă de hacker scrie programe care să avarieze sisteme si rețele de calculatoare. Acestei categorii i se datorează faptul că securitatea computerelor si fabricarea programelor antivirus au devenit ocupații full-time care costă companiile din toată lumea milioane de dolari, deoarece specialiștii in cauză sunt plătiți pentru a pune la punct rețele și sisteme de operare mai bine protejate. Ei sunt cunoscuți îndeobște și sub numele de crackeri.

Hackerul cu pălărie albă este exact opusul celui cu pălărie neagra, principalul său obiectiv fiind să furnizeze programe de securitate a computerului care vor proteja sistemele de la a fi penetrate ilegal și cu rea intenție .Adeseori acest tip de hackeri își publică programele lor de securitate a computerului pe internet sau prin companii de software ca un mijloc de a-i proteja pe ceilalți de vulnerabilitățile sistemului pe care ei le-au descoperit. Și acești hackeri vor căuta totuși computere-

țintă in care vor incerca mai apoi să intre neautorizat, însă odată ce reușesc, ei își vor inceta in mod normal activitatea și il vor alerta pe proprietarul computerului despre vulnerabilitatea in cauză [7, p. 60].

Hackerul cu pălărie gri reprezintă o combinație intre primele două tipuri, cel mai bun mod de a descrie aceasta clasă de hackeri este de a-i numi oportuniști. Dacă un hacker cu pălărie gri caută pe internet o țintă și reușește să obțină acces intr-un computer, acesta va notifica proprietarul sistemului. Însă, in loc să spună administratorului cum a fost exploatat sistemul, hackerul cu palarie gri va alege in mod normal să se ofere să repare defecțiunea pentru o anumită sumă de bani.

O altă tactică frecvent folosită de acest gen de hackeri era ca unul dintre membrii unui grup să obțină accesul ilegal într-un computer, iar apoi să recomande administratorului sistemului respectiv ca unul dintre prietenii săi, sau chiar el, să fie angajați pentru a securiza sistemul.

La începuturile hackingului, nu era ceva neobişnuit ca cineva care fusese condamnat pentru o infracţiune informatică să devină ulterior un consultant în securitatea calculatoarelor. Raţionamentul era că această persoană ştia cu siguranţă cum să compromită sistemele informatice şi putea ajuta la securizarea lor. Punctul de vedere alternativ era că această persoană avea în mod clar probleme etice, deoarece îşi dovedise deja disponibilitatea de a încălca legea.

S-a argumentat, de asemenea, că aceşti foşti infractori nu erau probabil cei mai performanţi căci, la urma urmelor, au fost prinşi. Argumentele pentru şi împotriva folosirii foştilor infractori au devenit mai puţin relevante în ultimii ani. Există acum experţi în securitate versaţi în tehnicile de compromitere a sistemelor informatice, care nu şi-au folosit niciodată cunoştinţele pentru a comite infracţiuni. Posedarea cunoştinţelor tehnice la înalt nivel asociată cu integritatea şi caracterul demn de încredere sunt esenţiale pentru profesionistul în securitatea calculatoarelor. Este foarte puţin probabil în prezent ca un fost infractor informatic să primească un post legat de securitatea calculatoarelor

Deși aceasta poate părea o formă de șantaj, in lumea afacerilor asemenea decizii pot ține de analiza costurilor și beneficiilor. Dacă este într-adevăr mai ieftin să angajezi respective persoana decât să pierzi datele sau să nu mai poți utilize rețeaua de calculatoare, atunci este foarte probabil ca firma să ofere un post acelei persoane. Recent, această practică a suferit un declin deoarece tot mai multe firme au optat să dea in judecată asemenea persoane.

Script kiddies sunt considerați a se afla la nivelul cel mai de jos al scării de hacking. În general, ei au puține competențe de programare a calculatorului sau acestea le lipsesc cu desăvârșire. Acești script kiddies (rom. „novici care preiau scenarii”) și-au caștigat numele prin abilitatea de a naviga pe internet in căutarea unor programe utilitare ale hackerilor, pe care apoi le lansează asupra unui computer țintă. Acest tip de hacker este foarte periculos deoarece acesta nu are nici cea mai vagă idee despre felul in care programul va afecta computerul asupra căruia este lansat atacul.

Uneori sunt numiți și vandalii Internetului. EI sunt de regulă tineri – adesea adolescenți – care au puţine abilităţi de programare sau deloc şi care în cea mai mare parte folosesc instrumentele de programare create de către alţii pentru a comite infracţiuni precum desfigurarea site-urilor şi lansarea (rareori scrierea însă) a viruşilor de calculator.

Sunt persoane care folosesc pur şi simplu instrumente ce pot fi găsite pe internet, având puţină metodologie sau tehnică judicioasă. Ei au multe şi variate motivaţii pentru a începe activitatea de hacking. Unii caută experienţă socială şi vor încerca să se alăture unui grup de hackeri (unele grupuri solicită dovada abilităţii de a face hacking înaintre de a acorda statutul de membru), altora le place provocarea sau vor să câştige un anumit statut în cadrul comunităţii de hackeri, iar alţii o fac din curiozitate şi o privesc drept o formă de divertisment [115, p.29-30].

Hactivistul este o persoană care face hacking ca mijloc de a răspandi un mesaj politic. Acești indivizi se disting de celelalte categorii sus menționate prin prisma motivației lor. Majoritatea atacurilor hactiviste implică transformarea paginii web, adică situația in care un hacker reușește accesul la un server care stochează pagina web, iar apoi modifică pagina pentru a afișa propriul său mesaj. Multe organizații teroriste angajează hactiviști pentru a prelua pagini web foarte populare și a le inlocui cu informații despre cauza susținută de grupul respectiv.

Astăzi, apariţia aşa-numitului „hactivism", cu alte cuvinte a activităţii de hacking cu o motivaţie politică, a arătat unde au hotărât să se poziţioneze anumiţi descendenţi ideologici ai hacker-ilor originari – prin încălcarea legii pentru ceea ce ei văd a fi nişte motive justificate, care nu le servesc decât lor înşile. Dintre diferitele grupuri care operează în prezent – şi acestea sunt într-o continuă dezvoltare, dispărând şi apoi reapărând – două bine-cunoscute grupuri sunt Anonymous şi Lulzsec. Ambele grupuri au ieşit în evidenţă prin atacarea şi pătrunderea prin hacking în site-urile companiilor şi organizaţiilor pe care le dezaprobă. Acestea au inclus în țintele lor Biserica Scientologică, site-uri de pornografie infantilă, Departamentul de Justiţie al Statelor Unite, F.B.I.-ul, Pentagonul, guvernul ugandez, guvernul sirian, ziarul britanic *The Sun* şi multe altele.

Teroristul informatic reprezintă convergența nefastă dintre spațiul cybernetic și terorismul clasic și se referă la un individ ce își foloseste abilitatea de hacking pentru a instala un sentiment de frică in populație, el atacând de regulă o porțiune din infrastructură de importanță critică. Infrastructura de importanță critică se referă la utilități precum purificarea apei, uzinele electrice sau centralele nucleare. Cu alte cuvinte ei vor ataca sisteme care deservesc domenii vitale cum ar fi alimentația, industria energetică, transporturile aeriene, industria farmaceutică, incercand să cauzeze pagube sau chiar decesul unor oameni și slăbirea economiei unei țări.

Conform unei definiții a F.B.I.-ului, terorismul informatic ar fi atacul premeditat, motivat politic, împotriva informațiilor, sistemelor de calculatoare, programelor și operărilor de date ce

conduce la violențe împotriva obiectivelor civile și necombatanților, atac exercitat de grupări subnaționale sau agenți clandestini" [94].

Doctrina definește terorismul informatic ca fiind difuzarea premeditată, metodologică și motivată ideologic de informații, înlesnirea comunicării, sau atacul împotriva informațiilor în format digital, sistemelor și programelor informatice, ce necesită o planificare din timp în scopuul de a produce un prejudiciu social, material, fizic și moral țintelor necombatante și publicului, sau orice răspândire de informații care este destinată să faciliteze realizarea acestor acțiuni [135, p.152-153].

Sau, confom unei alte opinii a unui analist american [42, p.1], terorismul informatic reprezintă convergența terorismului cu spațiul cibernetic. El se referă la atacurile și la amenințările de atac împotriva computerelor, rețelelor informatice și informațiilor stocate, săvârșite pentru a intimida sau a constrânge un guvern sau poporul său în scopul susținerii obiectivelor politice sau sociale ale grupării teroriste.

Dacă există suspiciuni că astfel de activități sunt sprijinite din umbră de guvernele unor țări, se poate ajunge la un veritabil război informațional,asa numitul „information warfare", acesta referindu-se la activitățile întreprinse de guverne, grupuri sau persoane, pentru a obține acces la sistemele de informații din alte țări, fie în scopul obținerii datelor din sistem, manipulării sau fabricării datelor, sau chiar prăbușirii acelui sistem pentru o perioadă de timp [62, p.27].

Conform unei alte definiții, acesta se referă la atacurile motivate politic săvârșite asupra tehnologiei informației și comunicațiilor în scopul de a accesa neautorizat sistemele și rețelele informatice ale unei țări, organizații sau grupuri cu intenția de a comite acte de spionaj sau de sabotaj [120, p.479-481].

Activitățile sus menționate se pot înfăptui atât în timpul unor războaie reale, dar și în timpul așa ziselor războaie reci. Războaiele informaționale implică nu doar calculatoarele, ci și informațiile sub orice formă și transmisia lor pe orice cale.

Spionii cibernetici - dacă hackerii ideologici sunt motivaţi de conştiinţa lor, spionii cibernetici acţionează din patriotism sau pur şi simplu deoarece se află pe statul de plată al guvernului lor. Spionajul, strângerea şi analiza informaţiilor secrete nu sunt ceva nou. Dar de când a început ceea ce am putea denumi era „războiului informaţiilor" şi dependenţa masivă a societăţilor moderne de sistemele digitale pentru a păstra în funcţiune iluminatul, apa şi majoritatea facilităţilor moderne, spionul cibernetic a devenit o achiziţie indispensabilă oricărui guvern. Aceşti spioni – a căror calificare principală este priceperea lor la calculatoare şi scrierea programelor informatice – nu caută doar să spioneze alte guverne, ci iau parte şi la spionajul industrial pe o scară largă şi globală.

Informația a devenit o proprietate națională vitală, ce are o valoare strategică, dacă nu este protejată poate fi cucerită sau distrusă. Problema numărul unu a sfârșitului de secol este cum să se asigure protejarea informațiilor atunci când sunt lansate în rețele. Ca urmare a acestui fapt, infowar-ul

a devenit o posibilitate reală, computerele și alte mijloace de informație transformându-se în ținte. Câmpul de luptă preferat este internetul, al cărui caracter deschis permite statelor (care fie că recunosc, fie că nu) să sponsorizeze hackerii care pătrund în computerele altor state și interceptează comunicațiile digitale. Cel care poartă războiul digital înarmat cu tastatură și cu „șoarecele", în fața terminalului său conectat la rețea, riscă foarte puțin să fie prins. Riscul de a fi detectat este și mai mic, iar cel de a fi condamnat este aproape nul [97, p.19-20].

Nu cunoaştem prea multe despre spionii cibernetici individuali angajaţi de guverne. Ei îşi petrec timpul în tăcere, în spatele unor uşi închise, investind ore nesfârşite în depistarea surselor ameninţărilor, punerea la cale a unor atacuri sau indicarea cu precizie a victimelor potenţiale. Aceasta este mai cu seamă adevărat în China, care este acuzată de – ceva ce ea neagă cu tărie – angajarea unor mari numere de hackeri, fie direct sau indirect prin companii aflate în proprietatea statului.

Vestul are şi el proprii spioni cibernetici, iar, într-o măsură tot mai mare, naţiunile vestice sunt mai deschise cu privire la ei. De exemplu, în Statele Unite, Universitatea din Tulsa oferă un curs de doi ani în spionarea cibernetică. Studenţii, care sunt învăţaţi cum să scrie viruşi de calculator, să pătrundă în reţele, să spargă parole şi să extragă date din diferite tipurii de dispozitive digitale, sunt adesea recrutaţi mai târziu de către Agenţia Naţională de Securitate sau C.I.A. Site-ul universității arată că a primit aproape 15 milioane de dolari de la Fundația Națională de Știință începând cu anul 2001 pentru „Programul Trupelor Cibernetice" pe care îl desfăşoară. Site-ul îl citează pe Dickie George, directorul tehnic de asigurare a informaţiilor la Agenţia De Securitate Naţională a Statelor Unite, ca spunând: „Ceea ce ne trebuie astăzi sunt războinici cibernetici de elită şi aceasta este ceea ce produce acest program" [154, p.82].

Solicitanţii cursului au variat mult în vârstă, de la 17 la 63 de ani. De asemenea, provin din medii diferite. Un număr semnificativ sunt veterani militari în timp ce alţii sunt profesionişti care caută o a doua carieră. Cursuri similare se ţin la Universitatea Statală Dakota din Dakota de Sud, Universitatea de Nord-Est din Boston şi Şcoala Navala Postuniversitară din California.

Pe lângă cursurile pentru potenţiali spioni cibernetici, agenţiile de informaţii din Vest îi monitorizează pe toţi tinerii care le atrag atenţia printr-o pricepere extraordinară la calculatoare, programe informatice şi internet. Există două motive pentru care agenţiile vestice fac acest lucru. Unul este pentru că aceşti tineri pot alege să-şi folosească aceste abilităţile tehnice deosebite în scopuri necinstite sau să fie abordaţi de către infractori şi să sfârşească prin a se muta în „tabăra întunecată". Un alt motiv este că aceasta este o formă de recrutare de talente – copiii minune ai calculatorului cu un potenţial uriaş pot fi recrutaţi de către serviciile de securitate.

Modul de operare al hackerilor specific pregătirii infracțiunilor informatice. Înțelegerea modului de operare al hackerilor, precum și a uneltelor pe care aceștia le folosesc va fi benefică in misiunea de a preveni proliferarea criminalității informatice. Mulți oameni trăiesc cu impresia că

activitătile legate de hacking sunt desfășurate din siguranța casei hackerului și implică numai computerul și internetul. Adevărul este însă că de multe ori incidentul de hacking va fi precedat de o etapă investigativă numita pre-hack [164, p.27].

Alegerea țintei este primul pas al etapei pre-hack. Acum, hackerul va hotărî ce calculator sau rețea va ataca. Se iau in considerare numeroși factori in cursul acestei etape, insă acești factori s-au modificat in ultimii ani pe masură ce tot mai multe companii s-au mutat pe internet. În trecut, majoritatea firmelor își mențineau toate conexiunile de rețea prin intermediul liniilor telefonice. Dacă un hacker reușea sa obțină accesul la numărul de telefon și o parolă atunci calculatorul era ușor de exploatat.

Astăzi, de regulă hackerii folosesc port scannere, acestea fiind pachete de software care scanează rețelele de calculatoare pentru a determina dacă vreun computer are setate porturi deschise.

Un port este canalul prin care computerul primește date din rețea. Deoarece aceste porturi permit informației să circule în și din computere, ele sunt, de asemenea o cale prin care hackerii câștigă accesul la un computer, iar odată ce preia controlul asupra computerului, rețeaua este la dispozitia hackerului [7, p.183].

Al doilea pas al etapei pre-hack este cunoscută drept faza de cercetare și adunare de informații. Aceasta este faza in care hackerul va contacta ținta in speranța de a câștiga informații care il vor ajuta la penetrarea sistemului. Astfel, spre exemplu, poate contacta administratorul de sistem sub pretextul de a fi un utilizator legitim, care nu mai poate avea acces la internet.

Dacă ținta este o firmă, hackerul poate pretinde a fi un nou angajat temporar care are probleme in accesarea sistemului. Companiile mai mari care mențin un volum mare de muncă temporară pot avea instalate parole presetate pentru situații in care un angajat va face parte din companie numai numai pentru o scurtă perioadă si va avea nevoie de acces doar la un spațiu limitat de retea.

Problema este că, odată ce hackerii au orice fel de acces la rețea, este doar o chestiune de timp pană când vor câștiga un nivel mai mare de acces care le va permite să facă ajustări la sistem. Mulți hackeri vor folosi in același timp această oportunitate ca un mijloc de a instala o parolă backdoor (rom. „pentru ușa din dos”) care le va permite să se intoarcă in rețea cand le este lor convenabil [164, p.28]. Acesta este de fapt un program instalat de atacatori după accesul neautorizat la un sistem informatic pentru a se asigura că ei pot continua să aibă acces nerestricționat la sistemul informatic, chiar dacă metoda lor inițială de acces a fost descoperită și blocată.

Odată ce stadiul de cercetare a fost finalizat, hackerul va incepe operațiunea propriu- zisă de hacking a calculatorului sau a rețelei. La inceperea atacului de hacking, potențialul hacker va recurge la utilizarea trusei de scule a hackerilor, o colecție de software necesară pentru a dobândi accesul entry-level room (rom. „la nivelul de intrare”).

Dacă acesta a fost obținut, atunci hackerul va incerca să obțină un nivel mai inalt de acces, care este uneori numit root acces (rom. „acces la rădăcină”). De aici și numele trusei de scule care se mai numește și *rootkit*. Acesta reprezintă un set de instrumente software folosite de atacator pentru a pătrunde într-un sistem informatic, a obține privilegii speciale în scopul efectuării de funcții neautorizate, și după aceea să ascundă toate urmele prezenței sale [43, p.102]. Orice trusă de scule a unui hacker trebuie să conțină articole cum ar fi: password grabber-e (rom. „șterpelitoare de parole”) și key logger-e (rom. „inregistratoare de taste”), sau packet snifer-e (rom. „adulmecătoare de pachete”) [164, p.30].

Password graber-ele si logger-ele reprezintă programe care pot fi plantate pe un calculator - țintă și pot rula in fundal fără cunoștiința proprietarului computerului. Cele două programe au in comun faptul că acestea sunt instalate pe un computer ca un mijloc de inregistrare a fiecarei taste apăsate de utilizatorul computerului țintă și de urmărire a activității utilizatorului prin capturi de ecran a tot ceea ce se întâmplă pe calculator. Apăsările tastelor sunt inregistrate intr-un fișier text special stabilit de catre hacker și ascuns undeva pe hard discul computerului țintă.

Metodele cu ajutorul cărora are loc procesul de keylogging sunt software, adică, după cum am văzut, există programe care pot fi instalate pe computerul utilizatorului fără ca acesta să aibă cunoștiință, dar și hardware, adică echipamente fizice care nu numai că nu pot fi detectate de programul antivirus, insă pentru un utilizator obișnuit, însăși reperarea lor vizuală reprezintă o sarcină dificilă.

Astfel, există keylogger usb, adică un dispozitiv mic care se conectează între mufa tastaturii și mufa calculatorului. Odată conectat între mufa tastaturii și mufa calculatorului, keylogger-ul va începe automat să inregistreze fiecare apăsare de buton a tastaturii. Pentru a vedea ce s-a tastat se va apăsa o combinație secretă de taste pentru a accesa memoria dispozitivului, astfel încât numai utilizatorul care are combinația corectă de taste va putea să îl acceseze .Este dificil de observat pentru un ochi neavizat deoarece are o lungime de numai 38 mm și este de aceeași culoare cu mufa tastaturii. Nu scoate nici un sunet și nu are nici un bec. Cu ajutorul lui se poate afla printer altele ce s-a vorbit pe messenger și ce pagini web au fost vizitate, totodată poate afla și memora parolele folosite de utilizator.

În afara infractorilor cibernetici, acesta este utilizat și de companiile preocupate de obiceiurile de muncă ale angajaților lor, acestea folosind aceste programe pentru a se asigura că angajații nu își urmăresc treburile personale in timpul de lucru.

Este un instrument care este util infractorilor cibernetici pentru pregătirea săvârșirii unor infracțiuni precum transferul neautorizat de date informatice, interceptarea ilegală a unei transmisii de date informatice sau fraudei informatice.

Packet sniffer-ul este un software de calculator proiectat să „adulmece” pachetele de date in timp ce informațiile sunt transferate prin rețea. Când cineva trimite un e-mail sau chiar solicită o

pagina web, informațiile trimise inapoi spre computer sunt in mod normal prea mari ca sa fie transmise toate deodată. Datele, sunt prin urmare, fragmentate in pachețele mai mici de date, ceea ce permite un transfer mai rapid de informații.

Odată ce intreaga colecție de pachete de date ajunge la computerul destinatar, fișierul original este reconstruit folosindu-se informațiile stocate in secțiunea de inceput a fiecărui pachet mai mic. Un packet sniffer este instalat pe o rețea și programat să examineze toate pachetele care trec prin aceasta. Utilizatorii acestor programe sunt, in general, cei care incearcă să fure parole sau informații de pe carduri de credit de pe site-urile comerciale [164, p.34].

Programe de acest tip pot fi folosite și în mod legal de către administratorii de rețele sau sisteme informatice pentru îmbunătățirea funcționării sau securității acestora sau uneori reprezintă chiar părți integrate ale sistemelor de operare, însă de multe ori astfel de programe sunt utilizate și de către atacotori în capturării informațiilor transmise între calculatoare

Este un instrument foarte des utilizat de către infractori, mai ales în cazul pregătirii infracțiunilor de interceptare ilegală a unei transmisii de date informatice, dar își arată utilitatea și în cazul comiterii fraudelor informatice.

Tehnici utilizate de hackeri în cazul infracțiunilor informatice. Instrumentele mai sus menționate sunt folosite pentru obținerea accesului intr-un computer sau o rețea țintă. Întrebarea care rămâne este: ce vor face hackerii odată ce au reușit accesul la un sistem țintă. Vor survola doar rețeaua si vor vedea ce informații sunt disponibile in sistem, vor fura informații din sistem, sau vor avaria și distruge sistemul? Răspunsul la aceste intrebari depinde in mare masură de tipul de hacker care a facut o breșă in sistem.

Atacurile la care recurg hackerii odată ce au accesul intr-un sistem pot varia de la atacuri sacâitoare care lansează date pe internet in incercarea de a forța un computer sa iasă offline, până la viruși de calculator care distrug date valoroase. În continuare vom aprofunda unele dintre aceste tehnici.

Manipularea datelor, aceasta referindu-se la procesul prin care o persoană schimbă sau șterge date dintr-un computer ca un mijloc de a cauza daune proprietarului acelui computer-daune care nu sunt de natură fizică, in schimb au aproape intotdeauna consecințe financiare.

O posibilă situație pentru acest tip de atac ar fi aceea a unor foști angajati care isi folosesc codurile de securitate pentru a dobandi acces la evidențe bancare si apoi transferă banii într-un cont bancar unde banii nu pot fi detectați. Tehnica rotunjirii sau a salamului (cum este denumita uneori datorita efectului sau de „feliere") este un exemplu de manipulare de date care implică informații financiare. Se inserează în secret in retea sau în computer instrucțiuni legate de programul software și când au loc schimbări in conturile bancare, programul va rotunji depozitele și va transfera fondurile in

exces într-un cont separat. Odată ce contul a atins un anumit nivel, banii pot fi transferati intr-un cont separat [164, p.37].

Este vorba despre o tehnică des utilizată în cazul comiterii unor infracțiuni precum alterarea integrității datelor informatice sau fraudei informatice.

Calul troian reprezintă un program care in mod aparent efectuează o acțiune folositoare, dar în fapt el efectuează acțiuni de distrugere care nu sunt cunoscute de utilizator [37, p.326].

Numele lor îsi are originea din epopeea Iliada lui Homer.de la calul de lemn care a reușit să intre pe poarta cetății Troia sub forma unui cadou în timpul bătăliei. Acest program reprezintă o metoda de inserare a unor instrucțiuni intr-un program, astfel încat programul va efectua o funcție neautorizată, in timp ce in aparență execută una obișnuită [2, p.145].

Deci, există posibilitatea ca un program legitim, dar obținut din surse suspecte, să fie alterat prin plasarea unor instrucțiuni neautorizate în cuprinsul său, instrucțiuni care execută funcții secundare necunoscute de utilizator [66, p.35].

Altfel spus, un troian informatic este un program informatic despre care utilizatorul crede că va realize un lucru și care poata să facă sau nu acel lucru, dar care va face cu siguranță altceva, ce nu este acceptabil pentru utilizator [98, p.100]. Spre exemplu, utilizatorul poate descărca un fișier cu muzică, un joc de pe un site web, sau un program de editat poze. Desigur,ne-am aștepta să putem juca jocul mult așteptat sau ca programul să fie util, dar atunci când îl vom deschide în locul lui se va dezlănțui un cal troian.

Calul troian poate efectua urmatoarele operațiuni: ștergerea sau modificarea fișierelor, transmiterea fișierelor prin rețea la atacator sau instalarea in sistemul informatic de alte programe si viruși. Troienii, spre deosebire de viruși sau viermi, nu se pot răspândi singuri.

Astfel încât acesta își arată utilitatea în comiterea unor infracțiuni informatice cum ar fi alterarea integrității datelor informatice sau perturbarea funcționării sistemelor informatice.

Programele malițioase (engl. *malware*) - cuvântul *malware* în limba engleză este o combinaţie între *malicious* (rom. „maliţios”) şi *software* (rom. „program informatic”) iar el denotă un program informatic care este conceput pentru a se infiltra sau a produce stricăciuni într-un computer fără cunoştinţa şi consimţământul proprietarului. Sunt multe tipuri de programe maliţioase, dar două sunt mai familiare: viruşii şi viermii

Virușii informatici sunt de fapt programe care infectează fișierele executabile ale unui computer. În general ei este atașați unui program, care poate ajunge in calculatorul atacat prin e-mail, transfer de fișiere și mesagerie instantanee. Orice program care se multiplică fără acordul utilizatorului este un virus.

Creatorii de viruși se bazează pe curiozitatea și pe disponibilitatea oamenilor de a accepta fișiere de la persoanele pe care le cunosc sau cu care lucrează, transmițând fișiere dăunătoare mascându-le ca fișiere benigne sau atașându-le unor asemenea fișiere [174, p.330].

De obicei un virus se atașează la un fișier astfel incat virusul rulează in memorie sau in sistemul de operare de fiecare data cand sistemul execută fișierul infectat [2, p.143], Odată ce virusul a infectat un computer prima sa sarcină este de de a se multiplica el insuși prin răspandirea către alte sisteme informatice.

Virușii informatici pot genera următoarele efecte: distrugerea unor fișiere, modificarea dimensiunii fișierelor, ștergerea totală a informațiilor de pe hard disc, inclusiv formatarea acestuia, încetinirea vitezei de lucru a calculatorului până la blocarea acestuia, diverse efecte grafice sau sonore inofensive [88].

Totodată, dintre consecințele unui virus mai am putea menționa trimiterea unor mesaje de e-mail către toate adresele existente în Adress Book, înregistrarea tuturor informațiilor tastate (utilizată pentru furtul de parole și numerelor de cărti de credit).

Daunele provocate de un virus poartă numele de *payload* (încărcatură virală). Declanșatorul încărcăturii virale este condiția sau evenimentul care activează virusul, care pot fi o dată calendaristică, rularea unui anumit program sau uneori chiar conectarea la internet.

Un virus prezintă trei caracteristici: un mecanism de replicare, un mecanism de activare și un obiectiv.

Mecanismul de replicare trebuie să îndeplinească funcțiile următoare [176, p.69]:

- caută alte programe pentru a le infecta;

- când găsește un program determină dacă acesta a mai fost infectat anterior,verificând dacă mai prezintă semnătura acelui virus;

- inserează instrucțiunile ascunse undeva în interiorul programului;

- modifică secvența de execuție a programului infectat astfel încât codul ascuns să fie executat ori de căte ori programul este folosit;

- creează o semnătură pentru a indica că programul a fost infectat, acest lucru fiind necesar deoarece fără această semnătură programele ar putea fi în mod repetat infectate și ar crește mult în dimensiuni, fapt care ar da de gândit.

Mecanismul de activare verifică dacă a avut loc un anumit eveniment sau dacă s-a întamplat o condiție .Când aceasta are loc, virusul își execută acțiunea dăunătoare. În cazul în care mecanismul de activare verifică dacă a fost atinsă o anumită dată pentru a executa obiectivul se spune că virusul este o bombă cu ceas (time bomb). Dacă verifică existența unei condiții (cum ar fi dacă programul a fost executat de mai multe ori) se spune că virusul este o bombă logică (logic bomb).

Ca și un virus biologic, un virus informatic are un ciclu de viață. Acesta include următoarele etape: creare (de către un programator), activare (virusul se lansează în execuție), detectare (virusul este descoperit,începe studierea acestuia), asimilare (producătorii de software antivirus include semnătura noului virus in tabelul de semnături) și eradicare (programele antivirus elimină virusul) [179, p.175-176].

Problema virușilor a preocupat cercetătorii din domeniul informatic și îi va preocupa, probabil multă vreme, atât timp cât vor mai exista calculatoarele și cei care încearcă să obțină diferite avantaje din folosirea lor. Preocupările pe această linie nu vin numai din partea celor angajați oficial în rezolvarea necazurilor care apar, mai ales pentru contracarea efectelor provocate de infestarea sistemelor cu viruși, ci, în special, din partea atacatorilor, care deseori sunt mult mai bine pregătiți [45, p.301].

Virușii sunt utilizați de către infractorii cibernetici pentru comiterea unor infracțiuni cum ar fi: alterarea integrității datelor informatice, perturbarea funcționării sistemelor informatice sau fraudei informatice.:

Viermii informatici (worms) sunt adesea confundați cu virușii informatici, însă chiar dacă activitatea programată poate fi similară (spre exemplu, ștergerea sau modificarea informațiilor), există o diferență importantă: viermii informatici nu au nevoie de un program gazdă pentru a se reproduce sau lansa in execuție [98, p.103].

Viermii informatici pot poza ca ceva interesant pentru utilizator cum ar fi un videoclip al unei formatii cunoscute. Dacă virușii se propagă bazându-se in special pe ignoranța sau neatenția utilizatorilor care deschid și lansează in execuție programe găsite pe internet sau fișiere dubioase atașate mesajelor, viermii se raspândesc in mod automat.

Emailul reprezintă una dintre cele mai folosite metode de împrăștiere a viermilor informatici. De obicei,imbracă forma unui email cu atașament (o poză sau un fișier text) , iar când utilizatorul rulează acest atașament,viermele va infecta calculatorul. După ce calculatorul este infectat,viermele va încerca să găsească alte adrese de email pe calculator (de obicei in fișierele de configurare ale clienților de email) și se va transmite automat la toate adresele pe care le găsește. pornind astfel un nou ciclu [91].

Trebuie precizat că virușii, viermii informatici și troienii poartă numele generic de *malware,* făcându-se referire aici la orice soft nociv care a fost creat cu scopul de a rula în mod neautorizat și ascuns față de utilizatorul computerului.

Viermii informatici pot fi utilizați în comiterea unor infracțiuni informatice precum alterarea integrității datelor informatice, perturbarea funcționării sistemelor informatice sau fraudei informatice.

Rețelele bot, adică acea situație când cineva preia controlul asupra computerului utilizatorului prin intermediul unui troian, vierme sau virus informatic. Prin intermediul acestora, atacatorul poate

prelua controlul computerului infectat de la distanță și se poate folosi de acesta pentru a răspândi viruși, a trimite spam sau chiar a comite fraude. Programele bot transformă calculatoarele inocente, precum cele folosite de persoane individuale sau companii, în calculatoare infectate.

Computerul infectat este cunoscut sub denumirea de "zombie". Cand sute, mii sau zeci de mii de computere zombie se află sub controlul unui atacator se creează un botnet [2, p.147]. Rețeaua bot este, în esența o armată de zombii digitali. Creatorii unei astfel de rețele poartă numele de botherderi, aceștia punând la dispoziția infractorilor armatele lor digitale în vederea desfășurării unor atacuri planificate.

Mulţi oameni continuă să-şi utilizeze calculatorul fără să realizeze că a devenit parte a unei reţele bot, deşi adesea acest fel de „infecţie" va afecta în mod negativ funcţionarea calculatorului. Iată in continuare câteva dintre simptomele care a trebui ne indice faptul că calculatorul nostru a devenit un astfel de computer zombie (aceasta deși unele simptome pot proveni și din alte cauze):

- avem lucruri in folderul de corespondență expediate pe care știm că nu le-am expediat, acesta fiind un mare semn de avertizare că trebuie să ne verificăm calculatorul la un specialist;

- dacă cineva ne trimite un email in care ne acuză că i-am trimis spam;

- calculatorul nostru devine neobișnuit de lent, chiar și in condițiile in care avem un antivirus și sistemul ne este actualizat;

- programele noastre software brusc nu mai funcționează.

Pericolul prezentat de către reţelele bot a condus la o campanie concertată împotriva lor condusă de guverne, firme de securitate şi mari corporaţii. Activitatea reţelelor bot este acum monitorizată prin utilizarea unor resurse masive, într-un mod similar celui în care este supravegheată activitatea seismică. Dispozitive sofisticate de „ascultare" plasate pe internet filtrează activitatea şi traficul de pe internet şi caută semne timpurii de activitate bot. Organizaţii mari precum firma de securitate informatică Symantec le monitorizează activitatea în centre de control şi apoi arată răspândirea atacului reţelelor bot.

În mod interesant, una dintre figurile-cheie în riposta împotriva reţelelor bot este Microsoft. În ultimii ani uriaşul producător de programe informatice a dedicat mult timp, efort şi bani atacării şi distrugerii reţelelor bot. Multinaţionala americană a înfiinţat ceea ce a denumit Proiectul Răspuns Activ Microsoft pentru Securitate (MARS – după iniţialele din limba engleză), al cărui scop declarat este să anihileze reţelele bot şi să contribuie la a face internetul un loc mai sigur pentru toţi.

Rețelele bot sunt utilizate în criminalitatea informatică pentru comiterea unor infracțiuni precum accesul ilegal la un sistem informatic sau perturbarea funcționării sistemelor informatice.

Spam-ul este acel email enervant care ne incarcă inbox-ul, sau altfel spus, reprezintă orice comunicare nesolicitată care este realizată prin intermediul poștei electronice.

Acesta a transformat verificarea mesajelor de poștă electronică într-o activitate nepăcută, consumatoare de foarte mul timp. Termenul tehnic pentru spam este email comercial nesolicitat trimis in masă. Un termen frecvent folosit este și acela de junk email (rom. „poștă electronică nedorită") [54, p.187].

Persoana care utilizează spam-ul pentru a-și atinge obiectivele, contrare de multe ori intereselor persoanelor care suportă acțiunile sale, se numește spamer. Spam-ul este mai mult decât a fi doar enervant - uneori este o tentativă voalată de phishing, iar alteori conține programe informatice vicioase care ne pot infecta calculatorul.

Oamenii înțeleg ce este spam-ul. Ei conștientizează cât de enervant este, dar puțini înțeleg cum ar putea profita cineva de pe urma lui. Banii sunt cei conduc la corespondența nesolicitată: costul pentru expedierea a milioane de mesaje nesolicitante este infim, și există suficient de multe persoane care răspund acestor mesaje pentru ca ele să fie extrem de profitabile. Expeditorii de corespondență nesolicitată încearcă să câstige bani, și nu le pasă câți oameni sunt deranjați în acest proces [117, p.4].

Distribuitorii de spam adună adrese de poștă electronică din orice sursă, cum ar fi pagini web, din camerele de discuții, în acest demers folosind programe cu sistem de căutare, numite și spambot care accesează pagină după pagină în căutare de adrese de poștă electronică pe care să le adauge în listele poștale.

Așa cum sunt milioane de oameni care șterg spam-ul, sunt și mulți care il deschid și răspund. Odată răspunsul trimis nu vom face decât să-i confirmăm expeditorului că adresa noastră de email este validă, iar aceasta este exact ceea ce și-a dorit. Astfel, adresa noastră de email și informațiile personale vor fi înregistrate și vândute ulterior unor companii, obținându-se astfel un profit de către distribuitorul de spam.

Ca și măsuri de protecție impotriva spamului, am putea preciza că nu este indicat să dăm click niciodată pe link-urile conținute in spam deoarece este foarte probabil să conțină programe nocive pentru computerul nostru. Nu este indicat să cumpărăm niciodată produse sau servicii oferite prin spam, aceasta deoarece o firmă care își respectă clienții și oferă produse și servicii calitative nu și le face cunoscute prin transmiterea de mesaje spam.

Nu trebuie să solicităm dezabonarea de la mesajele spam deoarece demersul ar fi inutil, de vreme ce utilizatorul nu a cerut niciodată abonarea la aceste mesaje. Oricum, spamer-ul va continua să le trimită, iar consecința directă va fi creșterea volumului de spam [179, p.129]. Spamerii știu astfel că au depistat o adresă de mail care este validă și vor trimite mesaje către ea în mod regulat .În plus, există riscul să ne infectăm sistemul cu un virus doar vizitând pagina indicată în legătura de dezabonare afișată în mesajul electronic.

Totodată, pentru reducerea spam-ului este de dorit a înceta să mai trimitem email-uri forward prietenilor noștri, în urma primirii unui email cu îndemnuri de genul: "Dacă trimiți acest email inapoi

și altor opt prieteni de-ai tăi, ceva minunat se va intampla in urmatoarea oră". Dacă ne conformăm și trimitem email-ul forward la cei opt prieteni nu vom reuși decât să oferim incă opt noi adrese de email pentru cei care trimit spam [54, p.190].

Este recomandată folosirea a cel puțin două adrese de e-mail: una privată, care să fie folosită pentru corespondența personală și una publică, menită a fi utilizată pentru înregistrarea pe forumuri, liste de discuții pentru plasarea de cumpărături online etc. Trebuie să ne gândim la adresa de mail privată ca la un număr de telefon secret (care nu apare în cartea de telefoane). Ea trebuie oferită cu cumpătare doar persoanelor în care avem încredere.

În același timp, utilizatorii pot apela și la o serie de programe antispam, cum ar fi SpamAssasin - aplicație gratuită care filtrează mesajele și incearcă să le identifice pe cele de tip spam folosind diverse tehnici cum ar fi analiza textului și baza de date a SpamAssasin [179, p.130].

În România, conform datelor oferite de Ministerul Telecomunicațiilor și Tehnologiilor Informaționale, există aproximativ 13 milioane de utilizatori de internet, iar pagubele pricinuite de spam sunt aproximate la circa 270 milioane de dolari. Printre altele, aceste pierderi se datorează și costurilor pentru spațiul de stocare suplimentar utilizat pe serverele de e-mail, traficului suplimentar legat de livrarea acestuia și de timpul necesar pentru a citi mesajele. Se estimează că.in medie,un utilizator poate pierde până la 50 de minute in fiecare zi pentru a verifica,sorta și sterge mesajele spam.

Este foarte utilizat de către infractorii informatici pentru comiterea unor infracțiuni cum ar fi frauda informatică sau perturbarea funcționării sistemelor informatice.

Atacuri de refuz al serviciului, numite adeseori atacuri DoS, provenind de la expresia engleza Denial of Service (rom. „refuzul serviciului") - reprezintă un tip de agresiune prin care se urmărește blocarea accesului la un sistem, sau la serviciul oferit de acesta, prin epuizarea unei resurse alocate sistemului sau serviciului respectiv - de exemplu lățimea de bandă sau numărul simultan de clienți cărora li se poate răspunde.

Acest tip de atac este de cele mai multe ori întreprins asupra companiilor, deși poate afecta la fel de bine și calculatoarele personale. Cel mai comun tip de atac DoS este cel care urmărește împiedicarea accesului utilizatorilor de internet la un anumit site web, ceea ce poate avea ca rezultat pierderi financiare imense în contextul unei firme ale cărei afaceri depind exclusiv de internet, cum ar fi magazinele online sau cazinourile și firmele de pariuri online.

Eficiența unui astfel de atac sporește considerabil atunci când sunt folosite mai multe calculatoare ce asaltează simultan cu cereri sistemul-țintă. Această suprâncărcare cu date va conduce la colapsul sau inchiderea sistemului-țintă. Scopul unui atac DoS nu este dobândirea accesului la un computer securizat, ci mai degrabă impiedicarea utilizatorilor legitimi de a accesa un anumit site, cu scopul de genera cât mai multe pierderi financiare și de a scădea profitul unei firme. De multe autorii acestor atacuri au drept țintă și serviciile oferite de serverele unor bănci.

Este folosit de către infractorii informatici mai ales pentru comiterea infracțiunii de perturbare a unui sistem informatic, urmărindu-se apoi încetarea atacului care a provocat perturbarea în schimbul unei sume de bani.

IP spoofingul se referă la operația de falsificare a adresei de protocol de internet (IP) a computerului. Software-ul de IP spoofing este de regulă folosit atunci cand cineva urmează să trimită cantitați mari de e-mail-uri.

Expeditorii de spam adesea folosesc aceasta tehnică deoarece astfel este mai dificil să se depisteze adevaratul expeditor al spam-ului. Aceasta a căpătat o mai multă importanță in ultimiii ani, când in multe zone au aparut legi impotriva trimiterii de spam.

Există o varietate de instrumente si tehnici la dispozitie pentru a falsifica adresa IP a unui computer. De regulă se foloseste un remailer anonim, care este un serviciu ce va ascunde adresa IP a expeditorului inainte de forward-area mesajului catre destinatar [164, p.40]. Această metodă este in mod frecvent utilizată și in atacurile DOS, având avantajul de a ascunde sursa atacului.

El își arată utilitatea pentru infractorii cibernetici care utilizează spam-ul în vederea IP-ului de pe care a fost expediat acesta.

Email spoofing-ul reprezintă o metodă de trimitere a unui mesaj e-mail în care adresa expeditorului și antetul e-mailului sunt modificate să apară ca și cum ar proveni de la o sursă diferită, urmărindu-se deci ascunderea sursei reale de unde provine mesajul. De precizat că orice mesaj e-mail conține două părți: antetul (header) și corpul mesajului (message body).Antetul cuprinde informații despre numele data expedierii mesajului, cine l-a expediat și traseul parcurs de respectivul email. Cât despre corpul e-mailului, acesta conține textul propiu-zis al mesajului și fișierele atașate dacă există. Acesta constituie o practică comună a creatorilor de spam.

La fel ca și în cazul mai sus menționat, este o practică curentă a infractorilor informatici care utilizează spam-ul și servește la ascunderea urmelor lor pentru a fi mai greu de identificați

Web spoofing-ul implică redirecționarea browser-ului de internet al utilizatorului către un website dat, atunci cand utilizatorul tasteaza o adresa URL (uniform Resource Locator, adică un mod uniform de a localiza un fisier sau un document pe internet) similară, aceasta tehnică fiind folosită de site-urile pornografice pentru a ademeni vizitatori catre site-urile lor. Cu alte cuvinte,spre exemplu, dacă noi specificămi o adresă web, browser-ul ne poate trimite către un alt site web cu o temă similară.

Odată prins de aceste site-uri este uneori greu să te retragi datorită numarului mare de reclame pop-up, adică a acelor ferestre cu reclame care apar pe ecran fără ca tu sa le fi cerut și care sunt lansate incă de la prima accesare a site-ului. Scopul reclamelor de tip pop-up este de a ne atrage atenția și de a ne forța să privim reclama, caz în care crește probabilitatea ca noi să executăm click pe reclamă sî să cumpărăm acel produs.

Dacă ne simțim invadați de ferestre pop-up, este posibil ca acestea să fie generate de un modul *spyware* sau *adware* existent în calculatorul dumneavoastră. O aplicație spyware este de fapt o aplicație ce se poate instala fără permisiune noastră și care ne poate monitoriza toate activitățile, raportând informațiile respective prin internet.Aceste aplicații pot fi descărcate prin intermediul unor alte programe pe care le descărcați de pe internet precum și prin fișierele atașate la un email.

Creatorii de module spyware vor să manipuleze ceea ce vedem și ceea ce facem online pentru a ne forța să cumpărăm lucruri de la ei și de la persoanele pentru care fac publicitate [117, p.126].

În ceea ce privește adware-ul, acesta reprezintă un software care afișează reclame, instalat de regulă pe calculatorul nostru fară să avem cunoștiință. Deci, mare atenție atunci când, la instalarea unui program gratuit ni se propune să instalăm și o bară de unelte, cum ar fi Ask.com, sau orice altceva care nu are legătură cu programul respectiv.

Acest tip de software este utilizat în general de companiile ce oferă publicitate pe internet, pentru a putea fi urmărit comportamentul online al potențialilor clienți. Prin intermediul adware se crează un profil comercial al acestora, astfel încât, la accesarea unui site, să li se prezinte reclamele ce ar putea să-l intereseze. Adware-ul poate afișa conținuturi neplăcute, cum ar fi site-urile de jocuri de noroc sau de pornografie. Publicitatea nedorită prin intermediul adware-ului poate devein o hărțuire.

O astfel de aplicație poate încetini considerabil calculatorul, consumând din memoria sistemului și din lărgimea de bandă a conexiunii la internet. De asemenea, pot intra în conflict cu alte aplicații, provocând vulnerabilitatea și instabilitatea sistemului.

Comportamentul online al potențialilor clienți este urmărit și cu ajutorul așa numitor *cookies*. Un cookie este o informație plasată în sistemul informatic de către un website, fiind un un text special trimis de website unui navigator web și apoi trimis înapoi de către sistemul informatic al navigatorului de fiecare dată când accesează acel site.

Aceste „cookies” colectează informații despre utilizator, precum adresele de e-mail, ce anume căutămi, ce anume cumpărăm, sau informații despre dispozitivul pe care-l folosim. Ca să strângă informații și mai multe despre noi, unele companii folosesc programe pentru a citi cookies ale altor companii. Acestea se numesc super cookies sau zombie cookies. și rețin ce anume am căutat sau am cumpărat și adresele noastre de e-mail pentru ca reclamele acelor companii să ne poată fi adresate [183, p.40].

Tehnicile precizate anterior, de cele mai multe ori sunt utlizate în comiterea infracțiunii de perturbare a funcționării sistemelor informatice.

Escrocherii prin site-uri web specializate în comercializarea unor produse. Unul din procedeele de comitere a acestor infracțiuni este înființarea unui site destinat vinderii de produse, iar de regulă, fie nu se trimite produsul comercializat, fie se trimite ceva mai puțin valoros decât s-a anunțat.

Prima categorie, netrimiterea produsului comercializat, este relativ clară. Victima trimite fonduri pentru un anumit obiect, iar vânzătorul nu-i trimite niciodată obiectul. Acesta este cel mai evident tip al fraudei de licitaţie şi de obicei cel mai uşor de investigat şi de trimis în instanţă.

Cea de-a doua categorie, trimiterea a ceva mai puţin valoros, este mult mai dificil de investigat şi de trimis în instanţă. Să presupunem că se cumpără o carte veche la o licitaţie online. Cumpărătorul crede că este un exemplar în stare perfectă, din prima ediţie, cu semnătura autorului. Însă când îl primește, articolul este de fapt în stare destul de proastă, un exemplar din a treia ediţie, dar purtând totuşi semnătura autorului. Vânzătorul va putea oricând invoca înţelegerea greşită a cumpărătorului – iar dacă anunţul de licitaţie este formulat suficient de vag, aceasta va fi o versiune plauzibilă. În unele cazuri, va fi necesară chiar implicarea unui expert în produsul respectiv (în acest caz, un expert în cărţi vechi) pentru a verifica dacă articolul corespunde descrierii din anunţul publicitar. Factorii amintiţi fac aceste cazuri foarte dificil de investigat sau de raportat. Cel mai adesea victimele nici nu întreprind vreo acţiune decât dacă suma de bani implicată este foarte mare.

Alt procedeu constă în inființarea de site-uri pentru a aduna numere de cardurii și alte informații personale de la clienții atrași de de achiziționarea unui produs sau unui serviciu. În realitate nu se livrează nimic, iar infractorul vinde informațiile altor infractori sau le folosește pentru propriile activități ilegale [16].

Această tehnică este estrem de des folosită de către infractorii ciberneticii în cazul comiterii infracțiunii de fraudă informatică.

Frauda nigeriană. În acest scenariu, se trimite un email unui număr mare de adrese de email aleatorii. Fiecare email conţine un mesaj care se pretinde a fi de la o rudă a vreunui oficial guvernamental nigerian decedat, întotdeauna fiind vorba despre cineva cu un statut social semnificativ (este mult mai probabil să convingi victimele că aranjamentul este legitim dacă pare să implice oameni cu un anumit statut social.).

Oferta arată astfel: o persoană are o sumă de bani pe care doreşte să o transfere în afara ţării sale şi din motive de securitate nu poate folosi canalele normale. Ea doreşte să utilizeze contul nostru bancar pentru a „parca” temporar fondurile. Dacă acceptăm să îi permitem accesul la contul nostru ni se promite că vom fi recompensați cu o sumă consistentă. În situația în care suntem de acord cu acest aranjament, vom primi prin poştă o gamă de documente cu un aspect foarte oficial – suficient cât să convingă pe cei mai mulţi analişti neavizaţi că aranjamentul este legitim. Vom fi apoi rugați să înaintăm nişte bani pentru a acoperi unele cheltuieli precum impozitele şi taxele pentru transferul bancar. În cazul în care însă chiar vom trimite banii, îi vom pierde – şi nu vom mai primi veşti de la acei indivizi niciodată. Este o tehnică uzitată constant de către infractori în cazul săvârșirii fraudelor informatice.

Un alt mod de operare al făptuitorilor este **cracking-ul.** Această modalitate de operare in criminalitatea informatică se referă la activitatea de folosire a unui program pentru a penetra parolele prost alese, denumit in genere spărgător de parole (cracker).

Multe dintre aceste programe folosesc o metoda prea puțin inteligentă și anume aceea de a incerca cuvânt dupa cuvânt, până când va fi găsit unul care să se potrivească.

Toate calculatoarele stochează parole în sistem, acestea având rolul de a certificafaptul că utilizatorii sunt cei care pretind a fi.

În general,este de dorit a se evita parolele simple, precum „123" sau „parolă" .Acestea sunt printre primele încercate de către crackeri. Ele se bazează pe comoditatea utilizatorilor de a-și alege parole cat mai scurte și cat mai simplu de memorat [137, p.94]. Dacă acestea totuși nu funcționează, sunt șanse mari ca parolele să conțină numele de familie al utilizatorului, numele soției sau copilului acestuia, al câinelui , ziua de naștere sau numărul mașinii sale. Numele de locuri faimoase, formații de muzică celebre, spectacole de televiziune etc, nu sunt nici ele indicate.

Dacă un infractor informatic nu poate totuși ghici parola, pasul următor constă în folosirea de programe specializate numite spărgătoare de parole. Acestea folosesc folosesc o gamă largă de metode până când identifică parola respectivă.

O asemenea tehnică implică utilizarea șablonului hash inerent al parolei. Un șablon hash este echivalentul numeric al cuvântului respectiv; acesta este generat când parola respectivă este transformată de aplicația de autentificare într-o valoare de lungime fixă prestabilită. De exemplu,parolei Lasa-măSăIntru poate să-i corespundă valoarea hash 1234 [126, p.376].

Un spărgător de parole in funcție de dicționar folosește cuvinte din dicționar încercand să găsească o corespondență intre șablonul hash și cuvinte cunoscute. Unele spărgătoare de parole bazate pe lexicoane creează de asemenea, forme hibride ale unor cuvinte cunoscute, sau adaugă la cuvinte numere. De exemplu, câine ar putea deveni câine01, câine02 și așa mai departe [126, p.376].

Această tehnică este foarte utilă infractorilor mai ales în cazul comiterii infracțiunii de acces ilegal la un sistem informatic.

Următorul mod de operare al făptuitorilor este **furtul de identitate.** Furtul de identitate a fost definit ca fiind furtul identitatii cuiva prin intermediul unei informatii de identificare care este apoi utilizata in activitatea de fraudare [164, p.61]. Acest termen descrie actele criminale prin care infractorul obține și utilizează în mod fraudulos identitatea altei persoane.

De cele mai multe ori, furtul de identitate reprezintă o etapă pregătitoare în comiterea infracțiunii de fraudă informatică.

Acesta se efectuează în mai multe faze:

- fapta de a obține informații referitoare la identitate;
- fapta de a transfera informații referitoare la identitate;

- fapta de a utiliza informații referitoare la identitate în scopuri infracționale.

În ultimii ani am fost martorii unei creșteri incredibile în răspandirea acestei infractiuni. Până ce nu am devenit victima unui furt de identitate sau nu am lucrat cu astfel de infracțiuni, nu putem aprecia cantitatea de timp necesară pentru repararea daunelor produse in urma acestui tip de infracțiune. Furtul de identitate este clasificat in patru categorii [54, p.61]:

- *furtul de identitate financiar* - folosirea identității altei persoane pentru obținerea de bunuri și *servicii;*

- *furtul de identitate infracțional* - pretinderea de a fi o altă persoană in caz de prindere asupra unei infracțiuni;

- *clonarea identității* - folosirea informațiilor despre o persoană in vederea asumării identității acesteia in viața de zi cu zi;

- *furtul de identitate de afaceri sau comercial* - folosirea numelui companiei altei persoane pentru a obține un credit.

In ceea ce privește prevenirea furtului de identitate, iată câteva sfaturi practice pe care trebuie să le urmăm pentru prevenirea acestuia;

- monitorizarea conturile bancare si cele ale cărților de credit, iar dacă există tranzacții pe care nu le recunoaștem, trebuie să contactăm imediat banca;

- trebuie să facem cel puțin două copii ale tuturor cardurilor noastre de credit, ale permisului de conducere, cărții de identitate, cardului de asigurare și ale oricăror alte acte pe care le purtăm de obicei in porofel, iar o copie o vom păstra acasă, iar cealaltă într-un loc sigur din afara casei;

- nu trebuie să uităm alte forme de identitate considerate minore, precum legitimațiile de bibliotecă și cardurile pentru obținerea de reduceri la magazine, facându-le copii și notificandu-i pe toți cei implicați in caz de furt, asta deoarece un lucru inofensiv precum o legitimație de bibliotecă poate fi prezentat drept o formă de identificare pentru a solicita o altă formă de identificare, infractorii putând merge din aproape în aproape pentru a-si atinge interesul.

Acest tip de infracțiune se poate realiza prin intermediul uneia dintre tehnicile prezentate in continuare.

Dumpster diving-ul sau căutarea prin containerele de gunoi pentru a găsi informații care incă pot fi utilizate. Multe informații despre o victimă pot fi găsite prin căutarea in gunoi, cum ar fi chitanțele noilor carduri de credit sau debit, acestea conținând ultimele patru cifre ale cardului, numele proprietarului si tipul de card utilizat. Toate aceste informații, când sunt utilizate, pot fi de folos in cazul unui potențial furt de identitate.

Este recomandabilă, deci, distrugerea cu mare atenție a acestor documente înainte de a fi aruncate, astfel încat informația care se regăsește pe acestea să nu mai poată fi reconstituită de către o eventuală persoană interesată.

Skiming-ul sau falsul cititor de carduri se referă la utilizarea unui dispozitiv manual, de mici dimensiuni, care poate stoca sute de numere de carduri, numele proprietarului și data expirării cardului fără ca acesta să aibă cunoștință.

Activitatea de copiere vizează datele de pe banda magnetică a cardului, inclusiv codul CVC. Codul de verificare a cardului, sau cod CVC, este un număr care oferă securitate suplimentară posesorilor de carduri de credit și de debit, în cazul în care o persoană neautorizată intră în posesia numărului posesorului de cont. Poziționarea codului CVC și numărul de cifre variază în funcție de tipul cardului. Astfel, in cazul MasterCard, Visa și Visa Electron este reprezentat de ultimele trei cifre ale numărului aflat pe spatele cardului dumneavoastră, pe bara de semnătură.

Evoluția tehnologică rapidă a permis infractorilor să sporească capacitatea de memorare a dispozitivelor de skimming, concomitent cu reducerea mărimi acestor dispositive, ele devenind astfel mai greu detectabile.

În principal, skimming-ul se bazează pe faptul că datele de pe banda magnetică pot fi înregistrate și apoi rescrise pe un card- nou sau contrafăcut- cu ajutorul unui calculator și a unui dispozitiv de rescris banda magnetică a cardurilor [104, p.355].

De regulă, aceste dispositive sunt atașate fie la fanta de intrare a cardului într-un bancomat sau ATM cum mai este numit acesta, fie la Pos-uri sau Point of sale, adică acel dispozitiv electromagnetic aflat lânga casele de marcat care permite retragerea de numerar din disponibilul de cont. Folosirea dispozitivului de skimming la ATM-uri implică adeseori și folosirea unei camere de luat vederi miniaturale, aceasta avand rolul de a permite vizualizarea codului PIN al cardului.

Dacă un card astfel contrafăcut este introdus în bancomat, în cazul în care contul este valid, emitentul cardului nu va sesiza că tranzacția este falsă deoarece codul CVC este citit împreună cu alte date conținute de banda magnetică și transmis electronic în timpul procesului de autorizare pentru a fi comparat cu cel inregistrat de emitent.

Dacă un utilizator scanează un card, trecându-l fără știrea lui printr-un skimmer, informațiile cuprinse pe card sunt transferate pe acest dispozitiv, creându-se o arhivă digitală in memoria skimerului care apoi va fi transferată pe computerul hoțului de identitate. De regulă, deținătorul nu este conștient că datele au fost copiate până cand tranzacții neautorizate apar în extrasul de cont.

Pentru prevenirea și evitarea unei astfel de fraude este foarte utilă activarea unor servicii de ultimă generație oferite de bănci,cum ar fi sms alert. Mesajul sms trimis pe telefonul nostru va conține următoarele informații:tranzacția efectuată,suma tranzacționată, locația în care s-a efectuat tranzacția,data și ora exactă a utilizării, soldul disponibil după efectuarea tranzacției. Astfel, proprietarul cardului va afla aproape instantaneu dacă cineva a retras bani de pe cardul respectiv fără ca el să aibă cunoștiintă.

Phishing-ul, adică procesul in care un hoț de identitate, care joacă rolul unei persoane de încredere va incerca să determine o potențială victimă să-i furnizeze informații personale în cadrul unei comunicări electronice, informații necesare pentru a se angrena in furtul de identitate al acestuia.

Phishingul țintește multe feluri de informații confidențiale, inclusiv nume de utilizator și parole, informații despre conturi bancare și cărti de credit, CNP - uri, date de naștere, precum și informații legate de întrebarea secretă,cum ar fi numele de fată al mamei sau cuvinte cheie. De regulă, victima, in aceste situații, nu sesizează că informațiile sunt cerute de catre o sursă neautorizată.

Metoda preferată constă in primirea de către victimă a unui e-mail sau a altei înștiințări care par a fi oficiale si care-i cer persoanei să trimită aceste informații pentru a-și păstra un cont. Victima, poate apoi trimite informațiile pe un site care poate părea legitim deoarece este aproape identic cu website-ul oficial al unei banci sau companii de carduri, dar in realitate nu este decat un site de colectare de date unde hoții de identitate adună informații de la cât mai multe victime.

Pentru a evita o astfel de înșelătorie, am putea, spre exemplu să retransmitem orice mesaj electronic suspect către compania în cauză pentru a afla dacă în realitate acesta este autentic și a fost expediat chiar de către aceasta.

Una dintre cele mai comune forme de phishing este așa numita “chemare la acțiune”. Ea constă in primirea de emailuri care ne avertizează că într-un fel sau altul, conturile noastre au fost compromise și ne oferă un link conținut in același email pentru a ne conecta la cont și a ne verifica informațiile. Alte tipuri de incercări de phishing prin chemarea la acțiune se realizează prin următoarele modalități:

- se pretinde a exista un nou serviciu la o instituție financiară, cu un link in email pentru a-l verifica, dar trebuie să ne grăbim deoarece oferta este limitată in timp;

- factură pentru produse pe care nu le-am autorizat sau comandat, cu un link prezent in email pentru a anula sau contesta comanda;

Infracţiunile care implică phishing pot fi deosebit de dificil de investigat dintr-o sumă de motive.

În primul rând, victimele adesea nu realizează că s-a comis o infracţiune decât la mult timp după ce aceasta a avut loc. Dacă cineva ne fură identitatea astăzi, cel mai probabil că ramificaţiile financiare ale acestul fapt nu vor fi pe deplin conştientizate decât după câteva săptămâni. Şi, ca în cazul altor tipuri de infracţiuni, cu cât mai curând după incident are loc investigaţia, cu atât mai uşor va fi să se adune probe criminalistice.

În al doilea rând, hoţii de identitate iscusiţi ştiu cum să îşi acopere urmele. Mai mult, ei vor efectua operaţia de phishing doar pentru o perioadă limitată de timp, iar apoi o vor închide. Aceasta înseamnă că în momentul în care se raportează infracţiunea şi începe investigaţia, este foarte probabil ca operaţia de phishing să fi fost deja închisă de câtva timp.

În al treilea rând, site-urile contrafăcute sunt găzduite de servere publice din ţările cu legislaţie mai permisivă, uneori chiar pe un server al unei terţe părţi, care nu are cunoştinţă despre ilegalitatea comisă. Apoi, aceste site-uri de internet sunt adesea desfiinţate de îndată ce făptaşul a dobândit o cantitate suficientă de date personale.

Aceşti factori presupun că investigările acestui tip de infracţiune trebuie iniţiate cât mai curând posibil după ce au avut loc, iar găsirea urmelor infracţiunii va necesita un nivel înalt de competenţă informatică judiciară.

După ce anterior am întreprins demersuri în cunoașterea infracțiunilor informatice, apreciem că este extrem de important ca aceasta să fie însoțită și de cunoașterea măsurilor de prevenire a infracțiunilor informatice, aceasta pentru a nu deveni victime sigure ale infractorilor informatici, dar și pentru o abordare adecvată a determinantelor acestui tip de infracțiuni și factorilor de natură să favorizeze săvârșirea lor. Cu atît mai mult, actele normative de referință vizează și prevenirea infracțiunilor informatice. Astfel de măsuri de prevenire constituie:

Actualizarea permanentă a sistemului. Când sistemul utilizat de noi ne alertează că sunt disponibile actualizări, acestea trebuie instalate imediat. Companiile de software precum Microsoft sunt notificate zilnic cu privire la vulnerabilitățile de securitate. În funcție de gravitatea vulnerabilității, toate actualizările și reparațiile sunt, în general, puse la pachet și lansate într-o singură actualizare. Faptul de a nu menține la zi aceste acualizări, lasă calculatorul deschis in fața unei game largi de probleme. Spre exemplu,Microsoft pune la dispoziție programul Windows Update pentru a simplifica obținerea actualizărilor de securitate.

Activarea sistemul firewall integrat în sistemul de operare utilizat. Un asemenea sistem este ceea ce sugerează numele: adică un fel de zid poziționat între calculatorul utilizatorului și internet care verifică tot traficul de intrare și de ieșire și blocând tot ceea ce pare periculos sau suspicios. Un sistem firewall poate fi de tip software sau hardware. Dacă este utilizat un ruter în scopul permiterii accesului cu dispozitive fără fir, acel ruter are, cel mai probabil,o serie de funcții firewall. Firewall-ul reprezintă prima linie de apărare în fata hackerilor, astfel încît el controlând tot traficul internet trebuie să fie configurat pentru a se specifica ce programe pot să acceseze rețeaua internet și ce programe au interdicție de acces.

Instalrea protecției antivirus. Aplicație software antivirus trebuie privită ca pe sistemul imunitar al corpului omenesc. Dacă suntem expuși unei boli, sistemul imunitar face tot posibilul să stopeze agentul infecțios înainte de a ne îmbolnăvi. Prin similitudine, scopul principal al unei aplicații software antivirus constă în împiedicarea infectării calculatorului utilizat.

Ultimele aplicații apărute pe piața de specialitate, precum Kapersky Internet Security sunt dezvoltate special pentru a proteja ceea ce contează cel mai mult în spațiul virtual: intimitatea, datele,

identitatea, banii și dispozitivul însuși. Tododată, noile soluții includ tehnologii avansate care permit navigarea în siguranță pe orice platformă, indiferent că aceasta este Windows, OSX sau Android.

Aplicația monitorizează tot ce intâmplă în calculator în timp real, încercând să blocheze virușii să pătrundă în sistem. Pe lângă monitorizarea permanentă, aplicațiile software antivirus au posibilitatea de a efectua și scanare completă a sistemului, pe parcursul căreia verifică tot ceea ce există în hard-disc în căutarea unor indicii sau urme de viruși.Acest proces poate dura mai mult de o oră, urmărindu-se detectarea posibilelor fișiere infectate pătrunse prin fisurile sistemului de protecție.

Aplicațiile software antivirus pot răspunde la detectarea unui virus în trei moduri [117, p.111]:

- stergerea fișierului virusat ,aceasta fiind cea mai sigură și simplă metodă;

- remedierea fișierului virusat,caz în care infecția este eliminată iar fișierul rămâne întreg (aceasta în situația în care trebuie să salvați un program sau anumite date);

- introducerea în carantină a fișierului virusat, aceasta în situația în care nu este nici o soluție de reparare a fișierului și dacă aveți speranța că veți purea recupera fișierul ulterior, ori dacă, dintr-un anumit motiv, vreți să țineți evidența virușilor cu care ați avut de-a face.

Odată instalat legal un program antivirus comercial, pe toată perioada contractului utilizatorul va primi automat reînnoirile bazei de viruși cunoscuți. Aceste reinnoiri se vor instala sub controlul programului antivirus, acesta depistand și neutralizând acești viruși, astfel încât calculatorul va putea fi folosit in relativă siguranță pe toată perioada de valabilitate a licenței programului antivirus. Este recomandată scanarea toate fișierele atașate și a tuturor programelor descărcate înainte de a le deschide.

Crearea unor parole puternice și ușor de memorat. Este necesară utilizarea unor parole cu o lungime minimă de opt litere. În realitate este mult mai ușor decât pare la prima vedere. Astfel, spre exemplu, trebuie să ne gândim la o la o expresie pe care ne-o putem aminti. Pentru a exemplifica vom folosi „Nu arăta niciodată că știi să trișezi celor cu care joci”. Luăm acum prima literă a fiecărui cuvânt – nancsstcccj și astfel rezultă 11 caractere, adică o lungime optimă pentru obținerea unei parole puternice.

O parolă de opt caractere care este însă compusă doar din litere mici poate fi spartă teoretic în aproximativ trei săptămâni, dat fiind că unele programe de spargere de parole cu forță brută pot verifica chiar și o sută de mii de parole pe secundă.

Dacă este folosită o parolă de opt caractere care să combine litere mici cu majuscule,numere și simboluri, procesul de spargere ar fi de aproximativ doi ani. Pentru a ne aminti o astfel de parolă, fie ea și mai lungă, trebuie să ne gândim la o propoziție care să aibă semnificație pentru noi,dar nu și pentru cracker. De exemplu putem transforma propoziția ”Cățelul meu Amigo a costat 300 de lei și este foarte răsfățat și jucăuș” în „CmAac300dlsefrsj”.

Securizarea routerelelor wireless prin parolarea acestora. Instalarea acestora cu setările originale din fabrică echivalează cu lăsarea ușilor descuiate noaptea, permițând oricui să intre și să ne fure bunurile. Dacă lăsăm conexiunea wireless nesecurizată, infractorii care l-au folosit. pot să fi dispărut de mult, dar evidențele vor arăta incă spre contul nostru, lăsându-se impresia că noi am fi autorii infracțiunii. În ceea ce privește punctele de internet wireless gratuit existente in cafenele sau in hoteluri, acestea prezintă periculozitate pentru utilizatorii de laptopuri deoarece marea majoritate a laptopurilor sunt configurate să se conecteze automat la rețeaua wireless cu cel mai puternic semnal.

În foarte multe dintre spațiile publice, de la centre comerciale, la cafenele, restaurant sau la biblioteci, există hotspot-uri gratuite, adică puncte de acces la internet prin intermediul conexiunii Wi-Fi. Din nefericire, utilizatra unui hotspot nu este lipsită de pericole. Pentru a facilita accesul și a atrage cât mai multe persoane, majoritatea acestor puncte de acces nu utilizează conexiuni securizate, conectarea realizându-se fără a fi nevoie de o parolă.

Dacă un hacker stă la două mese distanță de într-un local cu wireless gratuit, el poate cu ușurință să emită un semnal wi-fi mai puternic decat cel local și să determine conectarea noastră la laptopul său, de pe care va lua la cunoștiință numele de utilizator și parola noastră, informațiile legate de cardul de credit dacă acestea sunt accesate, efectiv aflând orice tastă pe care o apăsăm. Pentru a evita acest lucru trebuie modificate setările, astfel încât laptopul să nu se conecteze in mod automat la cel mai puternic semnal wireless [8, p.44].

Ca o măsură suplimentară de protecție pentru navigarea pe net în siguranță chiar și când nu suntem acasă, este folosirea unui serviciu VPN (virtual private network), cum este F – Secure Freedome. O rețea privată virtuală criptează traficul internet în așa fel încât acesta să nu poată fi interceptat de către cei care utilizează același hotspot gratuit.Criptarea înseamnă realizarea formei neinteligibile a unui mesaj pentru a nu fi utilizat de persoane neautorizate să-l acceseze. Conform unei alte definiții, criptarea reprezintă procesul de codificare a datelor, realizată cu scopul de a preveni utilizarea neautorizată a acestora, în special în timpul transmiterii lor prin diverse canale de comunicare [178, p.93].

Criptografia este un domeniu care se află la intersecția dintre informatică, matematică și inginerie și care are drept scop securizarea informației. Cele două tipuri principale de tehnologii criptografice sunt: criptografia prin chei simetetrice (chei secrete sau chei private) și criptografia prin chei asimetrice (chei publice).

Criptografia prin chei simetrice apelează la o singură cheie la ambele capete ale comunicării: emițătorul și receptorul. Emițătorul sau receptorul critează textul clar cu ajutorul unei chei secrete, iar receptorul sau destinatarul va decripta mesajul folosind aceeași cheie.

Spre deosebire de sistemele de criptare bazate pe chei secrete, care presupun o singură cheie cunoscută de emițător și receptor, sistemele bazate pe chei publice folosesc două chei: una publică și

una privată. Cheia publică este pusă la dispoziția oricărei persoane care dorește să transmită un mesaj criptat. Cheia privată este utilizată pentru decriptarea mesajului, iar nevoia de a face schimb de chei este eliminată. Decriptarea este procesul prin care un text cifrat este transformat într-un mesaj inteligibi [45, 131-133], sau altfel spus, decriptarea reprezintă procesul invers prin care din conținutul unui document ce a suportat un proces de criptare se obține conținutul mesajului inițial [190].

Scopul criptografierii este de a proteja informațiile transmise fără ca acestea să poată fi înțelese decât de către acele persoane cărora le sunt destinate.

VLN-ul nu reprezintă singura modalitate de a naviga pe internet într-un mod mai sigur, mulți utilizatori folosind și rețeaua gratuită Tor care se bazează pe combinarea criptării cu anonimatul utilizatorului.

În sens de utilitate practică, trebuie făcute *copii de siguranța ale datelor în mod periodic*. Salvarea datelor presupune efectuarea periodică a unui „back-up", altfel spus copierea acestora pe orice suport de stocare, de preferință altul decât calculatorul pe care sunt la momentul salvării.

Fie că este vorba de un dvd, cd, hard disk extern sau memory-stick, practic salvarea datelor înseamnă o copie de siguranță a acestora.

Se pot considera date importante într-un calculator orice fel de informații care ne sunt de mare folos, începând cu baza de date, rapoarte, referate, acte scanate, contracte, continuând cu fișiere de tip text pe care am făcut diverse notări (spre exemplu, parole folosite și username de logare), poze pe care le-am făcut, descărcat și păstrat in calculator (unele dintre ele cu caracter unic poate), toate acestea reprezintă informații prețioase care pot fi salvate, adică memorate, înregistrate, copiate pentru a putea păstra tot ceea ce definește și particularizează acel calculator [92]. Dacă sistemul ne este atacat, o salvare recentă a datelor ne poate scuti de un efort considerabil în reconstituirea muncii dumneavoastră.

Folosirea tehnologiei cloud. Cloud-ul în esenţă se referă la locul unde sunt stocate datele şi programele informatice ale cuiva. În trecut ne-am stocat de obicei datele pe hard discul calculatorului nostru şi am descărcat programele informatice pentru a le folosi după cum doream. În computerizarea cloud, informaţiile şi programele nu sunt stocate pe calculatorul nostru, ci pe serverele de reţea proprii unui furnizor de servicii cloud. Această reţea este de fapt „cloud-ul" pe care utilizatorul, în calitate de client al acelui furnizor cloud, îl poate accesa când doreşte.

Există multe avantaje ale computerizării de tip cloud, atât pentru indivizi, cât şi pentru firme. Se pot reduce costurile, cloud-ul putând fi accesat cu uşurinţă de oriunde şi, de asemenea, îi abilitează pe utilizatori să profite de cele mai recente tehnologii în programare, pe care s-ar putea ca altfel să nu le folosească. În teorie, stocarea datelor printr-un furnizor cloud ar trebui să fie mai sigură decât stocarea pe un calculator. Datorită extinderii şi mărimii acestor aplicaţii, furnizorii cloud pot cumpăra cele mai bune sisteme de apărare împotriva atacurilor cibernetice.

2.3. Concluzii la Capitolul 2

În raport cu definirea și caracterizarea fenomenului infracțional din domeniul informatic pot fi desprinse următoarele concluzii:

1. În zilele noastre ne aflăm nu doar în prezența unei explozii, proliferării perpetue și specializării criminalității, dar asistăm și la o concurență între infracțiunile care aparțin domeniului informatic și așa numitele infracțiuni tradiționale, aceasta deoarece activitatea ilegală nu mai are loc doar în spațiul material ci și în cel virtual.

2. Specific infracțiunilor informatice sunt următoarele caracteristici esențiale care se transformă în avantaje reale conferite făptuitorilor:

- caracterul transfontalier - acest fenomen nu ia în considerare granițele convențional stabilite;
- anonimitatea - făptuitorul nu trebuie să fie prezent la locul faptei;
- credibilitatea - făptuitorul creează aparența unei afaceri legale și corecte;
- rapiditatea - conferită de transmiterea aproape instantanee a datelor prin sistemele informatice;
- costurile foarte reduse în comparație cu beneficiile ce pot fi obținute.

3. Infracțiunea informatică este acea infracțiune care implică un computer în următoarele moduri:

- computerul ca instrument al infracțiunii;
- computerul ca focalizare a infracțiunii;
- computerul ca loc de stocare a dovezilor.

4. În domeniul informaticii, comportamentele infracționale nu se supun nici unui determinism social: delicvenții pot avea foarte bine 10 ani sau 60 de ani, să fie novici sau profesioniști. Autorii infracțiunilor informatice sunt adesea, oameni obișnuiți, dar pot fi și persoane cu aptitudini și talente excepționale. Practic, orice individ, având un minimum de calificare și stimulat de sfidarea tehnică, dorință de câștig, celebritate sau răzbunare, ori având motive ideologice, poate deveni un delincvent informatic.

5. Infractorii cibernetici nu reprezintă doar o schimbare de nume în ceea ce privește abordarea infracțiunilor tradiționale într-o formă nouă. Infractorii digitali, ca dealtfel și faptele comise de aceștia, reprezintă o transformare fundamentală în felul nostru de a trata problematica infracțiunii și a infracționalității. Deși infracțiunile informatice formează un nou tip de criminalitate, acestea sunt comise tot de oameni, tot cu vinovăție, și de regulă, tot întru realizarea unor beneficii patrimoniale.

6. În literatura de specialitate ca modalități tipice de realizare a elementului material specific infracțiunii informatice, inclusiv fraudei informatice sunt determinate: hacking-ul (pătrunderea,

infiltrarea, spargerea unui sistem (rețele) informatic, recurgându-se la diverse tehnici, mijloace, programe, urmărindu-se un scop cupidant, sau de altă natură); cracking-ul (acțiunea făptuitorului de folosire a unui program și tehnici respective, pentru a penetra parolele unui calculator, sistem (rețea) informatic); furtul de identitate sau *phishing-ul* (furtul identitatii cuiva prin intermediul unei informatii de identificare care este apoi utilizata in activitatea de fraudare; *furtul de identitate reprezintă o etapă pregătitoare în comiterea infracțiunii de fraudă informatică*, incluzând mai multe faze:

- fapta de a obține informații referitoare la identitate;
- fapta de a transfera informații referitoare la identitate;
- fapta de a utiliza informații referitoare la identitate în scopuri infracționale.

Pentru o mai bună prevenire a fraudei informatice, chiar la etapa actelor preparatorii, se propune introducerea în legislația penală a Republicii Moldova și a României a unei noi incriminări cu denumirea marginală de *furt de identitate (phishing)*, cu următoarea formulare legislativă: *Acțiunea prin care făptuitorul obține în mod fraudulos identitatea altei persoane cu ajutorul sistemelor informatice sau de telecomunicație prin inducerea în eroare a utilizatorului sistemului informatic datorită creării unei stări de aparență menite a determina utilizatorul să furnizeze date personale în cadrul unei comunicări electronice*. În C.pen. al României incriminarea ar urma să fie statuată în Titlul VII, Capitolul VI din Partea specială la art. 364^1, cu instituirea unei pedepse *de la 3 luni pînă la 2 ani sau cu amendă*. În C.pen. al Republicii Moldova incriminarea urmează să fie încorporată în Capitolul XI din Partea specială prin introducerea art. 260^7 și instituirea următoarei pedepse: *amendă în mărime de la 200 la 500 unităţi convenţionale sau muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau închisoare de pînă la 2 ani, cu amendă, aplicată persoanei juridice, în mărime de la 1000 la 3000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate*.

3. SEDIUL NORMATIV-PREVENTIV DE INCRIMINARE A FRAUDEI INFORMATICE: REGLEMENTĂRI INTERNAȚIONALE ȘI NAȚIONALE

3.1. Cadrul juridic internațional în materia incriminării fraudei informatice

Este o realitate incontestabilă **că a**tât în România cât şi în Republica Moldova, legiuitorul care a incriminat frauda informatică s-a inspirat din **Convenţia Consiliului Europei asupra criminalităţii informatice** [157], practic reproducând prevederile Convenţiei.

Convenţia Consiliului Europei privind criminalitatea informatică constituie un tratat în domeniul justiţiei penale care stabileşte dispoziţiile de drept penal pe baza drepturilor omului şi a principiilor statului de drept.

În timp ce măsurile de combatere a criminalităţii informatice au rolul lor în întărirea siguranţei naţionale şi a securităţii cibernetice, cooperarea internaţională în domeniul combaterii criminalităţii informatice bazată pe acest tratat contribuie la cooperarea dintre statele membre pentru a investiga atacurile informatice transfrontaliere.

Elaborarea Convenţiei a avut la bază o recomandare a Comitetului European pentru Probleme Criminale din cadrul Consiliului Europei, prin prisma ultimelor rapoarte în domeniul criminalităţii informatice, de elaborare a unei Convenţii care să angajeze răspunderea statelor semnatare atât referitor la obligaţia de a incrimina faptele săvârşite prin intermediul sistemelor informatice, cât şi în ce priveşte dispoziţii procedurale şi de asistenţă judiciară internaţională în acest domeniu.

În consecinţă, a fost constituit un comitet de experţi privind criminalitatea informatică, care a elaborat ceea ce avea să devină una dintre cele mai mediatizate convenţii internaţionale, Convenţia Consiliului Europei asupra Criminalităţii informatice, semnată la Budapesta la 23 noiembrie 2001. Aceasta tinde să devină un instrument juridic global fiind semnată şi ratificată de un număr din ce în ce mai mare de state din întreaga lume.

Momentul apariţiei Convenţiei coincide cu creşterea importanţei comerţului electronic, proprietăţii intelectuale, accesului rapid şi facil la internet şi utilizării pe scară largă a telefoniei mobile.

Analizând conţinutul prevederilor articolelor din Convenţie se poate presupune că prin acest act normativ legiuitorul european a avut drept principal scop să ajute statele să depăşească acele piedici şi provocări asociate de regulă activităţilor de investigaţie în mediul digital. Astfel de provocări ar putea fi considerate ca fiind: dificultatea de a identifica infractorul cibernetic, dificultatea de a soluţiona problema volatilităţii datelor în forma lor electronică şi menţinerea rapidităţii impuse în acest tip de investigaţie şi a secretului impus de aceasta, precum şi determinarea gradului de extindere a acestui fenomen infracţional.

Convenţia Consiliului Europei privind crimalitatea informatică are un triplu obiectiv. În primul rând aceasta defineşte dreptul penal material în cuprinsul Capitolului II, Secţiunea I, care constituie un efort de armonizare legislativă, având drept crearea unei baze comune de infracţiuni. În al doilea rând, se armonizează măsurile de investigare şi procedurile penale în cadrul Capitolului II, Secţiunea a II-a. În al treilea rând se deschid căi pentru cooperarea internaţională în cuprinsul Capitolului III.

Convenţia are patru capitole: I – Înţelesul unor termene şi expresii; II – Măsuri necesare a fi luate la nivel naţional – Drept penal şi procedură penală; III – Cooperarea internaţională şi IV – Dispoziţii penale.

Secţiunea I a Capitolului al II-lea (Dispoziţii de drept penal) se referă la atât la incriminarea unor fapte ca infracţiuni, cât şi la alte aspecte de drept material, referitoare la răspunderea penală, participaţie şi sancţiuni.

Sunt definite aici nouă infracţiuni care sunt grupate în patru categorii diferite. Astfel, sunt considerate infracţiuni ce aduc atingere confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice: accesarea ilegală (art. 2), interceptarea ilegală (art. 3), alterarea integrităţii datelor (art. 4), alterarea integrităţii sistemelor (art. 5) şi abuzurile asupra sistemelor (art. 6). Sunt prevăzute ca infracţiuni în legătură cu mediul informatic: falsificarea informatică (art. 7) şi frauda informatică (art. 8). O altă categorie de infracţiuni se referă la pornografia infantilă (art. 9), iar ultima categorie face referire la infracţiuni care aduc atingere proprietăţiii intelectuale şi drepturile conexe (art. 10).

Articolul 8 din Convenţie, care se referă la infracţiunea de fraudă informatică, stipulează adoptarea unor măsuri legislative care se dovedesc necesare pentru a incrimina ca infracţiune potrivit dreptului intern al unui stat, *fapta intenţionată şi fără drept de a cauza un prejudiciu patrimonial unei alte persoane prin:*

- *orice introducere, alterare, ştergere sau suprimare a datelor informatice;*

- *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.*

Secţiunea a II-a a Capitolului al II-lea cuprinde dispoziţii procedurale în materie penală, aplicabile în cazul comiteriii infracţiunilor stipulate în Secţiunea I. Astfel, se consacră măsuri referitoare la: conservarea rapidă a datelor informatice stocate (art. 16), privind conservarea şi dezvăluirea parţială rapidă a datelor referitoare la trafic (art. 17), privind ordinul de punere la dispoziţie a datelor (art. 18), privind percchezitia şi sechestrarea datelor informatice stocate (art. 19), privind colectarea în timp real a datelor referitoare la trafic (art. 20), precum şi interceptarea datelor referitoare la conţinut (art. 21). Totodată, sunt prevăzute dispoziţii referitoare la competenţă.

Capitolul al III – lea conţine dispoziţii referitoare la asistenţa judiciară penală în materie penală în privinţa infracţiunilor comise prin mijloace informatice, incluzând şi dispoziţii referitoare la extrădare.

Capitolul al IV – lea cuprinde prevederi referitoare la semnare şi intrare în vigoare, aderare, aplicarea teritorială, efectele Convenţiei, declaraţii, clauza federală, rezervele, statutul şi retragerea rezervelor, amendamente, rezolvarea dezacordurilor, reunirea părţilor, denunţarea şi notificarea.

Comisia care a elaborat Convenţia a luat în calcul perpetua dezvoltare a mediului digital şi necesitatea aducerii în timp de amendamende sau modificări. Astfel că, în art. 44 se consacră că vor putea fi propuse amendamente de către fiecare parte, iar acestea vor fi comunicate de către secretarul general al Consiliului Europei statelor membre care au participat la elaborarea Convenţiei, precum şi fiecărui stat care a aderat sau care a fost invitat să, în conformitate cu dispoziţiile art. 37. Orice amendamedament propus de către una dintre părţi va fi comunicat Comitetului European pentru Probleme criminale (CDPC), care va prezenta avizul său Comitelului de Miniştri cu referire la acel amendament. Comitetul de Miniştri va studia amendamentul propus şi avizul înaintat de CDPC şi, după consultarea statelor membre, care sunt părţi ale Convenţiei, va putea adopta amendamentul. Textul oricărui amendament care a fost adoptat de către Comitetul de Miniştri în conformitate cu paragraful 3al art. 44 va fi comunicat părţilor pentru acceptare.

Cei care s-au opus ratificării acestui act normativ au invocat printre altele: restrângerea libertăţii de exprimare în mediul digital, sporirea considerabilă a puterilor de investigare ale poliţiei, parchetelor sau a altor organisme de natura guvernamentală precum şi cerinţele tot mai sporite atât pentru companii dar şi pentru cetăţeni de a furniza organelor de cercetare informaţii care conduc la încălcarea libertăţilor cetăţeneşti.

Însă, Convenţia include inclusiv măsuri de protecţie a drepturilor şi libertăţilor omului, astfel, în prevederile art. 15 (Condiţii şi măsuri de protecţie) se precizează că fiecare dintre părţile semnatare va veghea ca stabilirea, realizarea şi aplicarea prerogativelor şi a procedurilor stipulate în actul normativ să fie supuse condiţiilor şi măsurilor de protecţie prevăzute în dreptul intern care trebuie să asigure o protecţie adecvată drepturilor şi libertăţilor omului, în special a dreptrilor stabilite în conformitate cu instrumentele internaţionale aplicabile privind drepturile omului, precum Convenţia Consiliului Europei pentru apărarea drepturilor omului şi a libertăţilor fundamentale (1950) sau a Pactului internaţional privind drepturile civile şi politice al Naţiunilor Unite.

Tot la nivelul Uniunii Europene, un alt document important îl reprezintă **Directiva 2013/40/UE** [39] **a Parlamentului European şi a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice** şi de înlocuire a deciziei-cadru 2005/222/JAI a Consiliului.

De subliniat faptul că Uniunea Europeană are o capacitate restrânsă de a legifera în domeniul dreptului penal, care a fost considerată întotdeauna ca un apanaj al suveranităţiii naţionale. Uniunea

Europeană reprezintă în primul rând o organizaţie a politicilor comerciale, având competenţe limitate în reglementarea dreptului penal. Faptul că aceasta are un drept de a legifera, chiar şi restrâns, în domeniul dreptului penal este o consecinţă a faptului că infracţiunea constituie un impediment în calea desfăşurării comerţului între statele membre ale Uniunii Europene, în vreme ce pentru o dezvoltare economică şi socială durabilă este nevoie de o cooperare judiciară eficientă în domeniul dreptului penal.

Dispoziţiile art. 83 alin. (1) din Tratatul privind funcţionarea Uniunii Europene [180] permit statelor membre ale Uniunii Europene să adopte directive care să stabilească norme minime cu privire la definirea infracţiunilor şi a sancţiunilor în domenii ale criminalităţii de o gravitate deosebită, de dimensiune transfrontalieră, ce rezultă din natura sau impactul acestor infracţiuni, ori din nevoia specială de a le combate pornind de la o bază comună. Infracţiunile care prezintă o gravitate deosebită şi un caracter transfrontalier sunt următoarele: terorismul, traficul de persoane şi exploatarea sexuală a femeilor şi copiilor, traficul ilicit de droguri, traficul ilicit de arme, spălarea banilor, corupţia, criminalitatea informatică şi criminalitatea organizată.

Revenind la directiva sus menţionată, în conformitate cu prevederile art. 1, acest instrument juridic îşi propune stabilirea unor norme minime privind definrea infracţiunilor şi a sancţiunilor penale relevante în domeniul atacurilor împotriva sistemelor informatice. În acelaşi timp această Directivă urmăreşte dezvoltarea unui cadru legal referitor la prevenirea unor astfel de infracţiuni, precum şi îmbunătăţirea cooperării dintre organele de punere în aplicare a legii.

În cuprinsul art. 2 din Directivă sunt prezentate mai multe definiţii, precum noţiunile de sistem informatic şi date informatice. Sistemul informatic este definit ca fiind un dispozitiv sau grup de dispozitive interconectate sau omoloage, dintre care unul sau mai multe asigură, prin intermediul unui program, prelucrarea automată a datelor informatice, precum şi datele informatice stocate, prelucrate, recuperate sau transmise de acest dispozitiv sau grup de dispozitive în vedera exploatării, a utilizării şi a întrţinerii lor Totodată, datele informatice se referă la o reprezentare de fapte, informaţii sau concepte într-o formă adecvată pentru prelucrare într-un sistem informatic, inclusiv un program care permite unui sistem informatic să execute o funcţie.

Directiva 2013/40/UE referitoare la atacurile împotriva sistemelor informatice cuprinde 5 categorii de infracţiuni săvârşite împotriva sistemelor informatice [1, p.374-383].

Prima categorie, prevăzută de art. 3 se referă la *accesarea ilegală a sistemelor informatice*. Această categorie de infracţiuni cuprinde o serie de atacuri informatice, cunoscute în doctrina de specialitate sub numele de hacking. Infracţiunea constă în accesarea cu intenţie şi fără drept a unui sistem informatic sau a unei părţi a acestuia prin încălcarea unei măsuri de securitate cum ar fi parolele sau codurile de criptare. Infracţiunea de accesare ilegală a sistemelor informatice trebuie să nu constituie un caz minor. În conformitate cu cele stipulate în Directivă, un caz poate fi considerat minor

în situaţiileîn care prejudiciile cauzate de infracţiune şi riscul la adresa intereselor publice sau private este nesemnificativ sau de alta natură încât aplicarea unei sancţiuni penale în cadrul limitelor legale sau angajarea răspunderii penale nu este necesară.

Al doilea tip de infracţiune este stipulată de art. 4 din Directivă şi se referă la *afectarea ilegală a integrităţii sistemului informatic*. Ea constă în perturbarea gravă sau întreruperea funcţionării unui sistem informatic prin introducerea, transmiterea, periclitarea, ştergerea, deteriorarea, modificarea, eliminarea datelor informatice sau prin a le face inaccesibile. Cel mai cunoscut atac împotriva unui sistem informatic care afectează integritatea sistemului informatic este atacul Denial of Service – DOS (refuzul serviciului). Alte atacuri împotriva unui sistem informatic care afectează integritatea acestuia sunt atacurile bazate pe programe maliţioase care îşi propun infectarea computerului, cum ar fi, spre exemplu, viruşii. La fel ca şi în cazul articolului precedent, infracţiunea de afectare ilegală a integrităţii sistemului informatic trebuie să nu constituie un fapt minor.

Al treilea tip de infracţiune se referă la afectarea ilegală a integrităţii datelor informatice şi constă ştergerea, periclitarea, deteriorarea, modificarea, eliminarea datelor informatice dintr-un sistem informatic sau în a le face inaccesibile. Această categorie a infracţiunilor informatice cuprinde mai multe varietăţi de atacuri informatice, dintre care cel mai cunoscut este utilizarea troienilor. La fel ca şi în cazul articolelor precedente, infracţiunea de afectare ilegală a integrităţii datelor informatice trebuie să nu reprezinte un caz minor.

A patra categorie de infracţiuni este prevăzută de art. 6 se referă la interceptarea ilegală şi constă în interceptarea prin mijloace tehnice a unor transmisii private de date informatice către un sistem informatic. O metodă des întâlnită în realizarea acestui demers infracţional este, spre exemplu, utilizarea unui keylogger. Acţiunea de interceptare prin folosirea mijloacelor tehnice presupune ascultarea, monitorizarea sau supravegherea conţinutului comunicaţiilor, fie direct, prin accesarea şi utilizarea sistemului informatic, fie indirect, prin utilizarea unor dispozitive electroice de ascultare şi/sau înregistrare. De asemenea, la fel ca în infracţiunile precedente din Directivă, şi infracţiunea de interceptare ilegală trebuie să nu reprezinte un caz minor.

A cincea categorie de infracţiuni se referă la instrumenele care servesc la săvârşirea infracţiunilor sus-menţionate. Astfel se cere statelor membre adoptarea de măsuri în vederea incriminării drept infracţiuni a producerii, vânzării, procurării în vederea utilizării, importului sau distribuirii următoarelor instrumente:

- un program de calculator, conceput sau adaptat în principal în scopul săvârţirii infracţiunilor informatice;

- o parolă de calculator, un cod de acces sau date similare, prin care un întreg sistem informatic sau orice parte a acestuia poate fi accesat (ă).

O prevedere importantă este cuprinsă în art. 10 alin. (1) al Directivei care permite angajarea răspunderii persoanelor juridice pentru oricare dintre infracţiunile sus-menţionate. atunci când săvârşite în beneficiul lor de către orice persoană, care acţionează fie în nume propriu, fie ca parte a unui organism al persoanei juridice. În ambele cazuri se impune ca persoana să ocupe o funcţie de conducere în cadrul persoanei juridice, în temeiul unei împuterniciri din partea persoanei juridice, unei prerogative de a lua decizii în numele persoanei juridice sau unei prerogative de a exercita controlul în cadrul persoanei juridice.

Răspunderea persoanelor juridice nu exclude aplicarea procedurilor penale împotriva persoanelor fizice în calitate de autori, instigatori sau complici la săvârşirea oricăreia dintre infracţiunile prevăzute la art. 3-8 din Directivă.

În conformitate cu prevederile art. 11 din Directivă, sancţiunile aplicate persoanelor juridice includ amenzi penale sau administrative, precum şi alte sancţiuni, cum ar fi, spre exemplu: decăderea din dreptul de a primi beneficii publice sau ajutor public; interdicţia temporară sau chiar permanentă de a desfăşura activităţi comerciale; punerea sub supraveghere judiciară; lichidarea judiciară; închiderea temporară sau permanentă a unităţilor care au servit la săvârşirea infracţiunii.

3.2. Incriminarea fraudei informatice în legislația altor state

Ca urmare a evoluţiei fireşti a societăţii, diverse colectivităţi şi-au adoptat diferite reguli, concepte, norme, legi etc. de protecţie proprie faţă diverse atentate asupra drepturilor, libertăţilor şi intereselor lor legitime. Reuşita unor măsuri în raport cu altele este dictată de o serie de factori, atât interni, cât şi externi, însă evoluţia şi perfectarea continuă a acestora poate fi atinsă doar în condiţiile adoptării şi influienţării lor reciproce.

Cercetarea comparativă încearcă să răspundă, în cea mai mare parte, la aceleași probleme specifice analizei calitative[47]. Analiza comparativă este un instrument puternic în mâna juristului-cercetător, destinat perfectării calitative a legislaţiei statului propriu, pe baza prevederilor şi experienţei obţinute de alte state.

Domeniul informatic, fiind unul relativ nou, este şi el afectat de o multitudine de atentate criminale, protecţia contra cărora se efectuează inclusiv şi prin mijloace de drept penal. Această legitate este prevăzută în toate statele lumii, fapt pentru care ne-am propus să analizăm legislaţiile penale ale mai multor ţării întru descoperirea normei care să prevadă frauda informatică.

În această ordine de idei, în conformitate cu art. 249 C. pen. al României, amplasat la Capitolul IV a părţii speciale (*Fraude comise prin sisteme informatice şi mijloace de plată electronice*), frauda informatică presupune: „*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" [25].

Similitudinea dispoziţiilor normei ce stipulează frauda informatică în legislaţia Republicii Moldova şi a României sunt evidente. Prin excepţie, deosebirea dintre aceste modele legislative de incriminare a fraudei informatice constă în natura urmării prejudiciabile, care este specifică pentru legislaţia penală a fiecărui stat în parte. Astfel, în calitate de urmare prejudicabilă necesară constatării existenţei componenţei de frauda informatică în legislaţia penală a R. Moldova se prezintă daunele în proporţii mari, iar în ceea ce priveşte legislaţia României – cauzarea unei pagube persoanei.

Dacă în Codul penal al Republicii Moldova este oferită noţiunea de daune în proporţii mari, care conform art. 126 C. pen. reprezintă „valoarea bunurilor sustrase, dobândite, primite, fabricate, distruse, utilizate, transportate, păstrate, comercializate, trecute peste frontiera vamală, valoarea pagubei pricinuite de persoană sau de un grup de persoane, care, la momentul săvârşirii infracţiunii, depăşeşte 40 de salarii medii lunare pe economie prognozate, stabilite prin hotărârea de Guvern în vigoare la momentul săvârșirii faptei[25]", atunci Codul penal al României nu elucidează lexemul: „pagube", acesta urmând a fi interpretat în conformitate cu regulile semantice sau gramaticale generale.

Diferenţe de reglementare există şi în privinţa regimului sancţionator, astfel încât art. 249 C. pen. al României prevede o pedeapsă cu închisoare de la 2 la 7 ani, iar art. 260^6 C. pen. al R. Moldova – închisoare de la 2 la 5 ani pentru componenţa de bază şi de la 4 la 9 ani pentru componenţa calificată, cea din urmă nefiind prezentă în legislaţia penală românească.

În cazul Codului penal al Federaţiei Ruse[218], Capitolul 28 din Secţiunea IX a părţii speciale (*Infracţiuni contra siguranței și ordinii publice*), intitulat „*Infracţiuni în domeniul informaţiei computerizate*", conţine doar 3 componenţe de infracţiuni, şi anume: art. 272 – accesul ilegal la informaţia computerizată, art. 273 – Producerea, utilizarea și distribuirea programelor de calculator maliţioase, art. 274 – Încălcarea regulilor de exploatare a mijloacelor de stocare, prelucrare sau transmitere a informaţiei computerizate şi a reţelelor informaice şi de telecomunicaţii.

Infracţiunea de fraudă informatică este regăsită în Secţiunea VII-a (*Infracţiuni comise în sfera economică*), Capitolul 21 (*Infracţiuni contra proprietăţii*), la art. 159.6, cu următorul conţinut: „*Frauda în domeniul informației computerizate, adică sustragerea bunurilor sau obţinerea drepturilor de proprietate asupra bunurilor prin introducerea, ștergerea, blocarea, modificarea informației computerizate sau altă intervenţie în funcţionarea mijloacelor de stocare, procesare sau transmitere a datelor informatice sau a rețelelor informatice şi de telecomunicații*" [218].

În calitate de semne circumstanţiale de agravare a răspunderii penale pentru comiterea fraudei informatice, la alin. (2), (3), (4), art. 159.6 C. pen. al Federaţiei Ruse, se prevăd următoarele circumstanţe, după cum urmează:

- comise de un grup de persoane prin înţelegere prealabilă, precum şi prin cauzarea daunelor considerabile cetăţeanului;
- comise de către o persoană cu folosirea situaţiei de serviciu, precum şi în proporţii mari;
- comise de un grup organizat sau în proporţii deosebit de mari.

Deosebirile dintre legislaţia penală a Republicii Moldova şi cea a Federaţiei Ruse în ceea ce priveşte incriminarea infracţiunii de fraudă informatică sunt multiple şi decisive.

La nivel semantic, dacă legiuitorul autohton prevede drept metodă de comitere a fraudei informatice – restricţionarea accesului la datele informatice, atunci în art. 159,6 C. pen. al Federaţiei Ruse, în calitate de metodă adiţională de comitere a infracţiunii este prevăzută blocarea informaţiei computerizate. Ambele noţiuni „restricţionare" şi „blocare" comportă acelaşi sens, diferă doar modul de exprimare lexicală. Acelaşi lucru se întâlneşte la modalitatea de „împiedicare în orice mod a funcţionării unui sistem informatic" prevăzută la art. 260^6 C. pen. şi „altă intervenţie în funcţionarea mijloacelor de stocare, procesare sau transmitere a datelor informatice sau a reţelelor informatice şi de telecomunicaţii" prevăzută la art. 159.6 C. pen. al Federaţiei Ruse.

La nivel compoziţional, consumarea fraudei informatice în legislaţia penală a Republicii Moldova este dependentă de survenirea daunelor în proporţii mari, deci componenţa de infracţiune este una materială, pe când legislaţia penală a Federaţiei Ruse nu prevede survenirea cărorva urmări prejudiciabile. Consumarea infracţiunii prevăzute la art. 159.6, alin. (1) C. pen. al Federaţiei Ruse depinde de momentul înscrierii banilor pe contul controlat de cel vinovat[212], indiferent, de prejudiciul cauzat prin această faptă.

La nivel sancţionator, în ceea ce priveşte pedeapsa penală stabilită pentru componenţa de bază a fraudei informatice, legislatorul din Federaţia Rusă prevede o pedeapsă mai redusă comparativ prevederii similare din legislaţia penală a R. Moldova, şi anume: „amendă de cel mult o sută douăzeci de mii de ruble sau în mărimea salariului ori a altor venituri a condamnatului pentru o perioadă de până la un an, sau prin muncă obligatorie pentru o perioadă de până la trei sute șaizeci de ore, sau munca corecţională pentru o perioadă care nu depăşeşte un an, sau privare de libertate pe un termen de până la doi ani, sau muncă în folosul comunităţii de până la doi ani, sau arest de până la patru luni. Merită de subliniat faptul, că în ceea ce priveşte circumstanţa agravantă „care a cauzat daune în proporţii mari", pedepsa penală pentru frauda informatică în ambele state nu diferă esenţial.

La nivel de circumstanţe agravante, se pune în evidenţă că legiuitorul din Federaţia Rusă prevede şi alte forme de organizare a activităţii criminale, care nu se întâlnesc în legislaţia penală naţională: un grup de persoane prin înţelegere prealabilă sau un grup organizat (cercetarea noţiunilor şi formelor participaţiei penale în legislaţia penală a Federaţiei Ruse excede obiectivul propus de

prezentul studiu). Totodată, frauda informatică prevăzută la art. 260[6] C. pen. al Republicii Moldova nu prevede agravarea răspunderii penale pentru folosirea situaţiei de serviciu.

În secţiunea a 15-a a părţii speciale a C. pen. al Ucrainei [220], intitulată „*Infracţiuni comise în sfera utilizării calculatoarelor*", sunt incluse o serie de infracţiuni din domeniul informatic: Accesul neautorizat la activitatea calculatoarelor, sistemelor automatizate, rețelelor de calculatoare sau de telecomunicații (art. 360), Producerea cu scopul folosirii, distribuirii sau vânzarii de mijloace tehnice sau produse program maliţioase, precum și distribuirea sau vânzarea acestora (art. 361-1), Vânzarea sau distribuirea informațiilor cu acces limitat, care sunt stocate în calculatoare electronice, sisteme automatizate, rețele de calculatoare sau pe purtători de astfel de informații (art- 361-2), Acţiuni neautorizate cu informații prelucrate de calculatoare, sisteme automatizate, rețele de calculatoare sau a celora stocate pe suporturi de informații, de către o persoană care are acces la ele (art. 362), Încălcarea regulilor de exploatare a calculatoarelor, sistemelor automatizate, rețelelor de calculatoare sau a rețelelor de telecomunicații, precum şi a regulilor de protecție a informației prelucrate de acestea (art. 363), Împiedicarea activităţii calculatoarelor, sistemelor automatizate, rețelelor de calculatoare sau a rețelelor de telecomunicații prin distribuirea în masă a mesajelor electronice (art. 363-1). Nici printre acestea, precum şi nici în rândul infracţiunilor contra patrimoniului, stipulate la secţiunea a 6-a a părţii speciale a C. pen. al Ucrainei, nu a fost depistat un articol separat destinat fraudei informatice.

Norma penală ce prevede sancţionarea acţiunilor de fraudă informatică este inclusă în calitate de circumstanţă agravantă la art. 190 C. pen. al Ucrainei, cu denuimrea marginală de *escrocherie*.

Conform art. 190 C. pen. al Ucrainei: „*1. Dobândirea bunurilor altei persoane sau obţinerea drepturilor asupra acestora prin înşelăciune sau abuz de încredere (escrocherie) - se pedepseşte cu amendă în mărime de până la cincizeci de venituri minime neimpozabile, sau muncă corecțională pe un termen de până la doi ani, sau cu privarea de libertate pe un termen de până la trei ani. 2. Escrocheria săvârşită în mod repetat, sau în urma unei înţelegeri prealabile de către un grup de persoane, sau care a provocat daune în proporţii considerabile - se pedepseşte cu amendă în mărime de la cincizeci la o sută de venituri minime neimpozabile sau muncă corecțională pentru un termen de la unu la doi ani, sau privare de libertate pe un termen de până la cinci ani, sau închisoare pe un termen de până la trei ani. 3. Escrocheria săvârşită în proporţii mari sau în urma unor operaţii ilegale efectuate prin intermediul calculatoarelor - se pedepsește cu închisoare pe un termen de la trei la opt ani. 4. Escrocheria săvârşită în proporţii deosebit de mari sau de un grup organizat - se pedepseşte cu închisoare pe un termen de la cinci la doisprezece ani, cu confiscarea averii*[220].

Modul de descriere a fraudei informatice de legiuitorul din Ucraina denotă mai multe distincţii vădite dintre aceasta şi modelul legislativ al fraudei informatice prevăzut de legislaţia Republica Moldova, care, printre altele: se consumă independent de survenirea urmării prejudiciabile sub formă

de daună în proporţii mari; nu implică enumerarea modalităţilor realizării faptei prejudiciabile sub care se prezintă escrocheria; se sancţionează mai aspru.

În conformitate cu C. pen. al Republicii Belarus[210], Partea specială, Titlul XII-a, Capitolul 31, denumit „Infracţiuni contra securităţii informatice" se prevăd următoarele infracţiuni din domeniul informatic:

- art. 349 – Accesul neautorizat la informaţia computerizată;
- art. 350 – Modificare informaţiei computerizate;
- art. 351 – Diversiune informatică;
- art. 352 – Dobândirea ilegală a informaţiei computerizate;
- art. 353 – Producerea sau vânzarea mijloacelor speciale destinate accesului neautorizat la un sistem sau rețea informatică;
- art. 354 – Proiectarea, folosirea sau distribuirea programelor maliţioase;
- art. 355 – Încălcarea regulilor de exploatare a sitemelor sau reţelelor informatice.

Analiza componenţelor acest din urmă infracţiuni scoate în evidenţă absenţa semnelor ce ar putea fi atribuite fraudei informatice.

Nici art. 209 C. pen. al Republicii Belarus (*Escrocheria*) nu prevede careva formă de realizare a infracţiunii specifică mediului informatic.

Totuşi, în Titlul al VIII-lea a Părţii speciale a C. pen. al Republicii Belarus, Capitolul 24, intitulat „*Infracţiuni împotriva proprietăţii*" se prevede o normă specială, dedicată protejării contra tuturor formelor de sustragere în mediul informatic, şi anume art. 212 C. pen. – Sutragerea prin utilizarea tehnologiilor informatiţionale.

Conform textului de lege: „*Sustragerea bunurilor prin modificarea informațiilor prelucrate într-un sistem informatic, stocate pe suporturi de informaţii sau vehiculate într-o rețea de date ori prin introducerea în sistemul informatic de informații false – se pedepsește cu amendă sau privarea de dreptul de a ocupa anumite funcții sau de a exercita o anumită activitate ori arestare, sau privarea de libertate pe un termen de până la trei ani, sau închisoare pentru același termen*" [210].

Astfel, una din deosebirile de bază dintre forma fraudei informatice prevăzute de legislaţia Republicii Belarus şi cea prevăzută de legislaţia autohtonă constă în aceea că numărul modalităţilor de comitere a infracţiunii în cazul Republicii Moldova este mai mare, fiind incluse astfel de forme de realizare a faptei prejudiciabile precum: ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic.

Cea de-a două diferenţă esenţială dintre incriminarea fraudei informatice în legislaţiile penale ale acestor două state constă în faptul că, pentru consumarea fraudei informatice conform C. pen. al Republicii Moldova este necesară survenirea consecinţelor prejudiciabile sub forma de daune în proporţii mari, pe când în C. pen. al Republicii Belarus astfel de urmare prejudiciabilă determină

existenţa componenţei cu circumstanţe agravante, prevăzute la alin. (3), art. 212 C. pen. al Republicii Belarus. Pedeapsa penală în acest caz, în conformitate cu legislaţia Republicii Belarus, se prezintă ca: închisoare pe un termen de la doi până la șapte ani, cu amendă sau fără de aceasta și confiscarea bunurilor sau fără confiscare și privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate sau fără astfel de privare.

Dintre alte circumstanţe agravante specifice fraudei informatice, dar care nu sunt prevăzute de art. 260^6 C. pen. al Republicii Moldova, sunt:

- săvârşirea în mod repetat, sau de un grup de persoane la înţelegere prealabilă sau în legătură cu accesul neautorizat la informaţiile computerizate (alin. (2), art. 212 C. pen. al Republicii Belarus),
- comiterea infracţiunii de către un grup organizat (alin. (4), art. 212 C. pen. al Republicii Belarus).

Codul penal al Poloniei[217] nu prevede vreun capitol aparte menit să protejeze proprietatea persoanei atunci când aceasta se reflectă în informaţiile stocate în spaţiul cibernetic. Infracţiunile din domeniul informatic, spre exemplu alterarea integrităţii datelor informatice dintr-un sistem informatic (art. 268, alin. (2) Cod penal polonez) prevăzută în Capitolul XXXIII al Părţii speciale a Codul penal al Poloniei (*Infracţiuni împotriva securităţii informaţiei*), condiţionează existenţa componenţei calificate de infracţiune şi sunt prevăzute în întrega parte specială a Codului penal polonez.

În ceea ce priveşte frauda informatică, aceasta din urmă se localizează în cadrul Capitolului XXXV al Părţii speciale (*Infracţiuni contra patrimoniului*), şi anume la art. 287 C. pen. polonez, având următorul conţinut: „*§1. Cineva, cine având scopul de a obține un beneficiu patrimonial sau de a provoca daune altei persoane, fără a avea acest drept, influienţează asupra procesării, stocării sau transferării de informații ori modifică, șterge sau introduce o nouă înscriere pe un suport de stocare a informaţiilor, se pedepseste cu închisoare pe un termen de la 3 luni la 5 ani. § 2. În cazuri mai puţin importante, făptuitorul va fi supus amenzii, privării de libertate sau închisorii pe un termen de până la 1 an. § 3. În cazul în care frauda se săvârşeşte în privinţa unei persoane apropiate, urmărirea penală începe la cererea victimei*” [217].

Se observă uşor că, deşi nu sunt utilizate expresii similare celor întâlnite în legislaţia penală naţională – influienţarea asupra procesării, stocării sau transferării de informaţii încorporează sensul de restricţionare a accesului la datele informatice, precum şi pe cel de împiedicare în orice mod a funcţionării unui sistem informatic –, totuşi conţinutul modalităţilor normative de comitere a infracţiunii şi scopul în care se săvârşeşte fapta prejudiciabilă sunt asemănătoare.

Diferenţa primordială între prevederile art. 260^6 C. pen. al Republicii Moldova şi art. 287 C. pen. al Poloniei constă în urmarea prejudiciabilă sub formă de daune în proporţii mari, specifică doar legislaţiei penale a Republicii Moldova. În calitate de delimitări adiţionale dintre legislaţiile penale ale

acestor două state evoluează prezenţa unei circumstanţe atenuante, prevăzute la art. 287, alin. (2) C. pen. polonez şi a unui caz particular de pornire a urmăririi penale la cererea prealabilă a victimei, prevăzute la art. 287, alin. (3) C. pen.al Poloniei. Este de remarcat faptul că, în confomitate cu art. 276 C. proc. pen. al Republicii Moldova[24], nu este obligatoriu ca urmărirea penală în cazul fraudei informatice (art. 260^6 C. pen. al Republicii Moldova) să pornească în baza plângerii prealabile a victimei.

O normă apropiată după conţiut cu art. 260^6 C. pen. al Republicii Moldova, se regăsește în C. pen. al Franţei[219], care, în Cartea a III-ea (*Despre infracţiunile şi delictele contra proprietăţii*), secţiunea II-a (*Despre alte atentate patrimoniale*), Capitolul III (*Despre atentatele asupra sistemelor automatizate de prelucrare a datelor*), prevede în cadrul a 4 articole (de la art. 323-1 şi până la art. 323-4) un model legislativ special de incriminare a fraudei informatice.

Astfel, conform art. 323-1 C. pen. al Franţei: „*Fapta, exprimată prin obţinerea sau salvarea, prin înşelăciune, a accesului total sau parţial la un sistem automatizat de prelucrare a datelor, se pedepseşte cu închisoare pe un termen de 1 an şi o amenda în măsime de 100.000 de franci.*

În cazul în care fapta a provocat distrugerea sau modificarea datelor ţinute în sistem sau înrăutăţirea funcţionării acestui sistem, pedeapsa o va constitui închisoarea pe un termen de 2 ani şi amenda în mărime de 200.000 de franci" [219].

Art. 323-2 C. pen. al Franţei prevede: „*Fapta, exprimată prin împidicarea funcţionării normale a sistemului automatizat de prelucrare a datelor, se pedepseşte cu închisoare pe un termen de 3 ani şi amendă de 300.000 de franci*" [219].

În conformitate cu art. 323-3 C. pen. al Franţei: „*Fapta, exprimată prin introducerea prin înşelăciune a datelor informatice în cadrul unui sistem automatizat de prelucrare a datelor, precum şi modificarea sau distrugerea prin înşelăciune a conţinutului datelor stocate în sistem, se pedepseşte cu închisoare pe un termen de 3 ani şi amendă în mărime de 300.000 de franci*" [219].

În cazul art. 323-4 C. pen. al Franţei se prevede în calitate de circumstanţă agravantă: „*participarea într-un grup organizat sau la o înţelegere prealabilă, îndreptată spre pregătirea uneia sau a mai multor fapte infracţionale prevăzute de art. 323-1, 323-2, 323-3, dacă această pregătire se caracterizează prin una sau mai multe acţiuni obiective, se pedepseşte conform sancţiunii prevăzute la articolele ce prevăd astfel de fapte infracţionale sau conform normei ce prevede o sancţiune mai aspră*" [219].

Pe lângă diferenţele textuale pe care le comportă norma penală în raport cu prevederile din C. pen. al Republicii Moldova, se evidenţiază clar lipsa obligativităţii producerii a cărorva urmări prejudiciabile necesare întru consumarea infracţiunii, indferent de forma pe care o preia aceasta. Respectiv, se confirmă o dată în plus, că consecinţa prejudiciabilă sub formă de daune în proporţii

mari, în ceea ce ţine de componenţa de bază a fraudei informatice, este specifică doar legislaţiei penale a Republicii Moldova.

În plan subsidiar, prevederile legislative ale C. pen. al Franţei nu indică la un scop determinat pentru care se acţionează ilegal asupra sistemului informatic, deşi nu se exclude şi scopul obţinerii unui beneficiu material pentru sine sau pentru altul.

Spre deosebire de legislaţia penală ale altor ţări, în cadrul Codului penal al Republicii Federative Germane[213] se dedică o secţiune aparte (secţiunea XXII a părţii speciale) pentru infracţiunile de escrocherie şi abuz de încredere (art. 263 – art. 266b C. pen.). În rândul acestor infracţiuni, o deosebită atenţie o atrage art. 263a C. pen., care poartă denumirea de *Fraudă informatică*.

În conformitate cu art. 263a C. pen. al Republicii Federative Germane: „*Cel ce acţionează în scopul obţinerii pentru sine sau pentru o persoană terţă a unui avantaj patrimonial ilicit şi prin aceasta cauzează o daună proprietăţii altei persoane, prin acţionarea asupra rezultatelor prelucrării datelor informatice, creând programe incorecte, folosind date incorecte sau incomplete, folosind neautorizat datele informatice sau influienţând asupra unui asemenea proces în alt mod ilegal, se pedepseşte cu închisoare pe un termen de până la 5 ani sau cu amendă*” [213].

Discrepanţa dintre art. 260^6 C. pen. al Republicii Moldova şi art. 263a C. pen. al Republicii Federative Germane constă, ca şi în cazul legislaţiilor penale ale statelor examinate anterior, în natura urmării prejudiciabile. Atfel, legiuitorul autohton invocă stringent obligativitatea survenirii consecinţelor prejudiciabile care preiau forma daunelor în proporţii mari, pe când legislativul din Republica Federativă Germană se limitează la specificaţia: „*daună proprietăţii altei persoane*”, fără să se axezeze pe un anumit cuantum concret al acestora.

În partea sancţiunii, politica penală a Republicii Moldova în ceea ce vizează frauda informatică, prin stabilirea limitelor minime ale amenzii, muncii neremunerate în folosul comunităţii şi a termenului de închisoare, este mai aspră.

Codul penal al Belgiei [214], în partea specială, la Capitolul 2 (*Infracţiuni bazate pe înşelăciune*), Secţiunea III (*Despre escrocherie ţi înşelăciune*) şi Secţiunea V (*Despre alte tipuri de înşelăciune*), nu prevede nici o normă care ar face referinţă la spaţiul informatic de comitere a escrocheriei.

Totuşi, cercetarea acestui act normativ scoate în evidenţă prezenţa unui capitol aparte destinat protecţiei sistemelor informaţionale şi a datelor ce sunt prelucrate în acestea, şi anume Capitolul X (*Infracţiuni contra confidenţialităţii, inviolabilităţii şi accesibilităţii sistemelor informatice şi a datelor care sunt stocate, procesate şi transmise de acestea*). Acest capitol include doar 2 articole: art. 550bis şi art. 550ter.

Art. 550bis. al C. pen. al Belgiei este destinat protecţiei contra acţiunilor de acces neautorizat la informaţia computerizată, iar art. 550 ter. al C. pen. al Belgiei este menit să protejeze orice formă de fals informatic. Deşi ambele articole nu corespund cu obiectul de studiu al prezentei cercetări, cu toate acestea, normele penale în cauză conţin unele prevederi ce ar putea fi catalogate drept componenţă de fraudă informatică.

Astfel, un scop special de înşelăciune sau cauzare a daunei materiale este prevăzut la:

1. alin. (2), art. 550bis. – „*Acel care, având scopul de a înşela sau de a cauza prejudiciu material, depăşeşte atribuţiile de serviciu în ceea ce priveşte accesul la sistemele informatice, se pedepseşte cu închisoare pe un termen de la 6 luni la 2 ani şi amendă în mărime de la 26 franci la 25 000 franci sau doar cu una din pedepsele nominalizate*";
2. alin. (3), art. 550bis. – „*Acel care, se află în situaţia prevăzută de alin (2) şi care: 1. extrage, indiferent de metodă, datele stocate, procesate sau transmite în cadrul unui sistem informatic; 2. foloseşte prin orice metodă sistemul informatic ce aparţine unei persoanei terţe sau se foloseşte de acest sistem informaţional pentru a accesa sistemul informatic al unei persoane terţe; 3. cauzează un prejudiciu, chiar şi din imprudenţă, sistemului informatic sau a datelor care sunt stocate, procesate sau transmise de acest sistem, aparţinând unei persoane terţe, se pedepseşte cu închisoare pe un termen de la 1 an la 3 ani şi cu amendă în mărime de la 26 franci pînă la 50 000 franci sau doar cu una din pedepsele nominalizate*";
3. alin. (5), art. 550bis. – „*Acel care, cu scopul de înşelăciune sau cauzare a unui prejudiciu material caută, acumulează, oferă, pune la dispoziţia terţilor, distribuie sau comercializează date informatice care au fost stocate, prelucrate, transmise într-un sistem informatic şiprin intermediulcărora pot fi comise faptele prevăzute la alin. (1)-(4), se pedepseşte cu închisoare pe un termen de la 6 luni la 3 ani şi cu amendă în mărime de la 26 franci pînă la 100 000 franci sau doar cu una din pedepsele nominalizate*"
4. alin. (4), art. 550ter. – „*Acel care, cu scopul de înşelăciune sau cauzare a unui prejudiciu material, analizează, pune la dispoziţia terţilor, distribuie sau comercializează datele informatice stocate,procesate, sau transmise de un sistem informatic, în acel timp cât este în cunoştinţă de posibilitatea folosirii acestor date pentru în vederea falsificării informaţiilor stocate în acest sistem informatic, împiedicatrea, totală sau parţială, a funcţionării corecte a sistemuluiinformatic, se pedepseşte cu închisoare pe un termen de la 6 luni la 3 ani şi cu amendă în mărime de la 26 franci pînă la 100 000 franci sau doar cu una din pedepsele nominalizate*" [214].

Deşi diferenţele dintre prevederile legislative ce incriminează infracţiunea de frauda informatică în legislaţia penală a Republicii Moldova şi a Belgiei sunt multiple, de esenţă rămâne

absenţa unui cuantum anumit al proporţiilor urmărilor prejudiciabile, specific fraudei inforamtice incriminate în C. pen. al Republicii Moldova.

Codul penal al Bulgariei [216] nu conține vreun capitol special consacrat protecției penale a informaţiei computerizate, nici careva norme speciale care să prevadă frauda informatică. Secţiunea IV-a (*Înşelăciunea*) şi Secţiunea VIII-a (*Abuzul de încredere*) a Capitolului 5 (*Infracţiuni contra proprietăţii*) a Părţii speciale a C. pen. al Bulgariei nu conţine vreo dispoziţie cu referire specială la domeniul informatic de săvârşire a infracţiunilor. Aceeaşi situaţie se atestă şi în cadrul C. pen. al Spaniei [215] (art. 248 din Secţiunea I, a Capitolului 4, denumit „*Despre însuşirea proprietăţii prin înşelăciune*", situație care prezumă aplicarea în calitate de normă generală pentru toate cazurile de escrocherie).

Cu referire la sistemul de drept anglo-saxon, specificul incriminării acţiunilor corespunzătoare fraudei informatice este inedit. Spre exemplu, în C. pen. al Canadei, art. 342.1 cu titlul „*Folosirea neautorizată a calculatoarelor*" conține următorul text:

„*Este vinovat de comiterea unei infracţiuni şi urmează a fi condamnat la închisoare pe un termen de cel mult 10 ani, sau este vinovat de comiterea unui delict ce urmează a fi pedepsit în modul corespunzător, cel ce în mod fraudulos şi fără a avea acest drept:*

(a) obține, în mod direct sau indirect, un serviciu prestat prin calculator;

(b) prin intermediul unui dispozitiv electro-magnetic, acustic, mecanic sau alt asemenea dispozitiv, efectuează interceptări, în mod direct sau indirect, a unei transmisii de date informatice efectuate într-un sistem de date;

(c) utilizează sau creează posibilitatea de a fi utilizat, în mod direct sau indirect, un sistem informatic, cu intenția de a comite o infracțiune prevăzută la litera (a) sau (b) a prezentului articol sau în conformitate cu art. 430 în ceea ce ţine de datele sau sistemele informatice;

(d) utilizează, posedă, pune în circulaţie sau oferă altei persoane accesul la o parolă de calculator, care face posibilă comiterea unei infracţiuni în conformitate cu alineatele (a), (b) sau (c) al prezentului articol".

În partea a doua a acestui articol - 342.1 C. pen. al Canadei - se oferă definiţiile la o serie de noţiuni din domeniul informatic, printre care: date computaţionale, parolă de calculator, program de calculator, serviciu prestat prin calculator, sistem informatic, dispozitiv electro-magnetic, acustic, mecanic sau alt asemenea dispozitiv, funcţie, interceptare, circulaţie.

Devine clar că art. 342.1 C. pen. al Canadei înglobează mai multe norme decât frauda informatică, acestuia atribuindu-i-se şi astfel de infracţiuni, care în C. pen. al Republicii Moldova sunt prevăzute la art. 259 (Accesul ilegal la informaţia computerizată), 260^1 (Interceptarea ilegală a unei transmisii de date informatice), 260^2 (Alterarea integrităţii datelor informatice ţinute într-un sistem

informatic), 260[4] (Producerea, importul, comerciali zarea sau punerea ilegală la dispoziţie a parolelor, codurilor de acces sau a datelor similare).

Totodată, pentru consumarea infracţiunii prevăzute la art. 342.1 C. pen. al Canadei nu se cere producerea a cărorva consecinţe prejudiciabile, fapt ce delimitează clar conceptul de fraudă informatică prevăzut în legislaţia penală a Canadei de cea din Republica Moldova.

Este de menţionat că art. 380 C. pen. al Canadei, care prevede răspunderea penală pentru inracţiunea de *escrocherie*, nu include şi careva referinţe la mediul electronic de comitere a infracţiunii.

În raport cu legislaţia penală a Marii Britanii, este bine cunoscut faptul că aceasta nu este codificată, de aceea spectrul infracțiunilor informatice este acoperit de o multitudine de acte normative, printre care: Legea cu privire la utilizarea abuzivă a calculatoarelor din 1990, Legea privind infracţiunile grave din 2015, Directiva Uniunii Europene 2013/40/UE, Regulamentul cu privire la acţiunile ilegale în telecomunicaţii (interceptarea comunicaţiilor) din 2000, Legea cu privire la protecţia datelor din 1988, Regulamentul cu privire la protecţia datelor personale în telecomunicaţii din 1999 etc. [206].

Spre exemplu, pe de o parte Legea cu privire la folosirea abuzivă a calculatoarelor din 1990[204], prevede răspundere penală pentru o serie de fapte ilegale precum este *accesul neautorizat la informaţia computerizată*, actul normativ fiind dedicat totalmente domeniul nou al infracţiunilor din ciberspaţiu. Pe de altă parte, Legea fraudei din 2006 [205], prevede o serie de infracţiuni, care au existat dintotdeauna, dar care capătă noi conotații prin intermediul tehnologiilor informaţionale. Astfel, dacă la art. 1 din Legea fraudei din 2006 sunt descrise modalităţile şi pedepsele pentru escrocherie, atunci la art. 7 se incriminează fapta de producere şi punere în circulaţie a mijloacelor tehnice folosite la comiterea fraudelor, inclusiv cele săvârşite în spațiul informatic.

Vreo normă distinctă dedicată fraudei informatice, în legislaţia penală a Marii Britanii, nu se conține. O paticularitate a sistemului de drept al acestei ţări constă în prezenţa în actele normative a unor *precedente de practică judiciară* - reguli de drept formal şi material - aecstea din urmă fiind divizate şi specificate, în sensul aplicării, pentru fiecare regiune în parte: Scoţia, Irlanda de Nord etc.

Concluziile desprinse din analiza comparativă a legislaţiilor penale ale diferitor state, aparținând atât sistemului de drept romano-germanic, cât şi celui anglo-saxon, privind incriminarea faptelor de fraudă informatică, sunt atât de ordin informativ, cât şi de ordin funcţional și practico-aplicativ.

Cercetarea structurală a legislaţiilor penale ale statelor lumii, aparținând diferitor sisteme de drept, în privinţa infracţiunii de fraudă informatică ne permite să efectuăm o clasificare a acestora, după cum urmează:

- **legi penale ce conţin o normă specială cu privire la frauda informatică**, aceasta fiind inclusă fie într-un capitol distinct dedicat infracţiunilor din domeniul informaticii şi/sau telecomunicaţiilor (Republica Moldova, Franţa, Belgia), fie într-un capitol comun cu alte infracțiuni contra patrimoniului (Federaţia Rusă, România, Republica Belarus, Polonia, Republica Federativă Germană) sau în alte capitole a legii penale (Canada);
- **legi penale ce nu conţin vreo normă specială care să prevadă infracţiunea de fraudă informatică**, aceasta fie că se încadrează în componenţa agravată a infracţiunii de escrocherie (Ucraina, Marea Britanie), fie se include în norma generală ce prevede înşelăciunea sau abuzul de încredere ca metode de comitere a sustragerii (Bulgaria, Spania).

Analiza și evaluarea structurii componenţei de infracţiune a fraudei inforamtice, mai ales în ceea ce ţine de momentul consumării infracţiunii, pune în evidenţă o particularitate specifică doar legii penale a Republicii Moldova în raport cu legislaţiile penale ale altor state, şi anume prezenţa în structura laturii obiective a infracţiunii a urmării prejudiciabile sub formă de daune în proporţii mari. Astfel, spre deosebire de C. pen. al Republicii Moldova, în legislaţia penală ale altor ţări (referindu-ne la statele a căror legislație penală a fost cercetată) urmările prejudiciabile nu condiționează existența infracţiunii de fraudă informatică.

3.3. Reglementări antifraudă informatică și locul incriminării fraudei informatice în legea penală a României și Republicii Moldova

În cadrul acestui compartiment al tezei urmează a fi relevat şi caracterizat sediul normativ aferent legislaţiei româneşti şi a celeia moldoveneşti care stă la baza prevenirii fraudei informatice ca fenomen infracţional. O primă precizare care se impune a fi făcută cu pregnanţă este că mecanismul preventiv cu caracter juridic, în afară de normele incriminatorii, încorporate în legislaţia penală, mai include şi alte legi, care mai stabilesc măsuri de altă natură necesare prevenirii eficiente a criminalității informatice (instituţionale, politice, administrative, economice, tehncie etc.). Prin urmare, înainte de a analiza locul incriminator în sistemul incriminărilor penale a infracţiunii ce face obiect de cercetare în cadrul acestui studiu, ne v-om opri şi la reglementări non-penale, care într-un fel sau altul au ca obiect de reglementare acest domeniu al relaţiilor sociale.

În ceea ce priveşte România, un act normativ de însemnătate îl constituie **Hotărârea 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** [84].

Conform actului normativ sus amintit, statul român îşi asumă rolul de coordonator al activităţilor desfăşurate la nivel naţional pentru asigurarea securităţii cibernetice, în concordanţă cu

demersurile iniţiate la nivel UE şi NATO. Evoluţia rapidă a naturii ameninţărilor cibernetice a necesitat adoptarea, şi de către Organizaţia Nord – Atlantică a unei noi politici în domeniul apărării cibernetice. În acest sens NATO a elaborat un plan de acţiune pentru dezvoltarea unei capabilităţi necesare protejării infrastructurilor cibernetice proprii. Tot în introducerea actului normativ se subliniază creşterea nivelului de conştientizare a costurilor şi pericolelor pe care le implică criminalitatea informatică.

Actul normativ îşi propune drept scop menţinerea unui mediu virtual sigur bazat pe infrastructurile cibernetice naţionale, iar pentru asigurarea securităţii cibernetice a României strategia stabileşte obiective precum: adaptarea cadrului normativ şi instituţional la dinamica ameninţărilor specifice spaţiului cibernetic sau dezvoltarea culturii de securitate a populaţiei prin conştientizarea faţă de vulnerabilităţile, riscurile şi ameninţările provenite din spaţiul cibernetic şi necesitatea asigurării protecţiei sistemelor informatice proprii.

Totodată, în cadrul acestuia este desluşit înţelesul unor termeni precum infrastructruri cibernetice – infrastructuri de tehnologia informaţiei şi comunicaţii, constând în sisteme informatice, aplicaţii aferente, reşţele şi servicii de comunicaţii electronice sau securitate cibernetică – stare de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a resurselor şi serviciilor publice şi private, din spaţiul cibernetic.

Dintre direcţiile de acţiune acest act normativ, prevede printre altele: dezvoltarea cooperării între sectorul public şi cel privat prin stimularea schimbului reciproc de informaţii privind ameninţări, vulnerabilităţi şi riscuri dar şi atacuri cibernetice sau derularea unor programe de conţtientizare a populaţiei, a administraţiei publice şi a sectorului privat, cu privire la ameninţările, vulnerabilităţile ţi riscurile specifice utilizării spaţiului cibernetic.

Principalul obiectiv al Strategiei de Securitate Cibernetică a României îl constiuie crearea unui sistem naţional integrat - Sistemul Naţional de Securitate Cibernetică (SNSC) - organism care are rolul de a superviza implementarea coerentă a tuturor măsurilor de prevenire şi reacţie la atacurile cibernetice împotriva instituţiilor publice sau a companiilor private şi care reuneşte autorităţile şi instituţiile publice cu responsabilităţi şi capabilităţi în domeniu.

Scopul SNSC este de a asigura elementele de cunoaştere, prevenire şi contracarare a ameninţărilor, vulnerabilităţilor şi riscurilor specifice spaţiului cibernetic care pot afecta securitatea infrastructurilor cibernetice naţionale, inclusiv managementul consecinţelor.

Consiliul Suprem de Apărare a Ţării este autoritatea care coordonează la nivel strategic activitatea SNSC. Guvernul României, prin Ministerul pentru Societatea Informaţională asigură coordonarea celorlalte autorităţi publice în vederea realizării coerenţei politicilor şi implementarea strategiilor guvernamentale în domeniu.

SNSC include, pe lângă autorităţile publice cu competenţe în materie (Serviciul Român de Informaţii, Ministerul Apărării Naţionale, Ministerul Afacerilor Interne, Ministerul Afacerilor Externe, Ministerul pentru Societatea Informaţională, Serviciul de Telecomunicaţii Speciale, Serviciul de Informaţii Externe, Serviciul de Protecţie şi Pază, Oficiul Registrului Naţional pentru Informaţii Secrete de Stat precum şi Secretarul Consiliului Suprem de Apărare a Ţării), actori din mediul asociativ neguvernamental, profesional şi de afaceri.

Actul normativ menţionat prevede că Consiliul Operativ de Securitate Cibernetică (COSC), reprezintă organismul prin care se realizează coordonarea unitară a SNSC. Din COSC fac parte, în calitate de membrii permanenţi, reprezentanţi ai Ministerului Apărării Naţionale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societatea Informaţională, Serviciului Român de Informaţii, Serviciului de Telecomunicaţii Speciale, Serviciului de Informaţii Externe, Serviciului de Protecţie şi Pază, Oficiul Registrului Naţional pentru Informaţii Secrete de Stat, precum şi secretarul Consiliului Suprem de Apărare a ţării. Conducerea este asigurată de un preţedinte (consilierul prezidenţial pe probleme de securitate naţională) şî un vicepreşedinte (consilierul primului – ministru pe probleme de securitate naţională). Coordonatorul tehnic al COSC este Serviciul Român de Informaţii.

Cu referire la Republica Moldova, un act normativ relevant îl reprezintă **Legea nr. 20 din 03.02.2009 privind prevenirea şi combaterea criminalităţii informatice** [124].

În cuprinsul art. 1 al Legii sunt definiţi unii termeni precum furnizor de servicii, date referitoare la trafic sau date referitoare la utilizatori.

Astfel, furnizorul de servicii este orice entitate publică sau privată care conferă utilizatorilor serviciilor sale posibilitatea de a comunica prin intermediul unui sistem informatic, precum şi orice altă entitate care prelucrează sau stochează date informatice pentru acest serviciu de comunicaţii sau pentru utilizatorii săi.

Datele referitoare la trafic sunt orice date avînd legătură cu o comunicare transmisă printr-un sistem informatic, produse de acest sistem în calitate de element al lanţului de comunicare, indicînd originea, destinaţia, itinerarul, ora, data, mărimea, durata sau tipul de serviciu subiacent, aceasta în timp ce datele referitoare la utilizatori reprezintă orice informaţie, sub formă de date informatice sau sub orice altă formă, deţinută de un furnizor de servicii, referitoare la abonaţii acestor servicii, altele decît datele referitoare la trafic sau conţinut, şi care permit stabilirea: tipului de serviciu de comunicaţii utilizat, identităţii, adresei poştale sau geografice, numărului de telefon al abonatului şi oricărui alt număr de contact, precum şi a datelor referitoare la facturare şi plată.

Art. 3 al actului normativ menţionat pune accent pe faptul că lupta pentru prevenirea şi combaterea criminalităţii informatice se face cu respectarea unor principii precum respectarea drepturilor şi a libertăţilor fundamentale ale omului şi protecţia datelor cu caracter personal.

Totodată, art. 4 stabileşte funcţiile autorităţilor şi instituţiilor publice cu competenţe în domeniul prevenirii şi combaterii criminalităţii informatice.

Astfel, Ministerul Afacerilor Interne efectuează măsuri speciale de investigaţii, de urmărire penală, de cooperare internaţională, de identificare a persoanelor care comit infracţiuni informatice.

Serviciul de Informaţii şi Securitate desfăşoară activităţi de prevenire şi combatere a criminalităţii informatice ce prezintă ameninţări la adresa securităţii naţionale, activităţi operative de investigaţii, de depistare a legăturilor organizaţiilor criminale internaţionale, alte activităţi în limita competenţei sale.

Procuratura Generală: a) coordonează, conduce şi exercită urmărirea penală, în modul prevăzut de lege; b) dispune, în cadrul desfăşurării urmăririi penale, la solicitarea organului de urmărire penală sau din oficiu, conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, faţă de care există pericolul distrugerii ori alterării, în condiţiile legislaţiei de procedură penală; c) reprezintă învinuirea, în numele statului, în instanţă de judecată în modul prevăzut de lege. Iar în final,

Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, în comun cu Serviciul de Informaţii şi Securitate, prezintă propuneri privind asigurarea protecţiei şi securităţii informatice.

În art. 5 al actului normativ se stipulează că autorităţile competente, furnizorii de servicii, organizaţiile neguvernamentale, alţi reprezentanţi ai societăţii civile colaborează prin schimb de informaţii, de experţi, prin activităţi comune de cercetare a cazurilor şi de identificare a infractorilor, de instruire a personalului, prin realizarea de iniţiative în scopul promovării unor programe, practici, măsuri, proceduri şi standarde minime de securitate a sistemelor informatice, prin campanii de informare privind criminalitatea informatică şi riscurile la care sînt expuşi utilizatorii de sisteme informatice, prin alte activităţi în domeniu.

Sunt prevăzue şi obligaţii atât pentru proprietarii de sisteme informatice dar şi pentru furnizorii de servicii.

Astfel, proprietarii de sisteme informatice, în cazul în care accesul la care este interzis sau restricţionat pentru anumite categorii de utilizatori, au obligaţia de a avertiza utilizatorii referitor la condiţiile legale de acces şi de utilizare, precum şi la consecinţele juridice ale accesului nesancţionat la aceste sisteme informatice. Avertizarea trebuie să fie accesibilă oricărui utilizator.

Aceasta în timp ce furnizorii de servicii, printre altele, trebuie să ţină evidenţa tuturor utilizatorilor de servicii, să comunice autorităţilor competente datele despre traficul informatic, inclusiv datele despre accesul ilegal la informaţia din sistemul informatic, despre tentativele de introducere a unor programe ilegale, despre încălcarea de către persoane responsabile a regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei, ori a regulilor de protecţie a sistemului informatic prevăzute în conformitate cu statutul informaţiei sau cu gradul ei de protecţie.

Hotărârea Guvernului Republicii Moldova nr. 808 din 07.10.2014 cu privire la aprobarea Planului naţional de acţiuni pentru implementarea Acordului de Asociere Republica Moldova – Uniunea Europeană în perioada 2014-2016 [83] face şi ea trimitere la criminalitatea informatică, stipulând în art. 16 lit. g) necesitatea ajustării cadrului legal privind prevenirea şi combaterea criminalităţii informatice precum şi a consolidării capacităţilor instituţionale prin instruirea specialiştilor, preluarea celor mai bune practici şi experienţe în domeniul schimbului de informaţii cu privire la combaterea criminalităţii informatice.

Instituţiile responsabile pentru implementarea acestor măsuri sunt Ministerul Afacerilor Interne, Procuratura Generală, Serviciul de Securitate şi Informaţii precum şi Ministerul Tehnologiei Informaţiei şi Telecomunicaţiilor, iar termenul stabilit pentru realizarea lor este perioada 2015-2016.

Hotărârârea Guvernului Republicii Moldova nr. 811 din 29.10.2015 cu privire la Programul naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 [81] defineşte în conţinutul său termeni precum: ameninţare cibernetică, apărare cibernetică, incident cibernetic, infrastructuri cibernetice, risc de securitate în spaţiul cibernetic, vulnerabilitate în spaţiul cibernetic ş.a.m.d.

Actul normativ prevede nişte principii pe care trebuie să se bazeze conceptul de securitate informatică, precum ar fi: protecţia drepturilor şi libertăţilor fundamentale ale omului; accesul pentru toţi la internet; rezilienţa cibernetică sau altfel spus, sesizarea preventivă a atacurilor şi ameninţărilor cibernetice, administrare multiparticipativă prin colaborarea dintre autorităţile publice şi sectorul privat şi, nu în ultimul rând, responsabilitatea comună şi răspunderea personalizată pentru asigurarea securităţii cibernetice.

Este tras şi un semnal de alarmă deoarece: **nu există un cadru legal privind delimitarea şi armonizarea competenţelor şi responsabilităţilor instituţiilor statului şi celor private în domeniul securităţii cibernetice, cadrul legislativ-normativ nu este armonizat integral la prevederile Convenţiei Consiliului Europei privind criminalitatea informatică, nu sunt asigurate educţia, formarea şi informarea continuă în domeniul securităţii cibernetice etc.**

Pentru rezolvarea acestor carenţe sunt stabilite de către actul normativ şapte obiective: procesarea, stocarea şi accesarea în siguranţă a datelor, inclusiv a datelor de interes public; securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice; dezvoltarea capacităţilor de prevenire şi reacţie urgentă la nivel naţional (reţeaua CERT naţională); prevenirea şi combaterea criminalităţii informatice; consolidarea capacităţilor de apărare cibernetică; educaţia, formarea şi informarea continuă în domeniul securităţii cibernetice; cooperarea şi interacţiunea internaţională în sferele ce ţin de securitatea cibernetică.

În final, un alt act normative important care trebuie menţionat este **Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020”** [82] **cuprinsă în Hotărârea Guvernului Moldovei 857 din 31.10.2013**.

Actul normativ indică că pe cît o societate este mai informatizată, cu atît este mai mult expusă riscurilor cibernetice, iar asigurarea securităţii spaţiului cibernetic trebuie să constituie o preocupare majoră a tuturor actorilor implicaţi, mai ales la nivel instituţional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu.

La fel se constată că în prezent, în Republica Moldova nu există autoritate publică direct responsabilă şi abilitată cu atribuţii, funcţii şi obligaţiuni privind securitatea cibernetică. La moment, sunt mai multe instituţii implicate în proces, fiecare dintre ele asigurînd acoperirea problematicii respective pe segmentul său de activitate. În acest sens, urmează a fi acoperit golul existent în cadrul legislativ-normativ în domeniul asigurării securităţii cibernetice.

Se punctează faptul că se resimte necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor informatice şi de comunicaţii, adesea insuficient informaţi în legătură cu potenţialele riscuri, dar şi cu soluţiile de contracarare a acestora.

Pentru un mediu digital securizat şi protejat textul de lege prevede obiective precum: sporirea nivelului de securitate cibernetcă a infrastructurilor critice naţionale (instituţii publice, reţele de comunicaţii electronice, apeducte, reţele de transport etc.); creşterea gradului de conştientizare a riscurilor spaţiului digital şi a necesităţii măsurilor de asigurare a securităţii cibernetice; promovarea şi dezvoltarea cooperării pe plan internaţional în domeniul securităţii cibernetice; completarea şi armonizarea cadrului legislative naţional în domeniul securităţii cibernetice; formarea profesională adecvată a persoanelor care îşi desfăşoară activitatea în domeniul securităţii cibernetice etc.

În cele ce urmează v-om determina locul incriminării fraudei informatice în legislaţia penală a României şi a Republicii Molodva.

În legătură cu legislaţia penală românească de referinţă se poate constata că printre modificările aduse de noul Cod penal român din 2009, se numără şi apariţia a două grupuri de infracţiuni care nu figurau în codul anterior**.**

Primul grup intitulat ”Fraude comise prin sisteme informatice şi mijloace de plată electronice”, face parte din infracţiunile contra patrimoniului (Titlul II, Capitolul IV din Partea specială) şi înglobează trei infracţiuni, anume; ”Frauda informatică” (art. 249 C. pen.), ”Efectuarea de operaţiuni financiare în mod fraudulos” (art. 250 C. pen.), ”Acceptarea operaţiunilor financiare efectuate în mod fraudulos” (art. 251 C. pen.).

Al doilea grup, intitulat ”Infracţiuni contra siguranţei şi integrităţii sistemelor informatice” este cuprins printre infracţiunile contra siguranţei publice (Titlul VII, Capitolul VI din Partea specială) şi înglobează şase infracţiuni, anume; ”Accesul ilegal la un sistem informatic” (art. 360 C. pen.),

”Interceptarea ilegală a unei transmisii de date informatice” (art. 361 C. pen.), ”Alterarea integrităţii datelor informatice” (art. 362 C. pen.), ”Perturbarea funcţionării sistemelor informatice” (art. 363 C. pen.), ”Transferul neautorizat de date informatice” (art. 364 C. pen.), ”Operaţiuni ilegale cu dispozitive sau programe informatice” (art. 365 C. pen.).

Fără doar şi poate că apariţia acestor infracţiuni a fost precedată şi impulsionată de adoptarea Convenţiei Consiliului Europei asupra criminalităţii informatice (semnată la Budapesta, în 2001) şi ratificată de Parlamentul României prin Legea nr. 64/2004, prin care statele părţi, între care şi România, şi-au asumat obligaţia să adopte măsurile legislative şi alte măsuri considerate necesare pentru a incrimina asemenea fapte.

În legislaţia anterioară, aceste infracşiuni erau consacrate în două legi speciale, anume în Legea nr. 365/2002 referitoare la comerţul electronic şi în Legea nr. 161/2003 cu privire la unele măsuri pentru asigurare a transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri. De aici, ele au fost preluate în noul Cod penal, iar ulterior, prin Legea nr. 187/2012, dispoziţiile de incriminare cuprinse în cele două legi speciale fiind abrogate.

În ceea ce priveşte Convenţia Europeană privind criminalitatea informatică, aceasta este împărţită pe patru secţini, fiecare fiiind constituită din mai multe articole. Prima secţiune (art. 1-13) este cea care stabileşte terminologia, definiţia şi măsurile care trebuie luate la nivel naţional sub forma prevederilor de drept penal material. A doua secţiune (art. 14-22) subliniază măsurile de ordin procedural şi de investigaţie în domeniu, cu particularităţile specifice. A treia parte a Convenţiei (art. 23-35) stabileşte liniile directoare ale cooperării internaţionale, care implică investigaţiile comune ale infracţiunilor informatice arătate în prima secţiune. Ultima parte a Convenţiei (art. 36-48), dar nu cea mai puţin importantă, cuprinde prevederi referitoare la semnare şi intrare în vigoare, aderare, aplicarea teritorială, efectele Convenţiei, declaraţii, clauza federală, rezervele, statutul şi retragerea rezervelor, amendamende, rezolvarea dezacordurilor, reunirea părţilor, denunţarea şi notificarea [98, p.131-133].

Din toate timpurile, legiuirile de un fel sau de altul au inclus norme de incriminare a comportamentelor care aduc atingere într-o manieră nejustificată patrimoniului [73, p.11].

Sistemele de drept penal moderne, deşi şi-au adecvat instrumentele, au menţinut un regim destul de sever pentru anumite forme de activitate infracţională îndreptate împotriva patrimoniului. Totodată, au extins cadrul incriminator şi la alte fapte specifice relaţiilor economice din societatea modernă [147, p.8].

După cum s-a precizat anterior, frauda informatică face parte din infracţiunile contra patrimoniului. Raţionamentul legiuitorului în acest caz a fost determinat de pagubele patrimoniale aduse victimelor acestui tip de infracţiuni.

Este deci foarte important pentru o bună înţelegere a fraudei informatice să avem o justă înţelegere a noţiunii de patrimoniu.

Întotdeauna, atunci când se pune problema ocrotirii penale a unor valori sociale este foarte important ca această valoare să fie corect percepută de către dreptul penal. Aceast demers nu este unul lipsit de dificultate, aceasta întrucât trebuie să se apeleze la definiţii care nu îi aparţin.

Din punct de vedere doctrinar, termenul patrimoniu desemnează o noţiune încadrată cu exactitate de dreptul privat: totalitatea drepturilor şi obligaţiilor evaluabile în bani ale unei persoane [99, p.37].

Noţiunea de patrimoniu în dreptul penal nu trebuie confundată cu aceea de proprietate, aceasta deoarece noţiunea de patrimoniu are în vedere drepturile şi obligaţiile pe care o persoană le are asupra bunurilor materiale, în timp ce noţiunea de proprietar relevă ideea de stpânire sau de capacitate şi drept de a dispune de bunuri materiale.

Dreptul de proprietate este garantat atât la nivel naţional, dar şi internaţional, pe plan intern având garanţii constituţionale, în timp ce pe plan internaţional beneficiază de pactele, tratatele, convenţiile internaţionale cu privire la drepturile omului. Art. 136 alin. (1) din Constituţia României stipulează că proprietatea este publică sau privată, iar art. 136 alin. (2) arată că proprietatea publică este garantată şi ocrotită de lege şi aparţine statului sau unităţilor administrativ-teritoriale, în timp alin. (5) prevede că proprietatea privată este inviolabilă în condiţiile legii organice.

Conform art. 17 al Declaraţiei Universale a Drepturilor Omului, orice persoană are dreptul la proprietate, atât singură cât şi în asociaţie cu alţii şi nimeni nu poate fi lipsit în mod arbitrar de proprietatea sa. Art. 1 al protocolului adiţional la Convenţia Europeană asupra Drepturilor Omului stipulează că orice persoană fizică sau juridică are dreptul la respectarea bunurilor sale şi că nimeni nu poate fi lipsit de proprietatea sa decât pentru cauză de utilitate publică şi în condiţiile prevăzute de lege şi de principiile generale ale dreptului internaţional.

Noţiunea de proprietate folosită în normele de mai sus nu acoperă sfera patrimoniului, fiind doar o parte a acestuia.

Dreptul la proprietate poate fi definit ca acel drept real ce permite titularului de a întrebuinţa lucrul potrivit naturii sau destinaţiei sale, de a-l folosi şi de a dispune de el, în orice fel doreşte, în mod exclusiv şi perpetuu, cu respectarea dispoziţiilor legale [110, p.85].

În temeiul principiului unităţii sistemului juridic, noţiunea de patrimoniu în dreptul penal, ca valoare socială şi obiect de ocrotire penală, ar trebui să aibă acelaşi înţeles ca în dreptul civil: restrângerea sau extinderea înţelesului noţiunii de patrimoniu putând avea loc numai atunci când legea penală prevede o derogare de la sensul obişnuit sau când derogarea ar rezulta implicit din natura faptei incriminate [60, p.278].

Din punct de vedere juridic, expresiile; patrimoniu, proprietar, posesie, deţinere ş.a. fac parte din limbajul juridic, având un conţinut bine determinat şi întâlnit în mod uzual, în materia dreptului civil.

Valorile conţinute în aceste expresii sunt ocrotite însă şi de dreptul penal, legea penală sancţionând infracţiunile contra patrimoniului. Este motivul pentru care, în doctrină, s-a pus problema semnificaţiei penale a noţiunilor utilizate de dreptul penal şi care aparţin, prin excelenţă dreptului civil [125, p.61].

Diferenţele între opiniile exprimate au repus în actualitate discuţiile referitoare la caracterul accesoriu, exclusiv sancţionatoriu al dreptului penal în raport cu dreptul civil. Un argument care sprijină o asemenea concluzie este legat de faptul că interesele patrimoniale au fost ocrotite iniţial de dreptul civil şi ulterior de dreptul penal.

Divergenţele în domeniu au trasat două concepţii. Într-o primă concepţie se afirmă că noţiunile de patrimoniu, proprietate, lucruri, bunuri, daune, posesie etc. îşi au originea în dreptul civil şi trebuie păstrate cu semnificaţia lor originară, chiar şi în domeniul dreptului penal.

Într-o altă concepţie, se susţine că asemenea noţiuni au un conţinut particular în dreptul penal, căci, în timp ce dreptul civil este preocupat de ocrotirea intereselor patrimoniale cu relevanţă economică, dreptul penal ocroteşte şi valorile patrimoniale cu caracter spiritual [59, p.11-12].

Totodată, în doctrina penală română, prof. V. Dongoroz afirmă că dreptul penal, deşi, de principiu, nu s-ar putea abate de la dreptul civil în ceea ce priveşte semnificaţia conceptelor folosite, este posibil ca, în penal, să existe derogări explicite, motivate chiar de natura normelor incriminate.

Acesta susţine că normele dreptului penal sunt în raport cu cele civile, norme de referire, iar cele civile sunt norme complinitorii. Dacă se modifică norma complinitoare se va modifica şi norma de referire. Specificul dreptului penal constă în aceea că ocroteşte situaţia de fapt a bunului împotriva acţiunii ilicite a unei persoane care ar urmări să modifice această stare de fapt, fiind fără interes, sub aspect penal, legitimitatea deţinerii bunului de către victima sustragerii. De asemenea, proprietarul care îşi distruge propriul bun, care are o valoare artistică, răspunde penal, aceeaşi acţiune neavând semnificaţie în dreptul civil [193, p.448].

În dreptul civil patrimoniul este definit ca o universalitate de drepturi şi obligaţii cu valoare economică, în timp ce în dreptul penal patrimoniul ni se înfăţişează ca o universalitate de fapt, o totalitate de bunuri, căci dreptul penal ocroteşte patrimoniul prin incriminarea faptelor îndreptate direct sau indirect împotriva bunurilor exterioare, asupra cărora se exercită drepturile patrimoniale, adică asupra bunurilor care, în materialitatea lor, pot fi sustrase, însuşite, distruse, ori cu privire la care poate fi tulburată posesia lor etc [125, p.62].

Astfel, dreptul penal ocroteşte doar bunurile care compun activul patrimonial, având în vedere nu doar lucrurile cu valoare economică, ci şi lucrurile care au o valoare afectivă (fotografii, scrisori etc.), deci bunuri care reflectă nevoile spirituale ale posesorului şi care scapă sferei de preocuare a dreptului civil.

Sub acest aspect, cea mai bună definiţie a patrimoniului, din punctul de vedere al ocrotirii penale, trebuie să aibă în vedere patrimoniul ca universalitate de drepturi şi bunuri susceptibile să satisfacă nevoile materiale şi spirituale ale oamenilor [138, p.36].

Se apreciază că infracţiunea n-ar putea fi săvârşită împotriva patrimoniului ca universalitate de bunuri, pentru că aceasta din urmă va exista întotdeauna indiferent de numărul sau valoarea bunurilor componente şi chiar dacă subiectul nu posedă nimic, ori numai datorii, aceasta deoarece nici o persoană nu poate fi lipsită de patrimoniu, ci cel mult de unul sau mai multe din bunurile care compun patrimoniul său. De aceea s-a exprimat şi punctul de vedere că denumirea corectă a acestor infracţiuni ar trebui să le indice ca fiind îndreptate contra bunurilor care fac parte din patrimoniu (patrimoniale), şi nu a patrimoniului însuşi [147, p.48].

Legea penală foloseşte noţiunea de infracţiuni ”contra patrimoniului”, iar nu pe cea de infracţiuni ”contra proprietăţii”, pentru a sublinia faptul că infracţiunile pot fi îndreptate nu numai împotriva proprietarului unui bun, ci şi împotriva celui care deţine posesia sau folosinţa bunului respectiv. Prin urmare, legea penală apără nu numai dreptul de dispoziţie, ci şi posesia. Mai mult decât atât, legea penală apără şi detenţia, fie ea şi detenţia precară. Detentorul precar este persoana care stăpâneşte bunul nu pentru sine, ca posesor, ci pentru altul, în virtutea actului juridic pe care l-a încheiat cu acesta (spre exemplu depozitarul, locatarul, împrumutatul etc.) [5, p.187].

Prin excluderea din denumirea acestei categorii de infracţiuni a noţiunii de proprietate s-a avut în vedere şi posibilitatea ca însuşi proprietarul bunului să poată fi subiect activ al vreunuia dintre infracţiunile contra patrimoniului (dacă, de pildă, proprietarul însuşi poate comite infracţiunea de furt atunci când sustrage bunul proprietatea sa dat în gaj ori ca împrumut unei alte persoane sau când proprietarul sustrage bunul aflat în indiviziune cu un alt coproprietar ori când nudul proprietar sustrage bunul asupra căruia există un drept de uzufruct al altei persoane) [60, p.279].

Deci, legea nu ocroteşte numai dreptul de proprietate. Posesia este ocrotită în aceeaşi măsură, iar din punctul de vedere al legii penale, detenţia precară se bucură de acelaşi regim de protecţie. Aceasta înseamnă că posesia sau detenţia legitimă este ocrotită chiar împotriva proprietarului [71, p.165].

Ocrotirea patrimoniului prin normele dreptului penal a constituit dintotdeauna un obiectiv prioritar al oricărui sistem de drept, patrimoniul reprezentând o componentă importantă a vieţii de zi cu zi a oricărei persoane fizice sau juridice, de care depinde atât satisfacerea cerinţelor curente, dar mai ales proprietatea, la nivel individual precum şi micro sau macro-social [118, p.172-205].

Dat fiind faptul că în viziunea legiuitorului român frauda informatică este încadrată în rândul infracţiunilor contra patrimoniului, considerăm ca absolut necesară o prezentare generală a acestor infracţiuni.

În actualul Cod penal a României, infracţiunile contra patrimoniului au fost sistematizate în cinci capitole, ţinând seama de situaţiile de fapt în care se pot găsi bunurile, ca entităţi patrimoniale, cât şi caracterul sau natura acţiunilor ilicite prin care pot fi modificate aceste situaţii de fapt [112, p.220].

Astfel, Capitolul I intitulat ”Furtul” reglementează furtul (art. 228), furtul calificat (art. 229), furtul în scop de folosinţă (art. 230), furtul la plângerea prealabilă (art. 231). Capitolul II intitulat ”Tâlhăria şi pirateria” incriminează tâlhăria în varianta tip (art. 233), tâlhăria calificată (art. 234), pirateria (art. 235) şi tâlhăria sau pirateria urmată de moartea victimei (art. 236). Capitolul III reglementează faptele contra patrimoniului care se săvârşesc prin nesocotirea încrederii, respectiv abuzul de încredere (art. 238), abuzul de încredere prin fraudarea creditorilor (art. 239), bancruta simplă (art. 240), bancruta frauduloasă (art. 241), gestiunea frauduloasă (art. 242), însuşirea bunului găsit sau ajuns din eroare la făptuitor (art. 243), înşelăciunea (art. 244), înşelăciunea privind asigurările (art. 245), deturnarea licitaţiilor publice (art. 246) şi exploatarea patrimonială a unei persoane vulnerabile (art. 247). Capitolul IV include fraudele patrimoniale săvârşite prin sisteme informatice şi mijloace de plată electronice: frauda informatică (art. 249), efectuarea de operaţii financiare în mod fraudulos (art. 250) şi acceptarea operaţiunilor financiare efectuate în mod fraudulos (art. 251) iar Capitolul V intitulat ”Distrugerea şi tulburarea de posesie” cuprinde infracţiunile: distrugerea (art. 253), distrugerea calificată (art. 254), distrugerea din culpă (art. 255) şi tulburarea de posesie (art. 256).

Prin această clasificare a infracţiunilor contra patrimoniului în mai multe categorii, noul Cod penal urmează tendinţele codurilor penale din alte state membre ale Uniunii Europene, cum ar fi spre exemplu Codul penal francez, Codul penal spaniol, Codul penal italian, Codul penal german etc.

Spre deosebire de această alcătuire, în Codul penal anterior, toate incriminările privitoare la ocrotirea patrimoniului erau aşezate într-o singură diviziune a Părţii speciale, mai precis în Titlul III, art. 208-222, titlu care nu era subdivizat în capitole distincte.

În vechiul Cod penal, o asemenea sistematizare nu exista, infracţiunile contra patrimoniului fiind clasificate sub acest aspect, exclusiv pe cale doctrinară, ţinându-se cont de specificul activităţii materiale în infracţiuni contra patrimoniului bazate pe sustragere (furt, tâlhărie, piraterie), infracţiuni contra patrimoniului bazate pe fraudă (abuzul de încredere, înşelăciunea) şi infracţiuni contra patrimoniului bazate pe samavolnicie (distrugere, degradare, tulburare de posesie) [95, p.232].

Această abordare doctrinară a fost însuşită de noul Cod penal, deoarece infracţiunile contra patrimoniului, sistematizate pe cinci capitole, aşa cum s-a menţionat mai sus, au fost grupate astfel: două infracţiuni contra patrimoniului bazate pe sustragere (furtul, respectiv tâlhăria şi pirateria), două referitoare la infracţiuni contra patrimoniului bazate pe fraudă (separate în funcţie de modalitatea de comitere a fraudei, respectiv prin sisteme electronice sau mijloace de plată informatice sau prin metode

tradiţionale), iar ultimul capitol se referă la infracţiuni contra patrimoniului bazate pe samavolnicie [188, p.212].

În noua reglementare a avut loc o creştere a numărului de infracţiuni contra patrimoniului. Această sporire a numărului de infracţiuni a fost consecinţa aducerii unor infracţiuni din legislaţia specială în noul Cod penal (de exemplu, a bancrutei simple sau frauduloase, a fraudei informatice etc.), dar şi de incriminarea unor fapte care nu aveau caracter infracţional în vechiul Cod (de exemplu, a abuzului de încredere prin fraudarea creditorilor, a înşelăciunii privind asigurările, a exploatării patrimoniale a unei persoane vulnerabile).

Din punct de vedere istoric, putem analiza infracţiunile contra patrimoniului prin prisma a două coordonate esenţiale care s-au dezvoltat în acelaşi timp [5, p.187]:

- noţiunea de proprietate şi bunurile care pot constitui proprietatea, care pot deveni obiect material al infracţiunilor contra patrimoniului, de la bunuri tangibile, la cele incorporale cum este, de exemplu, energia electrică;

- acţiunea făptuitorului, de la furtul săvârşit profitând de anumite circumstanţe sau de neatenţia victimei ori violenţă, până la infracţiunile contra patrimoniului săvârşite profitând de încrederea victimei (cum e cazul gestiunii frauduloase) şi infracţiunile săvârşite în domeniul sistemelor informatice.

În accepţiunea legii penale, patrimoniul şi drepturile legate de acesta sunt apărate doar în măsura în care acestea sunt păstrate în starea în care se aflau până în momentul activităţii ilicite a făptuitorului. Ulterior executării actului infracţional, valorificarea drepturilor patrimoniale privitoare la acel bun nu mai este posibilă, decât doar în măsura soluţionării penale a acelei cauze, inclusiv prin exercitarea acţiunii civile în cadrul procesului penal [4, p.158].

Formarea, desfăşurarea şi dezvoltarea relaţiilor sociale cu privire la patrimoniu este asigurată prin apărarea patrimoniului, mai ales sub aspectul obligaţiei de a menţine poziţia fizică a bunurilor în cadrul patrimoniului. Legea penală a considerat că, pentru a ocroti patrimoniul, se impune, întâi de toate, să fie protejată starea de fapt a bunurilor ce constituie patrimoniul, în sensul că acestea să fie menţinute în starea şi în condiţiile în care se aflau până la intervenţia ilegală a infractorului [169, p.527].

Ca o observaţie generală în domeniul infracţiunilor contra patrimoniului, este aceea că noul Cod penal aduce o reducere semnificativă a pedepselor pentru infracţiunile cuprinse în acest capitol.

Un alt element de noutate este acela că pentru majoritatea faptelor din acest capitol, noul Cod penal prevede posibilitatea împăcării părţilor drept cauză ce înlătură răspunderea penală. Prevederea reflectă o abordare pragmatică a legislativului care pune accent pe a motiva autorul să repare prejudiciul cauzat persoanei vătămate prin comiterea faptei şi nu pe intervenţia statului (uneori inutilă din perspectiva victimei) pentru a-l sancţiona pe vinovat [168, p.203].

Condiţii preexistente în cazul infracţiunilor contra patrimoniului.

A. *Obiectul juridic al infracţiunilor*

a) *Obiectul juridic generic* al infracţiunilor contra patrimoniului este reprezentat de valoarea socială pe care o reprezintă relaţiile sociale care se nasc, se desfăşoară şi se dezvoltă în legătură cu protecţia patrimoniului public sau privat.

Obiectul juridic poate fi unul complex, în situaţia unor infracţiuni contra patrimoniului fiind lezate şi valori cum ar libertatea de voinţă, integritatea personală (spre exemplu, în cazul infracţiunii de tâlhărie) sau încrederea persoanei (în cazul infracţiunii de gestiune frauduloasă).

b) *Obiectul material* al infracţiunilor contra patrimoniului îl reprezintă bunurile bunurile mobile sau imobile împotriva cărora a fost îndreptată activitatea infracţională [9, p. 65].

Obiectul material va fi, în toate cazurile, un bun mobil în cazul infracţiunilor de furt, tâlhărie, abuz de încredere, delapidare sau însuşirea bunului găsit.

Unele infracţiuni, cum sunt distrugerea (în oricare dintre formele sale) sau tulburarea de posesie pot avea ca obiect material un imobil asupra căruia se îndreaptă activitatea infracţională a făptuitorului.

Obiectul material poate să aparţină unei persoane fizice sau juridice (de drept public sau privat).

B. *Subiecţii infracţiunii*

a) *Subiect activ* al infracţiunilor contra patrimoniului poate fi orice persoană care răspunde penal, legea necondiţionând existenţa infracţiunii de o calificare specială a făptuitorului, cu unele excepţii, cum este situaţia gestiunii frauduloase, caz în care legea stabileşte o calitate specială a subiectului activ, şi anume cea de administrator judiciar.

Există cazuri când subiect activ al infracţiunii poate fi chiar şi proprietarul bunului (la infracţiunea de furt, atunci când proprietarul ia bunul din posesia legitimă a altuia).

În marea lor majoritate, infracţiunile contra patrimoniului se săvârşesc în participaţie penală, fie sub forma coautoratului, instigării sau complicităţii. Este posibilă şi participaţia improprie, în măsura în care la intervenţia intenţionată a instigatorului sau complicelui autorul a acţionat din culpă sau fără intenţie.

În doctrina dreptului penal se apreciază că poate exista coautorat la infracţiunea de abuz de încredere doar în măsura în care bunul mobil a fost încredinţat făptuitorilor în grija lor comună, iar la gestiunea frauduloasă doar atunci când făptuitorii aveau obligaţia comună de a administra sau conserva bunurile [72, p.193].

b) *Subiect pasiv* al infracţiunilor contra patrimoniului poate fi orice persoană fizică sau juridică, în funcţie de situaţie, precum şi statul în măsura în care bunurile asupra cărora a fost îndreptată activitatea infracţională constituie obiectul exclusiv al proprietăţii publice.

Codul penal în vigoare introduce o condiţie suplimentară pentru existenţa unităţii de infracţiune (existenţa unui subiect pasiv unic), iar legea de punere în aplicare prevede că această cerinţă este îndeplinită şi atunci când obiectul infracţiunii se află în coproprietatea mai multor persoane. În cazul infracţiunilor complexe (tâlhăria şi pirateria), există unitate de infracţiuni atunci când prin aceasta s-a adus atingere unor subiecţi pasivi secundari diferiţi, dar subiectul pasiv principal este unic [123].

În cazul majorităţii infracţiunilor contra patrimoniului, legea nu prevede condiţii de loc sau de timp pentru existenţa infracţiunii. În cazul furtului sau a tâlhăriei, cerinţele speciale referitoare la locul şi timpul săvârşirii infracţiunii pot constitui doar circumstanţe de agravare a infracţiunii.

În opinia unor autori [112, p.222-223], infracţiunile contra patrimoniului sunt condiţionate de existenţa unei situaţii premise şi care variază în raport cu specificul fiecărei infracţiuni. În cazul în care lipseşte situaţia premisă, infracţiunea condiţionată de o astfel de situaţie se consideră că nu este prevăzută de legea penală.

Astfel, la infracţiunile de sustragere (furt, tâlhărie, piraterie) situaţia premisă constă în existenţa unui bun care se află în stăpânirea de fapt a altei persoane decât cea care comite fapta; în cazul infracţiunii de abuz de încredere situaţia premisă o constituie raportul juridic patrimonial existent între persoana care deţine un bun al altuia şi persoana de la care a primit bunul; la abuzul de încredere privind fraudarea creditorilor situaţia premisă presupune existenţa unor raporturi juridice patrimoniale care să genereze obligaţii de această natură din partea făptuitorului faţă de creditorii săi; în infracţiunea de însuşire a bunului găsit sau ajuns din eroare la făptuitor, situaţia premisă constă în existenţa unei relaţii patrimoniale născută întâmplător între persoana care a găsit bunul ori l-a primit din eroare din eroare şi persoana în paguba căreia s-a produs pierderea bunului sau căreia i se cuvenea bunul respectiv etc.

Conţinutul constitutiv al infracţiunilor contra patrimoniului.

A. Latura obiectivă se compune din elementul material, cerinţe esenţiale, urmarea imediată şi legătura de cauzalitate,

a) Elementul material al laturii obiective al infracţiunilor contra patrimoniului se poate realiza în marea majoritate a cazurilor prin acţiune, şi doar în mod excepţional la infracţiunea prevăzută de art. 243 (însuşirea bunului găsit sau ajuns din eroare la făptuitor), una dintre modalităţile normative constă în inacţiune.

Unele infracţiuni au elementul material sub forma unei singure acţiuni (ex. furtul), altele, sub forma unor acţiuni alternative (ex. distrugerea) ori cumulative (ex. tâlhăria, pirateria), iar în alte situaţii acţiuni sau inacţiuni alternative (ex. însuşirea bunului găsit sau ajuns din eroare la făptuitor).

Sunt infracţiuni contra patrimoniului la care deşi elementul material constă într-o acţiune, nu se exclude posibilitatea unor acte omisive prin care să se realizeze acţiunea incriminată săvârşită în

condiţiile art. 17 C. pen. (comisiune prin omisiune) cum ar fi gestiunea frauduloasă şi distrugerea [58, p.287].

b) **Cerinţe esenţiale.** Elementul material al laturii obiective la infracţiunile contra patrimoniului este condiţionat, de regulă de anumite cerinţe esenţiale care devin elemente constitutive ale infracţiunii, fără realizarea lor fiind exclusă infracţiunea. De pildă, infracţiunea de furt este condiţionată de cerinţa unui bun mobil aflat în posesia sau detenţia altei persoane şi de lipsa consimţământului acesteia; la infracţiunea de tâlhărie, violenţele sau ameninţările trebuie să constituie un mijloc pentru săvârşire a furtului ori pentru păstrarea bunului furat [49, p.158] etc.

c) **Urmarea imediată** constă în producerea unei pagube patrimoniului unei persoane fizice sau juridice private sau unei persoane juridice publice. În cazul infracţiunilor cu obiect juridic complex, urmarea constă şi în afectarea altor valori sociale (de exemplu, integritatea corporală în cazul infracţiunii de tâlhărie sau piraterie).

d) **Legătura de cauzalitate** trebuie să existe între comiterea faptei şi producerea urmării periculoase. Ea implică existenţa unei relaţii ca de la cauză la efect ce se realizează între elementul material şi urmarea imediată. Dacă această urmare se datorează altor cauze decât acţiunii ilicite a făptuitorului, va fi exclusă existenţa infracţiunii. Legătura de cauzalitate rezultă, în cazul anumitor infracţiuni, din materialitatea faptei săvârşite, iar în alte situaţii trebuie dovedită cu probe [112, p.224].

B. Latura subiectivă. Forma de vinovăţie cu care se săvârşesc infracţiunile contra patrimoniului este, de regulă, intenţia directă sau indirectă, În cazul unor forme agravate ale tâlhăriei sau pirateriei, vinovăţia se poate realiza şi sub aspectul praeterintenţiei, iar în mod cu totul deosebit poate îmbrăca şi forma culpei în varianta distrugerii din culpă.

Forme. Modalităţi. Sancţiuni

A. **Forme**

a) *Actele de pregătire* nu sunt incriminate. Dacă au fost efectuate de altă persoană decât autorul şi au fost folosite de către acesta la săvârşirea infracţiunii, pot reprezenta acte de complicitate.

b) *Tentativa* este sancţionată potrivit prevederilor art. 232, art. 237, art. 238 din C. pen..

c) *Consumarea* are loc în momentul în care, prin săvârşirea unei fapte se produce o pagubă în patrimoniul unei persoane sau este pus în pericol un drept de natură patrimonială

d) *Epuizarea* poate exista în cazul infracţiunilor contra patrimoniului când activitatea infracţională are formă continuă sau continuată. În primul caz momentul epuizării faptei va fi acela al intervenţiei unei voinţe contrare de a face să înceteze prelungirea activităţii ilicite a autorului. La forma continuată, epuizarea are loc în momentul săvârşirii ultimului act al activităţii infracţionale [112, p.224].

B. **Modalităţi.** Infracţiunile contra patrimoniului în raport cu conţinutul lor legal, îmbracă modalităţi normative stabilite printr-un conţinut închis de incriminare sau printr-un conţinut deschis care permite şi alte modalităţi decât cele enumerate de legiuitor [4, p.161].

Modalităţile faptice pot fi diverse potrivit împrejurărilor concrete ale fiecărei activități infracţionale.

C. **Sancţiuni**. În ceea ce priveşte pedeapsa, noul Cod penal român prevede în general o sancţiune mai blândă pentru infracţiunile contra patrimoniului, raportându-ne la vechea reglementare. Pentru unele infracţiuni, Codul prevede şi pedeapsa cu amenda, alternativ la cea a închisorii (la infracţiunea de furt, abuz de încredere, bancrută simplă etc.) În cazul variantelor agravate, la unele infracţiuni se prevede şi pedeapsa complementară a interzicerii exercitării unor drepturi (tâlhărie, piraterie, distrugere calificată).

Aspecte procesuale. Pentru majoritatea infracţiunilor contra patrimoniului, acţiunea penală se pune în oficiu. Aceste infracţiuni sunt următoarele: furtul - art. 228 C. pen, furtul calificat - art. 220 C. pen., furtul în scop de folosinţă - art. 230 C. pen., tâlhăria - art. 233 C. pen., tâlhăria calificată - art. 234 C. pen., pirateria - art. 235 C. pen., tâlhăria sau pirateria urmată de moartea victimei - art. 236 C. pen., însuşirea bunului găsit sau ajuns din eroare la făptuitor - art. 243 C. pen., înşelăciunea - art. 244 C. pen., înşelăciunea privind asigurările - art. 245 C. pen., deturnarea licitaţiilor publice - art. 246 C. pen., exploatarea patrimonială a unei persoane vulnerabile - art. 247 C. pen., frauda informatică - art. 249 C. pen., efectuarea de operaţiuni financiare în mod fraudulos - art. 250 C. pen., acceptarea operaţiunilor financiare efectuate în mod fraudulos - art. 251 C. pen., distrugerea - art. 253 alin. (1) şi (4) C. pen., distrugerea calificată - art. 254 C. pen. şi distrugerea din culpă - art. 255 C. pen.

Acţiunea penală se pune în mişcare la plângerea prealabilă a persoanei vătămate pentru următoarele infracţiuni contra patrimoniului: faptele de furt săvârşite între membrii familiei, de către un minor în paguba tutorelui, ori de către cel care locuieşte împreună cu persoana vătămată sau este găzduit de aceasta - art. 231 C. pen., abuzul de încredere - art. 238 C. pen., abuzul de încredere prin fraudarea creditorilor - art. 239 C. pen., bancruta simplă - art. 240 C. pen., bancruta frauduloasă - art. 241 C. pen., gestiunea frauduloasă art. 242 C. pen., distrugerea - art. 253 alin. (1) şi (2) C. pen. şi tulburarea de posesie.- art. 256 C. pen.

Pentru următoarele infracţiuni contra patrimoniului împăcarea părţilor înlătură răspunderea penală: furtul - art. 228 C. pen, furtul calificat - art. 229 alin. (1) alin. (1), alin. (2) lit. b) şi c) C. pen; furtul în scop de folosinţă - art. 230 C. pen.; însuşirea bunului găsit sau ajuns din eroare la făptuitor - art. 243 C. pen.; înşelăciunea - art. 244 C. pen. şi înşelăciunea privind asigurările - art. 245 C. pen.

De regulă, urmărirea penală se efectuează de către organele de cercetare ale poliţiei judiciare sub conducerea şi supravegherea procurorului iar competenţa judecării cauzei în primă instanţă

aparţine judecătoriei, cu excepţia infracţiunii de distrugere calificată prevăzută de art. 254 C.pen care intră în competenţa tribunalului.

Pentru infracţiunile săvârşite cu intenţie depăşită care a avut ca urmare moartea unei persoane (art. 236 C. pen. român), competenţa efectuării urmăririi penale aparţine procurorului iar competenţa judecării cauzei în primă instanţă aparţine tribunalului.

În ceea ce priveşte *Codul penal al Republicii Moldova, frauda informatică* face parte din rândul infracţiunilor informatice, fiind reglementată în art. 260^6 C. pen., în Capitolul XXI intitulat ”Infracţiuni informatice şi infracţiuni în domeniul telecomunicaţiilor”.

Astfel, acest cod a încercat să se adapteze cât mai bine la noile concepte utilizate tot mai frecvent la scară internaţională, cum ar fi ”societate informatizată” sau ”societate telecomunicaţională”, încercându-se crearea unei noi doctrine privind infracţionalitatea informatică şi telecomunicaţională ce se doreşte a fi cuprinsă în legislaţia de drept penal a Republicii Moldova.

Totuşi, la fel de bine se poate observa că unele sisteme de drept (în special cel spaniol) nu au considerat necesară o separare conceptuală a infracţiunilor informatice de cele tradiţionale. Acestea plasează infracţiunile informatice în cadrul în cadrul unor forme asimilate ale unor infracţiuni tradiţionale ori le conturează ca fiind forme agravate ale unor infracţiuni tradiţionale [63, p.170].

Orice societate nu poate exista fără informaţie şi comunicarea ei. Cantitatea de informaţie este în continuă creştere şi aceasta este caracteristica evoluţiei societăţii umane care se află în faza societăţii informaţionale. Lumea în care trăim se află într-o continuă schimbare, asistăm astăzi la un proces de tranziţie de la societatea industrială la societatea informaţională. Societatea informaţională este acea societate în care economia se dezvoltă datorită progreselor tehnologice, în care informaţia joacă un rol pe care altădată (în societatea industrială) îl aveau bunurile materiale. Ea posedă trei caracteristici principale: informaţia este cea mai importantă resursă economică, consumul de informaţii este intens şi dezvoltarea structurii informaţionale globale este primordială [12, p.11].

Dacă deceniul trecut a fost marcat de apariţia şi perfecţionarea calculatoarelor personale, uşor accesibile şi la preţuri din ce în ce mai scăzute, deceniul actual este caracterizat de conectivitatea tot mai pronunţată, adică de fuziunea dintre calculatoare şi telecomunicaţii, Revoluţia tehnologiei informaţiei a dus la schimbări fundamentale în societate şi este foarte probabil ca aceste schimbări profunde să se producă în continuare. Unul dintre efectele informatizării tehnologice este impactul asupra evoluţiei tehnologiei telecomunicaţiilor. Comunicarea clasică prin intermediul telefoniei a fost depăşită de noile metode de transmitere la distanţă nu doar a vocii, ci şi a datelor, muzicii, fotografiilor sau filmelor. Aceste schimburi de informaţii nu mai apar numai între oameni, dar şi între oameni şi sisteme informatice, ori numai între acestea din urmă. Folosirea poştei electronice sau accesul la pagini Web prin intermediul Internetului constituie exemple ale acestei evoluţii, modificând profund societatea noastră. Această evoluţie a dat naştere la schimbări economice şi sociale fără precedent, dar

în acelaşi timp foloseşte şi scopurilor mai puţin legitime; apariţia unor noi infracţiuni; săvârşirea infracţiunilor tradiţionale prin intermediul noii tehnologii. Conceptele juridice existente sunt puse la încercare de apariţia noilor tehnologii. Dreptul penal trebuie să facă faţă noilor provocări ridicate de dezvoltările tehnologice [170, p.252-253].

Tehnologia informaţiei cu cele două subsisteme ale sale – informatic şi comunicaţii - într-un proces accelerat de evoluţie, adaugă permanent noi criterii în procesul de globalizare, mărind spectrul oportunităţii mediului informaţional, dar şi cel al riscurilor şi ameninţărilor ce îl vizează direct sau indirect prin transformarea organizaţiei pe care o deserveşte într-o ţintă socială [128, p.46].

Răspândirea tehnologiilor informatice este un fenomen care se bazează nu numai pe progresul cercetării ştiinţifice, ci si, mai ales, pe capacitatea extraordinară a tehnologiei informaţiilor şi comunicaţiilor de a satisface exigenţele organizatorice şi de gestiune ale întreprinderilor private dar si ale administraţiei publice până la punctul de a crea modele originale de gestiune, diferite de cele tradiţionale tocmai pentru ca sunt create in cadru "virtual" [36, p.13].

Aproape toate sectoarele societăţii contemporane sunt, deja, organizate de sisteme informatice: de la serviciul sanitar la transporturile publice, de la traficul aerian la sistemul bancar, de la sistemul telecomunicaţiilor la serviciul militar. Şi economia globala este consolidată de noile tehnologii care oferă mari oportunităţi pe piaţa internaţională. Multinaţionalele, dar şi întreprinderile mici si mijlocii, îşi desfăşoară comerţul şi afacerile lor mult mai uşor, fără bariere de spaţiu. Noile tehnologii permit, intr-adevăr, să se investească in activităţi noi, să se intre pe noi pieţe şi să se ofere produse şi servicii intr-un mod nou mai economic si eficient [53, p.8].

Sectorul tehnologiei se află înaintea sistemului de drept care a trebuit să recupereze decalajul prin adoptarea unor norme adecvate prevenirii şi combaterii infracţiunilor săvârşite prin intermediul reţelelor informatice, luându-se în calcul în acelaşi timp şi dreptul la viaţă privată al utilizatorilor legali ai internetului.

Noua civilizaţie informatică se bazează pe disponibilitatea şi accesabilitatea informaţiei. Aşa cum se arată în unele studii, producţia de informaţie reprezintă astăzi mai mult decât echivalentul fabricilor de ieri, pentru că informaţia nu se epuizează [46, p.90].

Apariţia şi dezvoltarea internetului nu constituie altceva decât o extindere a vieţii sociale asupra unui nou domeniu. Crearea tehnicii de calcul cu o potenţialitate de creştere şi funcţională enormă, implementarea acesteia într-o multitudine de activităţi sociale, economice sau manageriale, alături de creşterea exponenţială a valorii informaţiei au determinat necesitatea reglementării juridice a proceselor care au loc în sfera informatizării societăţii umane. Din păcate, însă, unele fapte indezirabile social care s-au petrecut şi se petrec în reţeaua internet reprezintă o chestiune atât de nouă şi cu o dezvoltare şi o diversificare atât de rapide încât legiuitorul este uneori depăşit de noile realităţi.

Noua economie se caracterizează prin influenţa internetului ca piaţă în societatea informaţională şi prin recunoaşterea importanţei bunurilor intangibile, care sunt nemateriale, au valoare şi crează valoare [142, p.6]. Informaţia stocată nu are nici o valoare în sine. Valoarea ei devenind neîndoielnică în momentul în care este utilizată, sau, mai rău, când nu este valorificată printr-o folosire eficientă şi rapidă.

Rolul determinant al informaticii în zilele noastre este ilustrat de faptul că însuşi statul este implicat în procesul de informatizare a societăţii şi progresul acesteia către o societate bazată pe informaţie, denumită societatea informaţiei. În cadrul acestui tip de societate un rol primordial îl au colectarea, stocarea, prelucrarea, transmisia, diseminarea şi utilizarea informaţiilor.

În Republica Moldova şi în întreaga lume, domeniul informatic şi cel telecomunicaţional au atins deja acel nivel, când relaţiile sociale din aceste domenii nu mai pot să se formeze, desfăşoare şi dezvolta fără o apărare juridico-penală eficientă. Locul infracţiunilor informatice şi al infracţiunilor în domeniul telecomunicaţiilor în peisajul juridic penal a devenit în scurt timp la fel de important ca acela al infracţiunilor ”clasice”, gravitatea acestora fiind accentuată de uşurinţa comiterii şi camuflării lor, de caracterul preponderent transfrontalier datorat mediului internet şi de potenţialul devastator al efectelor acesor fapte [170, p.254].

Dat fiind că în Codul penal al Republicii Moldova frauda informatică este încadrată în rândul infracţiunilor informatice apreciem ca fiind importantă prezentarea aspectelor generale ale acestor infracţiuni.

Condiţii preexistente în cazul infracţiunilor informatice şi în domeniul telecomunicaţiilor.

A. *Obiectul juridic al infracţiunilor*

a). *Obiectul juridic generic* îl reprezintă relaţiile sociale din domeniul informaticii şi al telecomunicaţiilor.

Prin informatică se înţelege domeniul de activitate care include prelucrarea şi transportarea datelor cu ajutorul sistemelor automatizate de calcul şi al mijloacelor de comunicaţie. În urma prelucrării datelor, acestea devin informaţii, care se vor distribui la locul unde au fost solicitate, într-o formă utilă pentru a fi utilizate la stabilirea unei decizii Prin prelucrarea informaţiei se înţelege colectarea, memorarea, organizarea, codificarea, transformarea, regăsirea, distribuirea ţi transmiterea informaţiilor [34, p.3].

Prin informaţie se înţelege, în sens general, posibilitatea de aducere la cunoştinţa unui operator uman a unui lucru, fapt, fenomen etc. Data, în sensul teoriei informaţiei, reprezintă codificarea informaţiei cu ajutorul unor simboluri sau semnale pe un suport sau mediu, în vederea prelucrării acesteia de către un sistem automat de calcul. Trebuie făcută distincţia între informaţie şi dată în sensul utilităţii lor, informaţia fiind accesibilă operatorului uman, iar data, în general, sistemului automat de calcul. Data este o reprezentare formală a conceptelor faptelor sau

instrucţiunilor, informaţia este înţelesul pe care data îl are pentru fiinţa umană. Data prezintă două aspecte diferite: pe de o parte este o potenţială informaţie pentru fiinţa umană, iar pe de altă parte se compune din instrucţiuni pentru calculator [34, p.3].

Noţiunea de informaţie face parte din viaţa cotidiană. Orice decizie, în orice domeniu, are la bază informaţii ce se obţin din prelucrarea unor date culese despre obiectul activităţii respective. Pentru a deveni informaţii, datele trebuie prelucrate în concordanţă cu cerinţele informaţionale; aceasta presupune culegerea datelor de la diverse surse; prelucrarea propriu-zisă şi distribuirea rezultatelor prelucrării – informaţiile – la locul în care sunt solicitate. Obiectul prelucrării datelor constă în convertirea acestora în informaţii care să stea la baza deciziilor [159, p.3].

Activitatea de prelucrare a informaţiei include [38, p.27-28]:

- culegerea datelor – reprezintă pregătirea ţi adunarea datelor ce urmează a fi prelucrate, date care sunt introduse şi care pot fi transferate pe un suport magnetic/optic până la prelucrare;

- prelucrarea datelor – datele care sunt subiectul activităţilor de prelucrare cuprind: calcule, comparări, sortări, clasificări sau însumări, iar aceste activităţi organizează, analizează şi manipulează datele convertindu-le în informaţii pentru utilizatori;

- transmiterea informaţionale – este activitatea în cadrul căreia informaţiile rezultate în urma prelucrării apar în forme variate pentru a fi transmise utilizatorilor în forma solicitată de către aceştia. În cadrul acestei activităţi, informaţiile trebuie să îndeplinească anumite condiţii de calitate care se referă la timp (viteza cu care informaţia ajunge la utilizator), conţinut (atributele care conferă valoare informaţiei) şi formă (felul în care informaţia ajunge la utilizator);

- stocarea produselor informaţionale, reprezintă activitatea dintr-un sistem informatic, în care datele şi informaţiile sunt depozitate într-un mod organizat în vederea unei utilizări ulterioare;

- controlul performanţelor sistemului – reprezintă o activitate care are în vedere următoarele elemente: un sistem informatic produce un un feed-back despre intrările, procesul şi ieşirile sale, precum şi despre activitatea de stocare a informaţiilor; feed-back-ul monitorizat şi evaluat pentru a determina dacă sistemul urmează să-şi atingă scopul prin performanţele sale, dar şi faptul că feed-back-ul va trebui utilizat pentru a efectua ajustări în activitatea sistemului informatic pentru a-i corecta deficienţele.

Prin telecomunicaţii înţelegem orice transmisiune, emisie sau recepţie de semne, semnale înscrieri, imagini, sunete sau informaţii de orice natură prin fir, radio, prin sisteme optice sau alte sisteme electromagnetice.

Fiecare dintre infracţiunile informatice şi infracţiunile în domeniul telecomunicaţiilor are un *obiect juridic special.* Acest obiect îl constituie relaţiile sociale cu privire la accesul legal la informaţia computerizată (obiectul juridic principal) şi relaţiile sociale cu privire la intervenţia legală în sistemul informaţional (obiectul juridic secundar) (lezate prin infracţiunea prevăzută în art. 259 C. pen. RM),

relaţiile sociale cu privire la circulaţia legală a mijloacelor tehnice sau produselor program (lezate prin infracţiunea specificată în art. 260 C. pen. RM); relaţiile sociale cu privire la legalitatea interceptării unei transmisii de date informatice care nu sunt publice (lezate prin infracţiuea prevăzută în art. 260^1 C.pen. RM); relaţiile sociale cu privire la integritatea, accesibilitatea şi circulaţia în condiţii de legalitate a datelor informatice (lezate prin infracţiunea specificată la art. 260^2 C. pen. al RM); relaţiile sociale cu privire la buna funcţionare a unui sistem informatic sub aspectul inviolabilităţii domiciliului informatic (lezate prin infracţiunea prevăzută la art. 260^3 C. pen. RM); relaţiile sociale cu privire la încrederea în datele informatice care permit accesul la un sistem informatic, în sensul utilizării corecte şi legale a acestora, precum şi în desfăşurarea corectă şi legală a operaţiunilor comerciale în legătură cu acestea (lezate prin infracţiunea specificată în art. 260^4 C. pen. RM); relaţiile sociale cu privire la încrederea publică în siguranţa şi fiabilitatea sistemelor informatice; la valabilitatea şi autenticitatea datelor informatice, a întregului proces modern de prelucrare, stocare şi tranzacţionare automată a datelor de interes oficial sau privat (lezate prin infracţiunea prevăzută la art. 260^5 C.pen. RM); relaţiile sociale cu privire la integritatea patrimoniului unei persoane, atunci când prezenţa respectivei persoane în spaţiul cibernetic se cuantifică într-un anumit volum de date stocate într-un sistem informatic sau, vehiculate într-o reţea (lezate prin infracţiunea specificată la art. 260^6 C. pen. RM); relaţiile sociale cu privire la securitatea sistemului informatic (lezate prin infracţiunea prevăzută la art. 261 C. pen. RM); relaţiile sociale cu privire la accesul autorizat la reţelele sau serviciile de telecomunicaţii (lezate prin infracţiunea specificată la art. 261^1 C. pen. RM) [170, p.254-255].

b) *Obiectul material sau imaterial* al infracţiunilor informatice şi din domeniul telecomunicaţiilor poate fi reprezentat de;

- informaţia computerizată, calculatoarele, sistemul informatic sau reţeaua informatică – în cazul infracţiunilor prevăzute de art. 259 C. pen. RM;

- informaţia protejată de lege – în situaţia infracţiunii prevăzute la lit. g) alin. (2) art. 259 C. pen. RM; mijloacele tehnice sau produsele program, concepute sau adaptate, în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 237, 259, 260^1-260^3, 260^5 şi 260^6 C. pen. RM – în ipoteza infracţiunii specificate la art. 260 C. pen. RM;

- transmisia de date informatice (inclusiv a unei emisii electronice) care nu sunt publice şi care sunt destinate unui sistem informatic, provin dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic – în cazul infracţiunii prevăzute la art. 260^1 C. pen. RM;

- datele informatice dintr-un sistem informatic, dintr-un mijloc de stocare sau cu acces limitat - în ipoteza infracţiunilor specificate la art. 260^2 C. pen. RM;

- datele informatice - în cazul infracţiunilor prevăzute în art. 260^3, 260^5, 260^6 C. pen. RM;

- parola, codul de acces sau datele similare care permit accesul total sau parţial la un sistem informatic – în situaţia infracţiunii specificate la art. 260^4 C. pen. RM;

- informaţia computerizată sau alte entităţi, inerente pe fundalul provocării unor urmări grave – în cazul infracţiunilor prevăzute la art. 261 C. pen. RM;

- reţelele sau serviciile de telecomunicaţii – în cazul infracţiunilor prevăzute de art. 261^1 C. pen. RM.

B. *Subiecţii infracţiunii*

a) *Subiect activ* al infracţiunilor informatice şi în domeniul telecomunicaţiilor este persoana fizică responsabilă care la momentul săvârşirii infracţiunii a împlinit vârsta de 16 ani (art. 259, 260^1-260^4, 261 şi 261^1 C. pen. RM) sau de 14 ani (art. 260 C. pen. R). Persoana juridică (cu excepţia autorităţii publice) este subiect în cazul infracţiunilor prevăzute la art. 259,260, 260^1, 260^1, 260^3, 260^4, 261 şi 261^1 C.pen. RM.

În anumite cazuri, subiectului activ al infracţiunilor analizate i se cere o anumită calitate specială. Astfel, doar persoana care nu este autorizată în temeiul legii sau al unui contract şi care depăşeşte limitele autorizării ori nu are permisiunea persoanei competente să utilizeze, să administreze sau să controleze un sistem informatic ori să efectueze cercetări ştiinţifice sau să desfăşoare orice altă operaţiune într-un sistem informatic poate fi subiectul infracţiunii prevăzute în art. 259 C. pen. RM.

b) Subiectul pasiv este caracterizat prin anumite calităţi speciale:

- proprietarul sau alt posesor al informaţiei computerizate, calculatorului, sistemului informatic sau reţelei informatice accesate ilegal – în cazul infracţiunii prevăzute în art. 259 C. pen. RM;

- persoana fizică sau juridică posesoare a mijloacelor tehnice sau a produselor program care au fost în mod fraudulos utilizate pentru a permite accesul într-un sistem informatic – în cazul infracţiunii prevăzute în art. 260 C. pen. RM;

- persoana fizică sau juridică care este posesoarea datelor informatice interceptate – în ipoteza infracţiunii prevăzute de de art. 260^1 C. pen. RM;

- persoana fizică sau juridică care posedă datele informatice care deţine datele informatice ce constituie obiectul imaterial al infracţiunii – în cazul infracţiunii prevăzute la art. 260^2 C. pen. RM;

- persoana fizică sau juridică posesoare a sistemului informatic, a cărui funcţionare este perturbată – în cazul faptei incriminate la art. 260^3 C. pen. RM;

- persoana fizică sau juridică posesoare a parolelor, codurilor de acces sau a altor asemenea date informatice care au fost în mod fraudulos utilizate pentru a permite accesul într-un sistem informatic – în cazul infracţiunii prevăzute la art. 260^4 C. pen. RM;

- persoana fizică sau juridică prejudiciată în propriile interese şi faţă de care se produc consecinţe juridice (de ordin patrimonial, moral sau social) în urma contrafacerii datelor informatice – în situaţia infracţiunii stipulate în art. 260^5 C. pen. RM;

- persoana al cărei interes patrimonial a fost prejudiciat prin acţiunea făptuitorului – în cazul faptei incriminate la art. 260^6 C. pen. RM;

- proprietarul sau alt posesor al resurselor sau al sistemelor informaţionale, al tehnologiilor şi mijloacelor de asigurare a acestora precum şi proprietarul sau alt posesor al informaţiei computerizate – în ipoteza infracţiunii specificate în art. 261 C. pen. RM;

- furnizorul de reţele de comunicaţii electronice sau furnizorul de servicii de comunicaţii electronice – în situaţia faptei incriminate în art. 261^1 C. pen. RM.

Conţinutul constitutiv al infracţiunilor informatice şi al infracţiunilor în domeniul telecomunicaţiilor.

A. **Latura obiectivă** a infracţiunilor informatice şi a infracţiunilor în domeniul telecomunicaţiilor se caracterizează prin faptul că fapta prejudiciabilă poate fi săvârşită prin modalitatea acţiunii (art. 259, 260, 260^1-260^6 şi 261^1 C. pen. RM) ori a acţiunii ori inacţiunii (art. 261 C. pen. RM).

Din punctul de vedere al structurii laturii obiective, infracţiunile în cauză sunt infracţiuni materiale (în ipoteza infracţiunilor specificate la art. 259, 260^2-260^6, 261 şi 261^1 C. pen. RM) sau formale (în cazul infracţiunilor prevăzute la art. 260 şi 260^1 C. pen. RM [170, p.256-257].

B. În ceea ce priveşte **latura subiectivă** în cazul infracţiunilor informatice şi a infracţiunilor în domeniul telecomunicaţiilor, acestea sunt săvârşite cu intenţie (în cazul infracţiunilor stipulate în art. 259, 260, 260^1-260^6 şi 261^1 C. pen. RM.

În situaţia infracţiunii prevăzute de art. 261 C. pen. RM, făptuitorul manifestă intenţie sau imprudenţă în raport cu fapta prejudiciabilă şi doar imprudentă în raport cu urmările prejudiciabile.

În rezultatul analizării alternative a locului de incriminare şi sancţionare penală a infracţiuni de fraudă informatică în legislaţia penală a Republicii Moldova şi a României putem sesiza o diferenţiere de concept în ceea ce priveşte politica instituirii locului incriminator de către legiuitorii statelor sus-menţionate.

Astfel, în legislaţia penală românească de referinţă frauda informatică este dislocată în Titlul II denumit *Infracţiuni contra patrimoniului*, Capitolul IV intitulat *Fraude comise prin sisteme informatice şi mijloace de plată electronice.*

Din această constatare se poate deduce că *conţinutul obiectul juridic generic al fraudei informatice incriminate în legislaţia penală românească îl formează relaţiile sociale a căror formare, existenţă şi dezvoltare sunt condiţionate de protejarea relaţiilor sociale cu caracter patrimonial. Prin urmare, dintr-o atare abordare legislativă frauda informatică este considerată drept o infracţiune patrimonială săvârşită prin utilizarea sistemelor informatice*.

O asemenea politică incriminatoare a fraudei informaţionale poate fi întâlnită şi în alte legislaţii penale, precum ar fi cea a Belorusiei, în care frauda informatică este descrisă în Titlul VIII *Infracţiuni contra proprietăţii şi ordinii de desfăşurare a activităţii economice,* Capitolul 24 *Infracţiuni contra proprietăţii* cu denumirea marginală de *sustragere prin folosirea tehnicii computerizate.* Astfel potrivit

art.212 C.pen. al Belorusiei infracţiunea constă în: *Sustragerea averii săvârşită prin modificarea informaţiei existentă în sistemul informaţional, pe suporţii materiali sau care este transmisă prin reţelele de transmitere a informaţie*i [87].

Într-un mod similar infracţiunea analizată este incriminată şi în legislaţia penală a Federaţiei Ruse la art. 159^6 C.pen. Potrivit textului de lege se pedepseşte penal fapta de escrocherie în sfera informaţiei computerizate, adică *sustragerea averii străine sau dobândirea dreptului asupra averii străine pe calea introducerii, ştergerii, blocării sau modificării informaţiei computerizate ori o altă influenţare a funcţionării normale a mijloacelor de păstrare, prelucrare sau transmitere a informaţiei computerizate sau a reţelelor de telecomunicare* [90].

Cu referire la legislaţia penală a Republicii Moldova se poate concluziona că locul incriminator al infracţiunii de fraudă informatică cunoaşte o altă amplasare, fapta fiind descrisă în Capitolul XI din Partea specială C.pen. al Republicii Moldova, cu denumirea marginală de *Infracţiuni informatice şi infracţiuni în domeniul telecomunicaţiilor.*

Prin urmare, rezultă că obiectul juridic generic al fraudei informaticii în legislaţie penală a R. Moldova îl formează un spectru specific de relaţii sociale a cărora existenţă şi desfăşare sunt condiţionate de protejarea informaticii şi telecomunicaţiilor. Prin urmare, dintr-o atare abordare legislativă frauda informatică este considerată drept o infracţiune informaţională care este, săvârşită prin utilizarea sistemelor informatice în scopul obținerii de benficii materiale.

În aceiaşi ordine de idei poate fi menţionat şi C.pen. al Estoniei, în care frauda informatică, cu denumirea marginală de escrocherie informatică este incriminată la art. 268 din Capitolul 14 C.pen. intitulat *Infracţiuni în sfera informaţiei computerizate şi prelucrării datelor*. Textul incriminator are următoarea formulare legislativă: *dobândirea averii străine, a avantajelor patrimoniale sau de altă natură prin introducerea programelor sau informaţiilor, prin modificarea, distrugerea, blocarea sau printr-o altă intervenţie realizată în procesul de prelucrare a informaţiei, care influenţează rezultatul acestuia şi care atrage după sine cauzarea unei daune materiale sau de altă natură proprietarului"* [195].

În lumina celor prezentate mai sus se poate concluziona că la baza institutorii locului incriminator al fraudei informatice în legislaţiile penale stau două criterii:

→ obiectul juridic de atentare;

→ mijlocul de comitere a infracţiunii.

Din noţiunea fraudei informatice, reiese în mod indubitabil că scopul final al infractorului nu este de a perturba sistemul informaţional, ci cel de a obţine anumite bunuri, beneficii sau drepturi asupra bunurilor. Prin urmare, anume aceasta este raţiunea legiuitorilor care incriminează frauda informatică ca infracţiune patrimonială. În această viziune legislativă relaţiile patrimoniale prevalează

faţă de relaţiile ce condiţionează existenţa sistemului informaţional, fapt pentru care frauda informatică este incriminată în compartimentul ce se referă ocrotirea penală a patrimoniului.

Totodată mijlocul de comitere a fraudei informatice este în măsură să perturbeze sau chiar să dăuneze în mod grav sistemul informaţional, afectându-se în acelaşi şi încrederea pe care persoanele o au în utilizarea acestora. În această abordarea deja relaţiile sociale referitoare la protejarea sistemului informaţional prevelază faţă de relaţiile sociale din domeniul patrimonial, fapt pentru care infracţiunea este incriminată în acel compartiment al legii penale care se referă la protejarea relaţiilor sociale din domeniul informaticii.

3.4. Concluzii la Capitolul 3

Concluziile desprinse din abordarea sediului normativ-preventiv de incriminare a fraudei informatice sunt următoarele:

1. Evaluarea cadrului normativ antifraudă din legislația Republicii Moldova și legislația României relevă faptul că în general acestea corespund cerinţelor impuse de Convenţia Europeană privind criminalitatea informatică, mai ales sub aspectului modelor incriminatoare instituite.

2. La baza poziționării locului incriminator al fraudei informatice în legislaţiile penale stau două criterii *obiectul juridic de atentare* şi *mijlocul de comitere a infracţiunii*.

3. Conţinutul obiectul juridic generic al fraudei informatice incriminate în legislaţie penală a României îl formează relaţiile sociale a căror formare, existenţă şi dezvoltare sunt condiţionate de protejarea relaţiilor sociale cu caracter patrimonial. Prin urmare, dintr-o atare abordare legislativă frauda informatică este considerată drept o infracţiune patrimonială săvârşită prin utilizarea sistemelor informatice, scopul infractorului fiind nu de a perturba sistemul informaţional, ci de a obţine anumite bunuri, beneficii sau drepturi asupra bunurilor. În această viziune legislativă relaţiile patrimoniale prevalează faţă de relaţiile ce condiţionează existenţa sistemului informaţional, fapt pentru care frauda informatică este incriminată în compartimentul ce se referă ocrotirea penală a patrimoniului.

4. Obiectul juridic generic al fraudei informaticii în legislaţie penală a Republicii Moldova îl formează un spectru specific de relaţii sociale a cărora existenţă şi desfăşare sunt condiţionate de protejarea informaticii şi telecomunicaţiilor. Într-o atare abordare legislativă frauda informatică este considerată drept o infracţiune informaţională care este, săvârşită prin utilizarea sistemelor informatice în scopul obţinerii de beneficii materiale. Mijlocul de comitere a fraudei informatice este în măsură să perturbeze sau chiar să dăuneze în mod grav sistemul informaţional, afectându-se în acelaşi timp şi încrederea pe care persoanele o au în acesta. Astfel, relaţiile sociale referitoare la protejarea sistemului informațional prevalează față de relațiile sociale din domeniul patrimonial, fapt pentru care fapta este incriminată în capitolul legii penale care se referă la protejarea relaţiilor sociale din domeniul informaticii.

5. Cercetarea structurală a legislaţiilor penale ale statelor lumii, aparținând diferitor sisteme de drept, în privinţa infracţiunii de fraudă informatică ne permite să efectuăm o clasificare a acestora, după cum urmează:

- **legi penale ce conţin o normă specială cu privire la frauda informatică**, aceasta fiind inclusă fie într-un capitol distinct dedicat infracţiunilor din domeniul informaticii şi/sau telecomunicaţiilor (Republica Moldova, Franţa, Belgia), fie într-un capitol comun cu alte infracțiuni contra patrimoniului (Federaţia Rusă, România, Republica Belarus, Polonia, Republica Federativă Germană) sau în alte capitole a legii penale (Canada);
- **legi penale ce nu conţin vreo normă specială care să prevadă infracţiunea de fraudă informatică**, aceasta fie că se încadrează în componenţa agravată a infracţiunii de escrocherie (Ucraina, Marea Britanie), fie se include în norma generală ce prevede înşelăciunea sau abuzul de încredere ca metode de comitere a sustragerii (Bulgaria, Spania).

6. Analiza și evaluarea structurii componenţei de infracţiune a fraudei inforamtice, mai ales în ceea ce ţine de momentul consumării infracţiunii, pune în evidenţă o particularitate specifică doar legii penale a Republicii Moldova în raport cu legislaţiile penale ale altor state, şi anume prezenţa în structura laturii obiective a infracţiunii a urmării prejudiciabile sub formă de daune în proporţii mari. Astfel, spre deosebire de C. pen. al Republicii Moldova, în legislaţia penală ale altor ţări (referindu-ne la statele a căror legislație penală a fost cercetată) urmările prejudiciabile nu condiționează existența infracţiunii de fraudă informatică.

4. INFRACȚIUNEA DE FRAUDĂ INFORMATICĂ ÎN LEGA PENALĂ A ROMÂNIEI ȘI REPUBLICII MOLDOVA

4.1. Conţinutul legal al infracţiunii

În legislaţia românească de referinţă *frauda informatică* este prevăzută în art. 249 al noului Cod penal român. În vechiul Cod penal această infracţiune nu exista. Infracţiunea este reprodusă fără modificări semnificative din 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 - se modifică doar pedeapsa în sensul reducerii ei. Legiuitorul roman a incriminat iniţial frauda informatică prin art. 49 al acestei legi.

În cuprinsul Titlului III al legii sus-menţionate erau definite trei categorii de infracţiuni;

a) infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice: infracţiunea de acces ilegal la un sistem informatic; infracţiunea de interceptare ilegală a unei transmisii de date informatice; infracţiunea de alterare a integrităţii datelor informatice; infracţiunea de perturbare a funcţionării sistemelor informatice; infracţiunea de a realiza operaţiuni ilegale cu dispozitive sau programe informatice;

b) infracţiuni informatice; infracţiunea de fals informatic; infracţiunea de fraudă informatică;

c) pornografia infantilă prin intermediul sistemelor informatice.

La rândul ei, această lege specială nu a făcut decât să reproducă textul art. 8 din Convenţia europeană pentru criminalitate informatică. Astfel, conform art. 8 din Convenţie, referitor la frauda informatică, fiecare parte va adopta măsuri legislative şi alte măsuri care se dovedesc necesare pentru incriminarea ca infracţiune, potrivit dreptului său intern, 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;

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.

Pentru a observa similarităţile, conform prevederilor art. 249 a noului Cod, prin fraudă informatică înţelegem 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.

Cu alte cuvinte, frauda informatică presupune intrarea, alterarea, ştergerea sau supraimprimarea de date sau de date pentru calculator sau orice altă intruziune care ar putea să genereze o influenţă a

rezultatului, cauzând prin aceasta un prejudiciu material sau economic intenţionat, făptuitorul urmărind să obţină un avantaj patrimonial pentru sine ori pentru altul [4, p.230].

Odată cu evoluţia tehnologică, oportunităţile de comitere a infracţiunilor contra patrimoniului s-au multiplicat. Bunurile care sunt reprezentate sau administrate cu ajutorul sistemelor informatice (fonduri electronice, depozite etc.) au devenit ţintele manipulărilor, la fel ca formele tradiţionale de proprietate [189, p.296].

Având în vedere această stare de fapt, s-a conturat nevoia legiuitorului de a elabora un cadru normativ specific, care să reglementeze, pe de o parte, folosirea sau desfăşurarea activităţii prin intermediul sistemelor informatice şi reţelelor de comunicaţii şi, pe de altă parte, să incrimineze nerespectarea regulilor stabilite pentru folosirea sau desfăşurarea acestei activităţi [69, p.194].

După cum se observă, în vechea reglementare, legiuitorul român încadra frauda informatică în cadrul infracţiunilor informatice, în timp ce noul Cod penal aduce o nouă viziune a legiuitorului, încadrând frauda informatică în cadrul infracţiunilor contra patrimoniului.

După cum am menţionat anterior, în ceea ce priveşte Codul penal al Republicii Moldova, frauda informatică face parte din randul infracţiunilor informatice, fiind reglementată în art. 260^6 C. pen., în Capitolul XXI intitulat ”Infracţiuni informatice şi infracţiuni în domeniul telecomunicaţiilor”.

Acesta prevede că prin fraudă informatică se înţelege "introducerea, modificarea sau ştergerea datelor 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 aceste acţiuni au cauzat daune în proporţii mari” [24].

Se poate observa că, în ceea ce priveşte conţinutul legal al infracţiunii, norma incriminatoare este relativ identică în legislaţia ambelor ţări, singura deosebire fiind că spre deosebire de Codul penal al României, unde nu contează valoarea acestui prejudiciu, fiind suficient să se dovedească faptul că patrimoniul persoanei vătămate a suferit o micşorare ca urmare a faptei comise de făptuitor, în Codul penal al Republicii Moldova este necesară cauzarea de daune în proporţii mari [9, p.31].

Conform art. 126 alin. (1) din Codul penal al Republicii Moldova se consideră proporţii mari valoarea bunurilor sustrase, dobîndite, primite, fabricate, distruse, utilizate, transportate, păstrate, comercializate, trecute peste frontiera vamală, valoarea pagubei pricinuite de o persoană sau de un grup de persoane, care depăşeşte 20 de salarii medii lunare pe economie prognozate, stabilite prin hotărîrea de Guvern în vigoare la momentul săvîrşirii faptei.

Deci, în cazul fraudei informatice, Codul penal al Republicii Moldova cere ca în momentul săvârşirii infracţiunii valoarei pagubei să depăşească 20 de salarii medii lunare pe economie prognozate, stabilite prin hotărîrea de Guvern în vigoare la momentul săvîrşirii faptei.

Similitudinea între cele două texte de lege îşi găseşte explicaţia în faptul că legislativul din ambele ţări a incriminat respectiva infracţiune reproducând textul Convenţiei Europene pentru criminalitate informatică.

În legătură însă cu textele normative comparate urmează să facem mai multe constatări.

În primul rînd, deși similtitudinea textelor normative dedicate incrimnării și pedepsirii fraudei informatice în legislaţia penală a R. Moldova şi a României este una vizibilă, aprecierea gradului prejudicabil sau a pericolului social al faptei în legislaţiile penale de referință este diferit.

În conformitate cu art. 15 C.pen. al R. Moldova, *gradul prejudiciabil al infracţiunii se determină conform semnelor ce caracterizează elementele infracţiunii: obiectul, latura obiectivă, subiectul şi latura subiectivă* [24].

În concepţia legiuitorului moldovean, gradul prejudiciabil al infracţiunii de fraudă informatică incriminată la art. 260^6 C.pen. al R. Moldova este determinat în mare parte de cuantumul evaluat în bani al urmării prejudiciabile ce survine în rezultatul comiterii infracţiunii. În baza acestei abordări legislative pentru existenţa temeiului juridic al răspunderi penale, prevăzut de art. 51 alin. (1) C.pen. R. Moldova este necesar ca în rezultatul săvârşirii faptei victimei să i se provoace o daună materială mai mare de 20 de salarii medii lunare pe economie prognozate, stabilite prin hotărîrea de Guvern în vigoare la momentul săvîrşirii faptei.

Cea de a doua constatare ţine de aprecierea naturii juridice a fraudei informaţionale în raport cu alte infracţiuni, precum ar fi, de exemplu, sustragerile, mai ales cea comisă prin escrocherie.

Numerose demersuri dedicate acestei problematici au fost iniţiate în doctrina dreptului penal, mai ales în cea rusă.

Într-o primă opinie, se consideră că fraudele informaţionale reprezintă infracţiunile săvârşite cu scop cupidant, prin intermediul manipulării programelor, datelor sau anumitor părţi componente ale computerului [221 p.71].

Potrivit unul alt punct de vedere, se afirmă că escrocheria informaţională reprezintă o infracţiune cu caracter informaţional, care presupune denaturarea, modificarea sau ascunderea intenţionată a datelor în scopul obţinerii cu ajutorul sistemului computerizat a unor beneficii băneşti [207, p.325].

Într-o altă accepţiune, escrocheria informaţională presupune dobândirea averii străine pe calea înşelăciunii, abuzului de încredere, însuşirii sau înstrăinării bunurilor, precum şi prin cauzarea de pagube materiale săvârşite prin utilizarea calculatorului [208].

După cum putem observa, în virtutea acestui ultim punct de vedere, este lărgită sfera de incidenţă a escrocheriei informaţionale, cuprinzând trei manifestări infracţionale incriminate distinct în legislaţia penală: escrocheria propriu-zisă; delapidarea averii străine; cauzarea de pagube materiale prin înşelăciune sau abuz de încredere.

Într-o altă viziune se consideră, pe drept cuvânt că extinderea conceptului de escrocherie informaţională la alte fapte penale săvârşite prin intermediul reţelelor informaţionale (cum ar fi, de exemplu, delapidarea averii străine, cauzarea de pagube materiale prin înşelăciune sau abuz de încredere, frauda informatică) poate fi acceptată doar în limitele unui studiu criminologic. Din perspectiva dreptului penal, o asemenea lărgire de concept nu poate fi acceptată, întrucât legiuitorul la art.190 C.pen. al R. Molodva fixează un cadru legal bine definit al escrocheriei, care nu poate fi extins la alte conduite ilicite cu caracter penal. De fapt, din raţiuni de tehnică legislativă, în vederea asigurării unei interpretări uniforme a normativului penal, nu poate fi acceptată ideea atribuirii unor înţelesuri diferite expresiilor şi termenilor folosiţi în legislaţia penală la descrierea componenţelor de infracţiune [26, p.19].

Dintr-o atare perspectivă, în vederea asigurării aplicării corecte a legii penale, în strictă consonanţă cu principiul legalităţii, este necesar de a stabili cu claritate normele cu caracter incriminator ce devin incidente în raport cu diferitele forme pe care le pot îmbrăca sustragerile din reţelele infromaţionale şi prin aceasta – limitele aplicării normei privitoare la escrocherie. Punctul de reper în acest sens, fără doar şi poate, îl constituie norma prevăzută la art.190 CP al Republicii Moldova, care stabileşte extremităţile de incidenţă a legii penale în ceea ce priveşte posibilitatea încadrării unei fapte ca escrocherie. În acest sens se concluzionează că fapta incriminată la art.190 C.pen. al R. Moldova devine aplicabilă când calculatorul şi informaţia computerizată sunt utilizate de către făptuitor pentru influenţarea voinţei victimei de a transmite benevol bunul sau dreptul asupra acestuia, sub dominaţia înşelăciunii sau abuzului de încredere [26, p.20].

După cum susţine T. Tropina, la operarea schemelor de inducere în eroare, *calculatorul* este utilizat în calitate de element adiţional, prin care se asigură apropierea cu victima, iar *mediul informaţional* – mediu alternativ celui fizic ce permite contactarea acesteia [211].

Se poate lesne observa că în această viziune escrocheria şi frauda informatică sunt abordate ca două infracţiuni distincte.

În accepţiunea noastră urmează a fi acceptat punctul de vedere exprimat de autorii S.Brînză şi V. Stati, potrivit cărora în raport cu infracţiunile prevăzute de art. 190 şi 196 C.pen. al R. Moldova, infracţiunea specificată la art. 260^6 C.pen. se distinge prin recurgerea la mijloace informatice (*e-mail*, mesagerie instantă, pagină *Web* etc.), aplicate într-un mediu informatic. Tocmai aceste mijloace speciale de săvârşire a infracţiunii au ca efect că alin. (1) al art. 260 C.pen. reprezintă o normă specială faţă de art. 190 şi 196 C.pen. În consecinţă, aplicarea alin. (1) art. 260^6 C.pen. eclude reţinerea la calificare a uneia dintre infracţiunile prevăzute la art. 190 sau 196 C.pen. [170, p.391]

Deşi ne solidarizăm acestei ultime opinii urmează să facem două precizări referitoare la incriminarea fraudei informaţionale în legislaţia de referinţă a R. Moldova.

În primul rând, din dispoziţia normei incriminatorii al art. 260^6 C.pen. nu rezultă în mod expres că frauda informatică ar reprezenta o formă specială a infracţiunii de escrocherie (art.190 C.pen.) şi a celeia de cauzare a daunelor materiale prin înşelăciune sau abuz de încredere (art.196 C.pen.). Această soluţia calificativă rezultă mai mult din substanţa lucrurilor, necunoscând, totodată, şi o consacrare legală.

În al doilea rând, regimul sancţionator al infracţiunii de escrocherie este cum mult mai diferenţiat şi, în acelaşi timp, mai aspru decât cel aplicat pentru infracţiunea de fraudă informatică (art. 260^6 C.pen.).

De exemplu, legiuitorul moldovean diferenţiază răspunderea penală pentru escrocheria comisă în proporţii mari (art. 190 alin. (4) C.pen.) şi escrocheria comisă în proporţii deosebit de mari (art. 190 alin. (5) C.pen). În primul caz, pedeapsa este de închisoare de la 7 la 10 ani cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de până la 5 ani. În cel de al doilea caz, închisoare de la 8 la 15 ani cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de până la 5 ani. Pentru frauda informatică săvârşită în proporţii mari, se poate aplica pedeapsa amenzii de la 1000 la 1500 unităţi convenţionale sau muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare de la 2 la 5 ani, iar pentru cea în proporţii deosebit de mari - de la 4 la 9 ani.

În acelaşi timp, după cum s-a menţionat anterior pentru existenţa componenţei de infracţiune descrise la art. 260^6 C.pen. este obligatoriu ca fapta să fie comisă în proporţii mari (care depăşeşte 20 de salarii medii lunare pe economie prognozate, stabilite prin hotărîrea de Guvern în vigoare la momentul săvîrşirii faptei), pe când în cazul escrocheriei condiţia limită este ca dauna să depăşească cuantumul de 25 de unităţi convenţionale ale amenzii. Prin urmare, frauda informatică săvârşită în forma escrocheriei în proporţii de până la 20 de salarii medii lunare pe economie prognozate rămâne în afara ariei de incriminare.

Or, avantajele imense ale informaticii sunt absolut evidente, aceasta influenţând decisiv progresul umanităţii. Pe bună dreptate se afirmă revoluţia informatică – în special aceea desfăşurată pe internet cea de a treia (şi probabil, ultima) revoluţie industrială [191, p.9]. Tehnologia informaţională atinge fiecare aspect al vieţii cotidiene a unei persoane fără a şine cont de poziţionarea geografică a acesteia. Tot mai multe activităţi comerciale, industriale, economice sau guvernamentale sunt dependente de reţele informatice. Calculatoarele sunt utilizate în primul rând pentru creşterea performanţelor economice şi industriale ale unei ţări, acestea devenind parte integrantă a dezvoltării activităţilor economice. Riscurile generate de dependenţa de sistemele şi tehnologiile informaţionale, de echipamentele tehnice şi *software-ul* aferent, cresc pe zi ce trece riscul de vulnerabilitate al reţelelor informatice, fiind din ce în ce mai greu de a se putea localiza un punct de acces ilegal în reţea sau un utilizator care are intenţii ilegale.

Astfel, de *lege lata* nu se pare a fi o soluţia echitabilă şi corespunzătoare realităţilor timpului de a pedepsi escrocheria informaţională în legislaţia penală a R. Moldova ca o variantă alternativă atenuantă a escrocheriei clasice.

Prin urmare, propunem reformularea textului incriminator al art. 260^6 C.pen. al R. Moldova, astfel încât, pe de o parte, frauda informatică comisă prin escrocherie să cunoască un regim diferenţiat de sancţionare faţă frauda informatică comisă prin cauzarea de daune materiale sau abuz de încredere, iar pe de altă, echivalarea gradului de prejudiciabilitate al escrocheriei incriminate la art. 190 C.pen. al R. Moldova cu cel al escrocheriei săvârşite prin fraudă informatică.

În acelaşi timp considerăm neîntemeiată soluţia legiuitorului moldovean de a limita cercul subiecţilor activi al fraudei informatice doar la persoanele fizice. Considerăm că în contextul progresului tehnico-ştiinţific, succeptibilitatea persoanelor juridice de a fi implicate în activităţi infracţionale legate de fraude informatice este una evidentă. În plus, poate fi exemplificată şi experienţa legislativă a României, care a recunoscut persoana juridică în calitate de subiect activ al fraudei informatice.

În cele din urmă propunem următoarea variantă a textului incriminator de la art. 260^6 C.pen. al R. Moldova:

Frauda informatică,

(1) Dobîndirea ilegală a bunurilor altei persoane, a avantajelor materiale sau de altă natură prin introducerea, modificarea sau ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic,

se pedepsesc cu amendă în mărime de la 550 la 850 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare până la 4 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 1000 la 3000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(2) Aceleaşi acţiuni săvârşite:

a) de un grup criminal organizat sau de o organizaţie criminală;

b) în proporţii mari

se pedepsesc cu închisoare de la 4 la 8 ani cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de până la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 3000 la 5000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(3) Acţiunile prevăzute la alin. (1)-(2) săvîrşite în proporţii deosebit de mari

se pedepsesc cu închisoare de la 7 la 12 ani cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de până la 5 ani, iar persoana juridică se pedepseşte cu

amendă în mărime de la 5000 la 10000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea persoanei juridice.

(4) Cauzarea de pagube materiale prin introducerea, modificarea sau ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic săvârşită în proporţii mari, dacă fapta nu este o însuşire

se pedepsesc cu amendă în mărime de la 200 la 500 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare de până la 3 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 500 la 3000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(5) Acţiunile prevăzute la alin.(4) săvârşite în proporţii deosebit de mari

se pedepsesc cu închisoare de la 3 la 6 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 3000 la 5000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

În continuare v-om analiza din punct de vedere juridico-penal infracțiunea de fraudă informatică din perspectiva a două legislații penale în vigoare: cea a României și a R. Moldova.

4.2. Condiţii preexistente

a) **Obiectul infracţiunii.** Obiectul juridic special îl constituie relaţiile sociale care protejează securitatea şi fiabilitatea activelor reprezentate sau administrate cu sisteme informatice (fonduri electronice, depozite, banking-ul electronic la domiciliu, gestiunea informatizată a stocurilor, conturilor, ghişeelor automate care pot fi manipulate) sau a altor instrumente care pot avea consecinţe asupra relaţiilor juridice de proprietate şi cele care se referă la încrederea în siguranţa şi fiabilitatea transferurilor efectuate [6, p.576].

Astfel, pentru exemplificare, în luna martie 2012, partea vătămată BR a identificat pe site-ul comercial „DER LANDWIRT-AGRICULTORUL” o ofertă de vânzare a unor tractoare marca Fendt şi fiind interesat de cumpărarea unor astfel de tractoare a purtat o corespondenţă electronică cu ofertantul, care s-a prezentat mag. diplomat Josef Valky şi dorind să cumpere două astfel de utilaje, a convenit cu acesta să vireze contravaloarea lor în contul indicat de vânzător, având codul IBAN SK6152000000000012543192.

Partea vătămată a fost convins de tranzacţia încheiată, de realitatea şi de siguranţa acesteia cu atât mai mult cu cât a constatat că mesajele informatice proveneau de la o adresă de e-mail creată pe numele firmei-vânzătoare(AGRO MASCHINEN) ce avea propria pagină de internet, astfel că la data de 28 martie 2012 a trimis suma de 11.500 de euro, iar la data de 10 aprilie 2012 diferenţa, respectiv 11.500 de euro în contul indicat, deschis la data de 11 martie 2011 pe numele inculpatului A.G, însă,

neprimind bunurile contractate a anunţat organele de poliţie care au constatat că pagina respectivă de internet între timp dispăruse, fiind evident că mag. diplomat Josef Valky cu care purtase corespondenţa, era de fapt inculpatul A.G.

Faptele inculpatului, aşa cum au fost expuse mai sus, respectiv acţiunea de introducere de date informatice în contextul inducerii în eroare prin folosirea de nume mincinoase cu ocazia încheierii unui contract de vânzare-cumpărare, ce a determinat crearea în mod repetat şi în baza aceleiaşi rezoluţii infracţionale un prejudiciu patrimonial (suma de 23.000 euro), întruneşte elementele constitutive ale infracţiunilor de fraudă informatică, prev. de art. 49 din Legea nr. 161/2003 (Fapta de a cauza un prejudiciu patrimonial unei persoane prin introducerea, modificarea sau ştergerea de date informatice, prin restricţionarea accesului la aceste date ori prin împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, care se pedepseşte cu închisoare de la 3 la 12 ani) şi de înşelăciune, prev. de art.215 alin. 1 (Inducerea în eroare a unei persoane, prin prezentarea ca adevărată a unei fapte mincinoase sau ca mincinoasă a unei fapte adevărate, în scopul de a obţine pentru sine sau pentru altul un folos material injust şi dacă s-a pricinuit o pagubă, se pedepseşte cu închisoare de la 6 luni la 12 ani), alin. 2 (Înşelăciunea săvârşită prin folosire de nume sau calităţi mincinoase ori de alte mijloace frauduloase se pedepseşte cu închisoare de la 3 la 15 ani) şi de alin.3 (Inducerea sau menţinerea în eroare a unei persoane cu prilejul încheierii sau executării unui contract, săvârşită în aşa fel încât, fără această eroare, cel înşelat nu ar fi încheiat sau executat contractul în condiţiile stipulate, se sancţionează cu pedeapsa prevăzută în alineatele precedente, după distincţiile acolo arătate) din Codul penal, texte de lege în baza cărora va fi condamnat [198].

Astfel, obiectul juridic special în acest caz l-au reprezentat relaţiile sociale de ordin patrimonial precum şi întregul fascicol de relaţii referitoare la încrederea în siguranţa şi fiabilitatea tranzacţiilor informatice.

Plecând de la locul diferit de incrimnare a fraudei informatice în legislația penală română și cea moldovenească, putem sesiza și diferențiere a conținutului relațiilor sociale ce formează obiect juridic special de atentare.

b) **Obiectul material** constă în bazele de date, aplicaţiile şi programele vizate de făptuitor, sau în componentele materiale care compun sistemele informatice, începând cu calculatoarele propriu-zise, elementele de stocare şi transmitere a datelor, sistemele de conectare.etc [155, p.269].

Prin *sistem informatic* se înţelege orice dispozitiv sau ansamblu de dispozitive care sunt interconectate sau care se află în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic.

Tradiţional, un sistem informatic a fost definit prin două componente: una referitoare la funcţia sa, iar o a doua referitoare la structura sa. Astfel, dintr-o perspectivă structuralistă, un sistem

informatic constă într-o colecţie de oameni, procese date şi tehnologii care formează o structură care serveşte anumite funcţii sau obiective. Pe de altă parte, dintr-o perspectivă funcţională, un sistem informatic este este un mediu implementat tehnologic, cu scopul de a înregistra, stoca şi transmite informaţii. Prin executarea acestor funcţii, un sistem informatic facilitează crearea şi schimbul de înţelesuri care servesc scopuri sociale cum ar fi executarea unor acţiuni sau formularea sau justificarea unei idei [61, p.841].

Prin *program informatic* se înţelege un ansamblu de instrucţiuni care pot fi executate de un sistem informatic în vederea obţinerii unui rezultat determinat, sau prin acesta se înţeleg programe pentru calculator, procedure şi documentaţie, care permit efectuarea unei sau mai multor operaţiuni pe un sistem informatic.

Prin *date informatice* se înţelege orice reprezentare a unor fapte, informaţii sau concept într-o formă care poate fi prelucrată printr-un sistem informatic. În această categorie se include şi orice program informatic care poate determina realizarea unei funcţiii de către un sistem informatic.

Pot fi considerate elemente de stocare a datelor: un hard disk (disc magnetic folosit pentru stocarea datelor); un CD (disc optic); o dischetă (suport magnetic); orice fel de dispositive portabile utilizate ca mediu de stocare a informaţiei (memory stick) etc.

Astfel, pentru a exemplifica, analizând probele administrate în cauză, respectiv: procesele verbale de sesizare din oficiu, procesele verbale întocmite cu ocazia efectuării percheziţiilor domiciliare, procesele verbale de transcriere a convorbirilor telefonice ale inculpaţilor, procesele verbale de transcriere a traficului internet al inculpaţilor, datele referitoare la instrumentele de plată electronică aparţinând unor cetăţeni români, procesele verbale de percheziţie s sistemelor informatice şi a suporturilor de stocare a datelor ridicate de la inculpaţi, declaraţiile martorilor, înscrisurile depuse de inculpaţi în apărare şi în circumstanţiere, raportul de expertiză tehnică şi răspunsul expertului la obiecţiunile formulate de părţi, declaraţiile inculpaţilor, instanţa de fond a reţinut următoarea situaţie de fapt:

Inculpaţii s-au cunoscut în cursul anului 2005, în timp ce erau elevi, fiind preocupaţi de jocurile pe calculator. Inculpatul R. D. C. le-a propus celorlalţi inculpaţi să comită împreună fraude informatice în vederea obţinerii, în mod ilegal, de date de identificare a cardurilor bancare aparţinând unor persoane din străinătate. Aceste date urmau să fie falsificate pentru efectuarea de operaţiuni de extragere de numerar sau de plăţi, fără consimţământul titularului, în scopul obţinerii de beneficii materiale.

Pentru realizarea acestui scop infracţional inculpaţii au creat cu ajutorul unor programe Software speciale, baze de date conţinând adrese valide de e-mail (useri şi parole) ale unor utilizatori ai platformelor comerciale eBay, PayPal sau ale unor bănci din străinătate (preponderent din S.U.A.),

au falsificat paginile de înregistrare ale site-urilor acestora, prin modificarea codului sursă, înlocuind adresa de contact a administratorului PayPal şi a băncilor cu alte adrese de e-mail ce le aparţineau.

Paginile false de înregistrare au fost transmise către adrese valide de e-mail din baza de date creată anterior (metodă denumită „spam”). O parte dintre utilizatorii care au primit mesajul „fals" de înregistrare sau reconfimiare a datelor au fost induşi în eroare şi şi-au introdus datele pe site-urile respective. Datele de înregistrare ale utilizatorului legitim au fost direcţionate, fară ştirea utilizatorului, către adresa de e-mail specificată în codul sursă, odată cu efectuarea click-ului pe „sign in". în acest mod inculpaţii au obţinut date de identificare ale unor carduri bancare valide aparţinând unor persoane din străinătate.

Ulterior, inculpaţii au utilizat datele cârdurilor bancare astfel obţinute, prin efectuarea de plăţi din conturile de card pentru diverse servicii sau prin transmiterea acestor date altor persoane în vederea transcrierii lor pe carduri blank, în scopul utilizării la ATM-uri pentru extrageri de numerar.

Din transcrierea traficului internet al sistemului informatic utilizat de către inculpaţii R. D. C., O. G. F. şi D. V. au fost identificate date referitoare la instrumentele de plată electronice aparţinând unor cetăţeni străini, nr. de card, titular, adresă, codul poştal, codurile PIN şi CVV2, data expirării (…). Pe traficul internet al inculpaţilor au fost identificate pagini de scam - pagini modificate ale site-urilor www.paypal.com., www.fairwinds.com, www.amazon.com, www.pinacle.com, www.maumaolinc.org., în scopul obţinerii datelor de identificare a cardurilor bancare.

Acţiunile de fraudă informatică desfăşurate de inculpaţi şi programele speciale utilizate de ei în acest scop au fost relevate de rezultatele percheziţiilor în sistem informatic efectuate asupra calculatoarelor ridicate de la aceştia.

Astfel, instanţa de fond a constatat că inculpatul D. V. avea stocat un fişier denumit „…”, ce conţinea datele de identificare ale unui cetăţean din S.U.A., precum şi datele unei cărţi de credit.

S-a mai constatat că în sistemele informatice şi de stocare a datelor informatice ridicate de la inculpatul O. G. F. au fost descoperite mai multe fişiere ce conţineau date de identificare ale unor cetăţeni americani, precum şi datele unor cărţi de credit. Astfel, au fost descoperite mai multe aplicaţii şi componentele acestora, cu ajutorul cărora inculpatul accesa neautorizat sisteme informatice, un fişier ce conţinea sursa unei pagini de spam prin care se solicita introducerea datelor de identificare (nume, prenume, data naşterii, adresa), precum şi date referitoare la cartea de credit (mr., data expirării, CVV2). S-a reţinut că din dosar rezultă că în urma percheziţiei suportului de stocare a datelor tip flash memory marca „Traxdata” au fost identificate 4 fişiere ce conţineau date de identificare ale mai multor cărţi de credit şi date referitoare la titularii acestora, precum şi 6 fişiere ce nu au putut fi accesate, întrucât au fost criptate cu ajutorul programului „…”, iar inculpatul a refuzat să dea relaţii despre parola folosită.

Prima instanţă a mai reţinut că în sistemele informatice şi de stocare a datelor informatice ridicate de la inculpatul O. A. au fost descoperite mai multe fişiere ce conţineau date de identificare ale unor cetăţeni străini, precum şi mai multe cărţi de credit obţinute ilegal de pe internet. Astfel, pe hard disk şi pe 5 CD-uri şi 1 DVD au fost descoperite mai multe adrese de I.P., folosite de inculpat pentru a trimite mail-uri tip spam, conturi şi parole ale mai multor utilizatori ai site-ului wwvv.paypal.com, documentaţii crak şi hack, aplicaţii scanner.exe şi ws2check.exe folosite de inculpat pentru realizarea activităţii infracţionale.

S-a mai reţinut de către instanţa de fond, că în sistemele informatice şi de stocare a datelor informatice ridicate de la inculpatul R.D.C. au fost descoperite fişiere conţinând adrese de I.P. folosite pentru a trimite mail-uri tip spam, conturi şi parole ale mai multor utilizatori ai site-ului www.paypal.com, date de identificare ale unor cetăţeni americani, datele unor cărţi de credit şi numere de identificare ale mai multor bănci din S.U.A.. în urma percheziţiei dispozitivului MP3 player au fost găsite date de identificare ale unor cetăţeni străini, datele referitoare la cărţilor lor de credit, numere de identificare ale mai multor bănci din SUA, fişiere în format HTML conţinând pagini de spam ale site-ului www.paypal.com. adrese IP, nume de servere şi parole de accesare a acestora. Totodată, s-a constatat că a fost identificat şi un fişier criptat ce nu a putut fi accesat, inculpatul refuzând să declare parola utilizată.

S-a mai stabilit de către Tribunalul Neamţ că, după ce intrau în posesia datelor de identificare ale cetăţenilor străini şi a datelor referitoare la instrumentele de plată electronice aparţinând acestora, cu ajutorul aplicaţiei CC2 Bank.exe, inculpaţii verificau băncile emitente ale cârdurilor, pentru a se asigura că acestea sunt valabile. Instanţa de fond a apreciat că vinovăţia inculpaţilor a rezultat, fară nici un dubiu, din materialul probator administrat în cauză. în acest sens, a constatat că din declaraţia inculpatului D. V. a rezultat că, în cursul anului 2006 a cooperat împreună cu inculpaţii R. D. C. şi O. G. F. în vederea obţinerii de foloase materiale ilicite prin activităţi de fraudă informatică.

De asemenea, a mai reţinut că Inculpatul O. G. F. a recunoscut şi el că în anul 2005 şi ulterior în anul 2007, a lucrat, împreună cu inculpaţii R. D. C. şi O. A., pentru acelaşi scop infracţional, iar inculpaţii susmenţionaţi au arătat că iniţiativa în constituirea asocierii a aparţinut inculpatului R. D. C., că acesta i-a învăţat să utilizeze programele informatice, că şi-au utilizat calculatoarele pentru a obţine date de identificare ale card-urilor, pe care le-au pus la dispoziţia inculpatului R. D. C. Inculpaţii au oferit detalii referitoare la activitatea lor infracţională, la modul de operare şi la rolul pe care 1-a avut fiecare dintre ei în comiterea infracţiunilor informatice.

Aceste declaraţii, coroborate cu procesele verbale de transcriere a traficului pe Internet şi a datelor referitoare la instrumentele de plată electronică, identificate cu ocazia percheziţiei informatice, au relevat un mod de operare comun, îndreptat spre obţinerea aceluiaşi rezultat. Inculpaţii au plănuit împreună să comită infracţiuni informatice, repartizându-şi rolurile, sens în care au cooperat pe

parcursul mai multor luni de zile. Infracţiunea de asociere a fost comisă cu intenţie directă, întrucât toţi inculpaţii au cunoscut scopul asocierii, dorind să obţină foloase materiale ilicite [198].

Obiectul material în acest caz a constat în bazele de date, aplicaţiile şi programele vizate de făptuitor pentru obţinerea unor beneficii materiale.

Subiectul infracţiunii. a) Subiect activ al acestei infracţiuni poate fi orice persoană fizică sau juridică, în practică, însă, manipulările constatate sunt comise cel mai adesea de angajaţi sau funcţionari sau de persoane cu cunoştinţe avansate în domeniul calculatoarelor [99, p.144]. Subiect activ ar putea fi chiar unul dintre angajaţii unei societăţi comerciale care ar trebui sa supravegheze bunul mers al sistemelor de gestiune informatizată, situaţie în care descoperirea lui este mult îngreunată. Participaţia penală este posibilă sub toate formele (complicitate, coatorat instigare).

Conform Codului penal al Republicii Moldova subiect activ al infracţiunii poate fi orice persoană fizică responsabilă care a împlinit 16 ani.

b) Subiect pasiv al infracţiunii este persoana fizică sau juridică (publică sau privată) proprietară sau utilizatoare a sistemului informatic afectată patrimonial prin comiterea fraudei informatice.

În unele situaţii poate exista subiect pasiv colectiv, constând într-o mulţime de persoane fizice sau juridice afectate de perturbarea sistemului informatic la care sunt interconectate [155, p.369].

Astfel, organele de urmărire penală din România au fost sesizate de mai mulţi cetăţeni străini cu privire la faptul că începând cu anul 2005 aceştia au fost induşi în eroare prin intermediul internetului de inculpaţii şi învinuiţii menţionaţi, în sensul că accesând site-urile Ebay sau ale altor companii specializate în vânzarea unor produse on-line, au luat legătura cu aceştia şi au negociat prin e-mail sau prin telefon condiţiile de tranzacţionare a unor bunuri, în special utilaje agricole şi telefoane mobile, iar după ce au transferat banii în România, prin Western Union sau prin altă modalitate de plată, reprezentând un avans sau preţul total al obiectului contractului, aşa zişii vânzători au întrerupt orice legătură cu victimele.

De asemenea, organele de cercetare penală ale poliţiei judiciare din cadrul Serviciului de Combatere a Criminalităţii Organizate Vâlcea s-au sesizat din oficiu cu privire la faptul că un grup infracţional organizat, coordonat de C.A., aşa cum s-a stabilit mai târziu, acţionează în special în municipiile Drăgăşani şi Bucureşti, în scopul inducerii în eroare a cetăţenilor străini în modalităţile descrise anterior, grupul având o structură bine definită, incluzând paliere ierarhice de coordonare şi execuţie, de racolare a altor persoane dispuse contra unui comision să ridice banii care aveau ca sursă fraudele informatice şi care erau transferaţi de victime prin sistemul Western Union sau în alte moduri.

În sfârşit, companiile Ebay şi Paypal au formulat sesizări şi au prezentat date şi informaţii din cuprinsul cărora rezultă că grupul infracţional organizat a deţinut date informatice prin utilizarea cărora au fost fraudate conturi ale utilizatorilor legitimi ai celor două companii, generând astfel prejudicii localizate în patrimoniul lor.

Pe baza probelor administrate în faza urmăririi penale s-a stabilit că faptele ce constituie obiectul dosarului au fost comise de inculpaţii C.A., M.N.G., C.I.C. şi P.D.CV., precum şi de învinuiţii C.N.I. şi B.C.G. în circumstanţele ce vor fi descrise în cele ce succed, după o analiză succintă a structurii organizatorice a grupului şi a modalităţilor lor de operare.

Astfel, aceştia, în perioada 2005-2008, prin accesarea nelegală a unor conturi aparţinând unor companii specializate în vânzarea on-line, prin crearea unor site-uri şi conturi capcană în cuprinsul cărora ofereau în mod mincinos spre vânzare diferite bunuri, cu preponderenţă utilaje agricole şi telefoane mobile, precum şi prin lansarea on-line a unor licitaţii frauduloase au prejudiciat nenumăraţi cetăţeni străini, cărora le-au produs o pagubă însumată extrem de mare, dacă ar fi să luăm în calcul toate formularele de plata Western Union ridicate de la instituţiile bancare, până în prezent depunând plângere penală 32 de cetăţeni străini şi două companii, care au suferit un prejudiciu total de aproximativ 278.000 lei.

S-a apreciat că organizatorul şi coordonatorul grupului infracţional organizat este inculpatul C.A. care i-a atras în activitatea infracţională, în funcţie de aptitudinile fiecăruia, pe ceilalţi inculpaţi, învinuiţi şi făptuitori şi pe care i-a folosit în principal la ridicarea sumelor de bani ce proveneau din licitaţiile electronice frauduloase şi la racolarea altor persoane care să procedeze în acelaşi mod.

Se distinge sub acest aspect inculpatul C.I.C. care i-a racolat pe făptuitorii P.S. , M.I. şi D.C.N. în scopul de a ridica bani transferaţi din străinătate ce proveneau din fraude informatice, după ce el însuşi a prestat această activitate. Astfel de activităţi de recrutare au fost efectuate şi de inculpatul Popa Dumitru - Cătălin, care supraveghea activitatea inculpatului M.N.G., conducându-l la unităţile Western Union în vederea ridicării banilor pentru C.A.. În susţinerea aceleiaşi idei, din actele dosarului se observa că sub coordonarea lui C.A., ceilalţi inculpaţi, învinuiţii şi făptuitorii au avut roluri precise în structura organizatorică a grupului, acesta funcţionând pe parcursul mai multor ani, perioadă în care s-au obţinut beneficii materiale considerabile.

Toate aceste aspecte se desprind din analiza probelor administrate care constau în interceptarea şi înregistrarea convorbirilor telefonice, precum şi a comunicărilor informatice derulate prin adresa de e-mail „transfer_important@yahoo.com”, formularele Western Union, plângerile victimelor şi corespondenţa prin e-mail, declaraţiile martorilor şi ale inculpaţilor, precum şi ale învinuiţilor, constatările grafoscopice efectuate în cauză, rezultatul perchiziţiilor informatice efectuate asupra sistemelor informatice şi a suporturilor de stocare a datelor informatice ridicate de la inculpaţi, precum şi în celelalte acte ale dosarului. In cauză au fost efectuate percheziţii la domiciliile şi reşedinţele inculpaţilor, învinuiţilor şi făptuitorilor, fiind identificate obiecte si înscrisuri cu valoare probatorie ce întregesc dovedirea activităţii infracţionale, constând în calculatoare, telefoane mobile, suporturi de stocare a datelor informatice etc. conţinând date şi informaţii referitoare la fraudele informatice,

accesul fără drept la sisteme informatice, deţinerea fără drept de date informatice, adrese de e-mail folosite la înşelarea victimelor, fotografiile şi parametrii bunurilor tranzacţionate etc.

1. În luna februarie 2005, cetăţeanul singaporez Yen Young Sim Edmund a vizitat site-urile Ebay în ideea de a achiziţiona telefoane mobile marca Nokia 9500, împrejurare în care a luat legătura cu titularul adresei de e-mail redbear925@hotmail.com care l-a convins să transfere în România pe numele inculpatului M.N.G. prin sistemul rapid de plată Western Union în două tranşe, suma totală de 1.860 dolari singaporezi. Este de observat că ofertantul i-a indus victimei ideea că reprezintă o companie prosperă, specializată în tranzacţii on-line şi totodată şi-a impus propriile reguli de derulare a tranzacţiei, în sensul că banii urmau să fie transferaţi prin Western Union, ceea ce s-a şi întâmplat, iar bunul să fie trimis prin serviciul internaţional de livrare UPS, reguli care nu au nicio legătură cu serviciile Ebay şi Paypal. În scopul ridicării banilor de la instituţiile bancare, inculpatul M.N.G. a completat formularele de plată Western Union cu MTCN 9926441858 şi 1815877860.

Partea vătămată s-a constituit parte civilă în procesul penal şi a solicitat să fie despăgubită cu suma 1.860 dolari singaporezi.

2. În data de 27.07.2005 Daryoush Ghanbarpour i-a transferat prin sistemul Western Union suma de 210 USD învinuitului C.N.I. reprezentând contravaloarea unui telefon mobil marca Nokia N90, pe care evident că victima nu l-a primit, negocierea având ca punct de plecare tot site-urile platformei Ebay. Suma de 210 USD, care compune prejudiciul pricinuit victimei, a fost încasată de inculpat în data de 28.07.2005 de la o agenţie Western Union din municipiul S., unde a completat formularul de plată cu MTCN 2345470457.

Partea vătămată s-a constituit parte civilă în procesul penal şi a solicitat să fie despăgubită cu suma de 210 USD reprezentând daune materiale.

3. În cadrul unei comisii rogatorii autorităţile judiciare din Germania au înaintat depoziţia părţii vătămate Dennis Chmielewski conform căreia în luna august 2005, în urma unei negocieri derulată prin internet i-a transferat în România lui C.N.I.suma de 250 euro, reprezentând jumătate din contravaloarea unui număr de 5 telefoane mobile marca Nokia 9300i. Sub pretextul că şeful lui o să-i facă mari necazuri pentru că a trimis telefoanele fără să primească toţi banii, reprezentând preţul lor, ofertantul l-a convins pe cetăţeanul german să trimită în România şi diferenţa de 250 euro, prejudiciul total suferit de victimă fiind de 500 euro. În data de 19.08.2005 inculpatul C.N-I. a completat la Poşta Română SA Agenţia Craiova formularul cu MTCN 3317782491.

4. Cetăţeanul german Dorothee Schmid a comandat două telefoane mobile pe Ebay, în cursul lunii august 2005, pentru achiziţionarea cărora i-a transferat învinuitului C.N.I. suma de 300 euro, banii fiind încasaţi de învinuit în data de 23.08.2005 de la un oficiu poştal din mun. Craiova, împrejurare în care a completat formularul de plată Western Union cu MTCN 5093184592.

Victima Dorothee Schmid a solicitat despăgubiri civile în cuantum de 300 de euro, precum şi tragerea la răspundere penală a persoanelor vinovate de comiterea faptei.

5. În cursul lunii septembrie 2005 un alt cetăţean britanic Richard Showan a fost indus în eroare de membrii grupului, în sensul că după ce l-a contactat pe site-ul Ebay.co.uk pe ofertant, a acceptat propunerea de a transfera suma de 1.250 lire sterline prin sistemul Western Union inculpatului C.N.I.cu titlu de preţ al unui număr de 15 telefoane mobile în posesia cărora nu a intrat niciodată pentru simplul motiv că vânzătorul nu a intenţionat să i le trimită.

Richard Showan a solicitat să fie despăgubit cu suma de 1.250 de lire sterline, reprezentând prejudiciul suferit de el (...)

31. În urma cererii de comisie rogatorie internaţională, înaintată de Biroul Teritorial Vâlcea autorităţilor judiciare competente din Ungaria, acestea au procedat la audierea părţii vătămate Horwath Gyula, împrejurare în care acesta a relatat amănunţit circumstanţe în care a fost indus în eroare prin intermediul sistemelor informatice, de o persoană din România care s-a prezentat sub identitatea lui C.N.I. şi care i-a pricinuit o pagubă de 2.275 de euro.

Astfel, în luna februarie 2008, pornind de la website-ul de licitaţii www.mascus.hu inculpatul C.A., prezentându-se sub identitatea lui C.H. din Franţa i-a oferit spre vânzare un tractor de tipul E64 Case 1056 XLA, la preţul de 4.500 euro şi pentru că victima a acceptat tranzacţia a primit prin e-mail de la vânzător un contract de vânzare-cumpărare redactat în două limbi, cu semnătura scanată şi în cuprinsul căruia figura la rubrica „vânzător" inculpatul C.I.C..

În data de 19.02.2008, partea vătămată a transferat prin sistemul Western Union, în România, inculpatului C.I.C. suma de 2.275 euro, reprezentând jumătate din valoarea tractorului, însă este evident că nu a primit bunul ce formase obiectul tranzacţiei, inculpatul completând în data de 19.02.2008 formularul de plată cu MTCN: 1679573998.

La fel fel ca în alte cazuri inculpatul şi-a ademenit victima prin faptul că i-a transmis detalii privitoare la regulile de încheiere a tranzacţiei, contractul de vânzare-cumpărare, parametrii tehnici şi fotografiile tractorului etc.

Partea vătămată Horwath Gyula se constituie parte civilă în procesul penal şi solicită să fie despăgubită cu suma de 2.275 euro.

32. În luna martie 2008 Ferdando Ferreira Da Silva din Portugalia a identificat pe un site de licitaţii on-line oferta privind vânzarea unui tractor cu încărcător, fabricat în anul 2007, marca Kubota B*24, aşa încât a luat legătura cu titularul ofertei, care l-a convins să încheie tranzacţia în termenii stipulaţi de el. Astfel pseudo-vânzătorul, mai precis inculpatul C.A. i-a transmis prin e-mail cumpărătorului un contract de vânzare-cumpărare pentru un tractor folosit, în cuprinsul căruia la rubrica "vânzător" figura inculpatul C.I.C., iar la rubrica "cumpărător" partea vătămată Ferdando Ferreira Da Silva, obiectul contractului constituindu-l tractorul menţionat anterior ce urma să fie

tranzacţionat la un preţ de 6.500 euro. În scopul ridicării banilor, C.I.C. a completat formularele de plată cu MTCN: 4748403872 şi 6788531326.

Trebuie făcută precizarea că înscrisul transmis victimei de inculpatul C.A. purta o semnătură scanată, în scopul de a induce victimei certitudinea că afacerea este una corectă.

Partea vătămată se constituie parte civilă în cauză cu suma 6.716.70 euro.

33. Ebay Inc. este o companie din Statele Unite ale Americii, ce administrează site-ul ebay.com specializat în licitaţii on-line şi vânzarea de bunuri, prin intermediul căruia persoane şi companii cumpără şi/sau vând bunuri şi servicii pe mapamond. Compania Paypal este deţinută de către compania eBay şi are în principal rolul de a monitoriza şi facilita efectuarea plăţii bunurilor şi serviciilor cumpărate prin site-ul ebay.com, aşa încât pe lângă datele personale şi alte date, utilizatorii au obligaţia de a indica un card bancar valid. Accesul la cont se face pe baza unui ID şi a unei parole sustrase adesea de piraţii internetului prin metoda phishing.

Datele şi informaţiile prelevate la efectuarea percheziţiilor informatice conţinute în rapoartele en-case au fost transmise celor două companii. Analizând datele puse la dispoziţie ce provin de la inculpatul C.A. şi coroborate cu baza de date a celor două companii, reprezentanţii acestora au identificat un număr de 14 seturi de informaţii personale ale unor cetăţeni străini compromise la compania eBay. Din cele 14 seturi de informaţii personale compromise, au fost identificate 14 conturi de acces la sistemul de banking on-line (Paypal) împreună cu parolele aferente.

Fiecare set de informaţii conţine următoarele date compromise, cont acces la platforma eBay, Inc., cont acces la sistemul de banking on-line paypal, nume titular, adresa, telefon, cod personal (SSN), numele de fata al mamei, numar card bancar, cod CVV2 card bancar, cod PIN card bancar, număr cont bancar, cod routing bancar.

În cauză au fost administrate proba cu acte, declaraţii de inculpaţi date fie în faza urmăririi penale (inculpaţii ,în faza cercetării judecătoreşti s-au prevalat de dreptul la tăcere, conform art. 70 C. pr. pen.), declaraţii de martori, expertiză contabilă efectuată în faza judecării cauzei şi au fost reevaluate şi valorificate probele administrate în faza urmăririi penale.

Ca urmare a formulării de plângeri penale de către părţi vătămate de naţionalitate străine privind înşelăciunea pe internet, (acestea fiind trecute în actul de sesizare al instanţei) FBI a sesizat autorităţile judiciare din România să se efectueze cercetări sub acest aspect.

Tribunalul constată că, impresionaţi de numărul mare al tinerilor, cunoştinţe sau prieteni, implicaţi în utilizarea calculatoarelor şi a programelor informatice, pentru a induce în eroare diverşi cetăţeni români sau străini, de asemenea, de uşurinţa cu care aceştia obţineau sume mari de bani şi nu în ultimul rând de lipsa de măsuri imediate împotriva unor astfel de acte materiale, fiecare din inculpaţii C.A. şi P.D.C., a hotărât să procedeze în acelaşi mod, ocupându-se doar de a-şi perfecţiona modul de operare şi a obţine din ce în ce mai mulţi bani, utilizând în acest sens şi abilităţile altor

participanţi. Primele noţiuni despre modul cum trebuiau să acţioneze le-au dobândit la sălile de internet din D. , fie observându-i pe cei cu astfel de preocupări fie întrebându-i, ulterior, după ce au realizat că actele materiale frauduloase aveau efecte mult mai mari în condiţiile în care acţionau împreună, ajutându-se unul pe celălalt, locuind împreună, folosind aceleaşi conturi, aceleaşi discuţii pe care le purtau cu părţile vătămate (copiate pe stick-uri şi transmise de la unul la celălalt) ori apelând la aceleaşi persoane ce le puteau pune la dispoziţie programe informatice mai performante, pagini false sau site-uri prin intermediul cărora definitivau procesul de inducere în eroare, evitând totodată să fie identificaţi.

În consecinţă, deşi doar o parte din ei erau cunoscători de limbă străină, au ajuns la performanţa de a reuşi să încheie tranzacţii de vânzare-cumpărare a unor bunuri, pe internet, cu persoane de diferite cetăţenii.

În acest sens, folosind fie calculatoarele sălilor de internet, fie pe cele proprii, au procedat iniţial la postarea, pe site-uri comerciale, eBay, Paypal, a unor anunţuri prin care comunicau că oferă spre vânzare telefoane mobile, utilaje agricole, ori alte bunuri (noi sau la mâna a doua), pe care în realitate nu le deţineau, la preţuri situate sub preţul pieţelor.

Această operaţiune nu necesita efectuarea vreunui demers special, întrucât lansarea ofertelor se realiza în principal pe site-uri ce nu solicitau plata anunţurilor, accesibile oricărei persoane, unde nu trebuiau să declare prea multe informaţii în afară de nume, adresă de email, număr de telefon şi textul ofertei, (eventual imaginea bunului). Operaţiuni mai complicate (cumpărare de domenii, creare de conturi de utilizator, etc) necesitau însă sit-urile oneroase, eBay, Paypal, platforma respectivă fiind accesată de regulă de inculpa C.A. ce a combinat în activitatea sa două moduri de operare.

O mare parte din datele de identificare pe care le introduceau în momentul înscrierii anunţurilor pe site-urile cu oferte gratuite erau false, fiind reale doar cele ce permiteau contactarea lor de persoanele interesate (număr de telefon, adresă de email). Pentru a realiza descrierea produselor, susnumiţii căutau pe GOOGLE anunţuri de vânzare a unor produse similare cărora le copiau conţinuturile (ce aveau de multe ori şi imagini) folosindu-le astfel în scop propriu.

În convorbirile cu potenţialii cumpărători se recomandau sub alte identităţi, folosind nume false, (în acest sens a se vedea interceptările convorbirilor telefonice autorizate de instanţă).

Amatorii unor astfel de produse îi contactau, fie la adresa de email ataşată anunţului, fie prin intermediul site-ului comercial ce permitea celor interesaţi solicitarea de informaţii suplimentare. Intrarea în corespondenţă electronică determina astfel declanşarea procesului de inducere în eroare, (situaţie premisă a infracţiunii de înşelăciune) constând în convingerea celor cu care conversau că tranzacţia este sigură şi că nu există nici un risc să vireze banii ce reprezentau contravaloarea lor. Pentru a crea aparenţa de seriozitate a tranzacţiei autorii procedau la a-i informa pe cumpărători că aceasta urma să fie garantată de o firmă de transport ori curierat, sau chiar de un alt site, cunoscute de

utilizatorii de internet (eBay,) după care, modificând informatic adresele de email ale acestor firme le trimiteau mesaje ce păreau că vin din partea reprezentanţilor lor.

Totodată, în funcţie de cât de „convingători" trebuiau să fie, achiziţionau în prealabil de la alte persoane ce se ocupau cu astfel de activităţi, drepturi de a utiliza site-uri false (prin introducerea unui nume de utilizator şi a unei parole) ce conţineau numere de colet pe care, de asemenea, le introduceau în corespondenţa dintre ei şi cumpărători cărora le comunicau că se pot folosi de aceste informaţii pentru a putea urmări traseul geografic al coletului lor, cei interesaţi putând să le acceseze şi astfel având convingerea că totul este sigur.

Totodată, cooperarea autorilor, denumiţi „lansatori" în cadrul procesului de fraudare, prin utilizarea în comun a aceloraşi conturi, aceloraşi texte de inducere în eroare, prin punerea la dispoziţie, de la unul la celălalt, a unor mijloace logistice ce permiteau optimizarea modurilor de operare, prin transportul săgeţilor comune, prin primirea banilor comuni de la coordonatori, etc, finalizate cu împărţirea proporţională a sumelor astfel obţinute ori cu plata serviciilor oferite, a determinat prejudicierea unor victimele comune care sunt, de altfel, părţile vătămate din cauză, cu excepţiile ce se vor specifica la fiecare inculpat.

Mecanismul de fraudare presupunea în continuare comunicarea către potenţialii cumpărători a posibilităţilor de a trimite banii, sens în care aveau nevoie de alţi participanţi care să le asigure nu numai anonimatul, pentru a nu fi identificaţi în cazul unei eventuale cercetări, dar şi timpul suficient pentru a pune în aplicare rezoluţia infracţională, scutindu-i astfel de a mai avea şi alte atribuţii. În acest sens stabileau de la început procentul din aceste sume la a căror obţinere aveau o contribuţie esenţială, pe care urmau să-l primească, respectiv 60-70%.

Din probele administrate în cauză rezultă că inculpatul C.A. a iniţiat şi constituit un grup infracţional în scopul săvârşirii de infracţiuni informatice asociate cu infracţiunea de înşelăciune în convenţii a peroanelor fizice cetăţeni străini, iar inculpaţii P.D.C., C.I.C., M.N.G. şi C.N.I., au aderat şi sprijinit acest grup prin săvârşirea unor asemenea fapte, fie în forma autoratului, fie sub forma instigării sau/şi complicităţii [202].

Este de remarcat numărul extrem de mare al subiecţilor pasivi care au fost afectaţi patrimonial într-un interval de timp relativ scurt, şi anume în perioada 2005-2008 de comiterea infracţiunii de fraudă informatică.

Condiţii de loc şi de timp. Textul incriminator nu prevede cerinţa unor condiţii de loc sau de timp pentru săvârşirea infracţiunii. Specific infracţiunii analizate este faptul că poate fi săvârşită şi de la distanţă.

4.3. Structura şi conţinutul juridic al infracţiunii

Structura şi conţinutul juridic al infracţiunii cuprinde: **situaţia premisă** şi **conţinutul constitutiv al infracţiunii.**

A. Situaţia premisă. Această infracţiune nu poate exista în absenţa unui sistem informatic în stare de funcţionare sau funcţionabil, asupra căruia făptuitorul să acţioneze fraudulos în modalităţile specificate pentru realizarea scopului prevăzut în textul de lege.

Dintr-o perspectivă funcţională, un sistem informatic este un mediu implementat tehnologic cu scopul de a înregistra, stoca şi transmite informaţii. Prin exercitarea acestor funcţii, un sistem informatic facilitează crearea şi schimbul de înţelesuri care servesc scopuri sociale precum exercitarea unor acţiuni, luarea unor decizii sau formularea sau justificarea unor idei [61, p.600].

Un sistem informatic cuprinde componente hardware, programe informatice sau altfel spus, componente software şi sistemul social care dirijează furnizarea organizată a informaţiei, formându-se astfel o reţea socio-tehnică.

B. Conţinutul constitutiv al infracţiunii. a) **Latura obiectivă.** Tehnologiile informaţiei şi comunicaţiei oferă numeroase modalităţi de comitere a fraudei informatice; de asemenea, facilitează comiterea acestor infracţiuni prin posibilitatea de a acţiona de la mare distanţă sau prin abuzul acordării de autorizări, prin costul redus al comiterii acestor infracţiuni şi prin riscul scăzut la care se expun făptuitorii [58, p.601].

Elementul material al infracţiunii se realizează printr-o acţiune alternativă de introducere, modificare sau ştergere de date informatice, de restricţionare a accesului la aceste date ori de împiedicare în orice fel a funcţionării unui sistem informatic.

Introducerea de date se referă la introducerea de date inexacte sau introducerea fără autorizaţie de date informatice, referindu-ne deci la date care nu existau înainte în sistemul respectiv Este indiferentă amploarea sau natura acestei operaţii [8, p. 47].

Modificarea de date cuprinde alterarea, variaţiile sau schimbările parţiale de date informatice, având drept consecinţă apariţia de noi date informatice diferite de cele iniţiale şi neconforme cu realitatea.

Ștergerea de date se referă la ştergerea datelor de pe suporturi fizice, care nu mai sunt disponibile pentru tranzacţii electronice licite. Nu prezintă importanţă dacă fenomenul se produce instantaneu sau după un anumit interval de timp, prin virusarea acestora.

Restricţionarea accesului cuprinde reţinerea, ascunderea, criptarea sau modificarea autorizărilor pentru utilizatorii legitimi. Nu este semnificativ faptul că restricţionarea accesului este definitivă sau este limitată la anumite perioade.

Împiedicarea funcţionării unui sistem informatic cuprinde atacuri fizice (spre exemplu, tăierea de cabluri, întreruperea alimentării cu energie electrică etc.) şi atacuri logice care împiedică pornirea normală a unui calculator (spre exemplu, prin modificarea setărilor iniţiale), atacuri de ”refuz al serviciului”, blocarea sistemului prin folosirea de contaminanţi informatici (viruşi, troieni), blocarea tastaturii, consumarea resurselor de memorie sau a spaţiului de stocare de pe discuri etc.

Cerinţa esenţială constă în aceea ca făptuitorul să fi acţionat fără drept în scopul de a obţine un beneficiu un beneficiu material pentru sine sau pentru altul şi să provoace o pagubă unei persoane.

Acţiunile menţionate trebuie să fie efectuate de făptuitor în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dar pentru existenţa infracţiunii nu este necesar să îl şi obţină [139, p.57].

Astfel, în actul de sesizare a instanţei s-a reţinut în esenţă faptul că inculpatul D.G.M, în luna octombrie 2004, a postat licitaţii fictive pe internet, cauzând un prejudiciu patrimonial (400 euro), părţii vătămate S.F., prin introducerea, modificarea sau ştergerea de date informatice într-un sistem informatic în scopul de a obţin un beneficiu material pentru sine, iar, în perioada septembrie 2005-martie 2006, la intervale diferite de timp, dar în baza aceleiaşi rezoluţii infracţionale, a postat licitaţii fictive pe internet prin diferite magazine virtuale (eBay, Amazonia, etc), cauzând prejudicii patrimoniale părţilor vătămate J.G. (210 USD), T.R. (500 AUD),K.B. (590 USD), J.P. (700 USD), S.S. (380 USD), M.J.J. (110 lire sterline), A.M.M. (1060 euro) şi S.M (1150 euro), precum şi altor cetăţeni străin, prin introducerea, modificarea sau ştergerea de date informatice într-un sistem informatic în scopul de a obţin un beneficiu material pentru sine, cât şi pentru inculpatul B.I., care l-a ajutat la săvârşirea acestor infracţiuni (în sensul că i-a furnizat cu ştiinţă datele lui de identitate, pentru ca licitaţiile să fie postate în numele său, şi a retras sumele de bani, transmise de cetăţenii străini prin Western Union şi Money Gram, bani pe care i folosit ambii învinuiţi).

De asemenea, în ceea ce-l priveşte pe inculpatul B.I., s-a reţinut prin actul de sesizare a instanţei, că acesta l-a ajutat pe inculpatul D.G.M. la săvârşirea infracţiunilor informatice (fraudă informatică), în sensul că i-a furnizat datele lui de identitate şi la intervale diferite de timp, dar în baza aceleiaşi rezoluţiuni infracţionale, a retras în numele său sume de bani prin intermediul unor companii specializate în tranzacţii internaţionale (Western Union şi Mony Gram), cunoscând că acei bani provin din licitaţii fictive, cauzând prejudicii patrimonia ei cetăţenilor străini, J.G. (210 USD), T.R. (500 AUD), K.B. (590 USD), J.P. (700 USD), S.S. (380 USD), M.J.J. (110 lire sterline), A.M.M. (1060 euro) şi S.M. (1150 euro), precum şi altor cetăţeni, obţinând beneficii materiale , atât pentru el, cât şi pentru inculpatul D.G.M. (...).

Pentru realizarea scopului propus, şi anume postarea licitaţiilor fictive pe internet şi înşelarea cetăţenilor străini, învinuitul D.G.M. a folosi una din următoarele metode („Phishing" sau „Escrow”).

Această metodă „phishing" în special este utilizată de inculpaţi pentru comiterea de infracţiuni informatice, prin intermediul platformelor comerciale on line, (cum este, de exemplu, *platforma de eBay*).

Acestea sunt portaluri de comerţ on-line, fară frontieră,unde se poate vinde sau cumpăra orice, şi oferă clienţilor săi şansa de a afişa produse spre vânzare pe site-urile sale prin licitaţie sau chiar vânzare directă şi, de asemenea, oferă posibilitatea să participe la asemenea licitaţii, sau de a accede la produsele afişate spre vânzare, pe site-uri.

Pentru a vinde sau cumpăra prin intermediul acestor platforme trebuie să fiii utilizator înregistrat, acesta fiind un proces structurat pe trei etape: întâi sej completează informaţiile de către utilizator şi se dă apoi acordul, această cerinţă, servind la verificarea identităţii utilizatorului pentru ca cei cu care vine în contact să aibă încredere în cooperarea, cu utilizatorii platformei comerciale; apoi se creează un user şi o parolă, care reprezintă identitatea utilizatorului în cadrul platformei comerciale; la final, după ce se completează suportul cu informaţii despre utilizator, platforma comercială trimite un e-mail, cu confirmarea acestora pentru a se asigura că s-a introdus corect adresa utilizatorului.

Persoana care intenţionează să vândă un produs, postează o ofertă de vânzare cu un preţ minim de la care porneşte licitaţie on-line. Produsul este afişat pe site-ul platformei comerciale pentru o perioadă determinată. în această perioadă orice, utilizator poate accesa produsul pe Internet.

Persoana interesată de un anumit produs poate utiliza browser-ul de căutare pe categorii de produse, iar în ofertă găseşte informaţiile postate de vânzători, referitoare la particularităţile produsului, fotografii ale acestuia, iar pentru neclarităţi poate fi utilizată opţiunea „Ask Seller a Question"(pune vânzătorilor o întrebare). Totodată în pagina cu oferta poate fi observat feedback-ul vânzătorului, (care este un punctaj acordat pe baza tranzacţiilor finalizate anterior, pozitiv de către vânzător pe site-ul comercial).

După o tranzacţie încheiată cu succes, fiecare parte îi îmbunătăţeşte feedback-ul celuilalt.

Dacă se intenţionează vânzarea unui produs se accesează link-ul corespunzător din bara de meniu, după care se completează un formular onrline cu preţul minim, perioada de licitaţie, datele de contact caracteristicile produsului, fotografi, etc. La finalizarea licitaţiei se contactează câştigătorul (cel care a oferit preţul cel mai bun) prin e-mail, se stabilesc condiţiile de plată, şi trimitere a produsului (detaliile taxelor aferente şi ale comisioanelor) după care se trimite produsul cumpărătorului la adresa specificată de acesta. În scopul postării de licitaţii fictive pe platformele comerciale, inculpaţii îşi creează baze de date care conţin adrese valide de e-mail (usere şi parole) ale unor utilizatori ai platformei comerciale. în acest sens, se falsifică pagina de înregistrare „sign-in" şi site-ul de licitaţii, prin modificarea codului sursă, în sensul că se înlocuieşte adresa de contact a

administratorului platformei comerciale, cu o altă adresă de e mail, controlată de inculpaţi. Pagina falsă de înregistrare se transmite către adresele valide de email din baza de date, creată anterior (spam).

O parte din utilizatori care primesc mesajul nesolicitat de înregistrare (sau reconfirmarea datelor de înregistrare), sunt induşi în eroare de mesajul aparent autentic şi îşi introduc datele de înregistrare pe site-ul comercial.

Datele de înregistrare ale utilizatorului legitim introduse la rubrica „user ID" şi „password" (parola) sunt apoi direcţionale fară ştirea utilizatorului către adresa de e-mail, specificată în codul sursă, odată cu efectuarea clik-ului pe „sign-in".

După sustragerea acestor conturi inculpaţii schimbă parolele userelor şi mail-urilor, pentru ca titulari legitimi să nu mai poată folosi aceste date şi apoi postează licitaţi fictive, în sensul că folosesc usere care nu le aparţin (deci nu poate fi verificată identitatea lor) şi oferă spre vânzare bunuri care în realitate nu le deţin, ştiind că în cazul în care un potenţial client trimite banii pentru produsul oferit, acesta nu va primi niciodată bunul.

Ulterior, inculpaţi iniţiază o corespondenţă prin e-mail, cu persoana interesată şi în cazul în care acesta este de acord cu încheierea tranzacţiei încurajează potenţialul client, să trimită contravaloarea produselor obţinute (la preţuri avantajoase), sau a unui avans printr-un sistem rapid de transmitere a banilor (Western Union sau Money Gram). Astfel, inculpaţii solicită apoi o copie scanată a chitanţei din care rezultă că au fost trimişi banii, iar când se primeşte pe e- mail copia scanată a chitanţei de transmitere a banilor, aceştia se prezintă la instituţiile bancare şi ridică sume de bani, fără a transmite vreodată bunul pentru care i s-au trimis banii.

Pentru a ridica sume de bani astfel trimise, destinatarul trebuie să cunoască; doar numele persoanei care a făcut depunerea şi M.T.C.N. - ul Money Transfer Control Number-ul numărul de control al transferului de bani, aceste date fiind suficiente pentru a se ridica sumele de bani trimise.

Prin utilizarea metodei „Escrow", inculpaţii postează licitaţii fictive pe diferite site-uri comerciale în modurile descrise mai sus, iar atunci când potenţiala victimă este interesată să cumpere produsul inculpaţii propun potenţialului client intermedierea tranzacţiei printr-un site escrow, falsificat şi controlat tot de ei. Această metodă este folosită în cazul clienţilor suspicioşi sau reticenţi, care nu doresc să trimită banii printr-un sistem rapid de transfer al sumelor de bani, şi care folosesc în mod regulat site-uri de tip escrow , cunoscute pentru garantarea tranzacţiilor on-line.

După ce clientul (victimă) s-a înregistrat pe site-ul escrow propus de inculpaţi, acesta primeşte un mesaj care apare a fi de la firma ce administrează site-ul escrow şi care are drept scop crearea convingerii victimei că transmiterea produsului licitat a fost confirmată, însă în realitate mesajul este trimis tot de inculpaţii care au falsificat site-ul escrow. Totodată, prin acelaşi mesaj se solicită şi transmiterea sumelor de bani, deşi produsul licitat nu va fi trimis niciodată de inculpaţi.

Astfel, prin una din aceste metode, învinuitul D.G.M. postat licitaţii fictive pe internet, atât în numele său, cât şi în numele învinuitului B.I., cu ajutorul sistemelor informatice proprii, cât şi cu sisteme informatice de la sala de Net IQ, înşelând diferiţi cetăţeni străini, cu diferite sume de bani, pe care cei doi învinuiţi i-au împărţit (...) [200].

În acest caz avem în special de-a face cu o acţiune de introducere şi de modificare de date informatice, fie prin metoda phishing-ului, care a fost deja detaliată în capitolul II al tezei, fie prin cea numită escrow. După ce victima s-a înregistrat pe site-ul propus de făptuitor, aceasta recepţionează un mesaj, ce aparent provine de la societatea comercială, care administrează site-ul şi care are drept obiectiv întărirea convingerii victimei, că expedierea produsului licitat a fost confirmată, în realitate însă, mesajul fiind expediat tot de către făptuitor prin falsificarea siteu-lui escrow. Totodată, prin intermediul aceluiaşi mesaj se solicită şi transmiterea sumelor de bani, aceasta în condiţiile în care produsul licitat nu va fi transmis niciodată.

În context pot fi evidențiate următoarele modalități faptice de comitere a infracțiunii de fraudă informatică:

- **phising-ul**, este recunoscut ca o formă modernă de inginerie financiară, ce constă în obţinerea frauduloasă a informaţiilor confidenţiale (numele de utilizator, parola şi detalii legate de cartea de credit) prin imitarea, aproape de perfecţiune, a paginii web a unei companii credibile cu utilizarea unei forme de comunicare electronică. Băncile care efectuează tranzacţii *online* sunt ţintele predilecte, phishingul realizându-se prin intermediul e-mail-ului sau al mesageriei instant şi, de obicei, redirecţionează utilizatorii spre o pagină identică cu cea a companiei credibile, unde utilizatorului i se cere să-şi introducă informaţiile personale;

- **frauda cu valorile mobiliare**, schemele de fraudare presupun obţinerea de beneficii din contul vânzării valorilor mobiliare costul real al cărora este majorat în mod fictiv. Răspândind date eronate despre emiţător şi condiţia economică a acestuia, făptuitorul în mod fraudulos influenţează creşterea ofertei şi a preţurilor, după care încheie tranzacţii de vânzare a acţiunilor la un preţ majorat. Ulterior, preţurile pe piaţă se restabilesc la nivelul real, iar investitorii de rând suportă daune materiale [209].

- **postarea licitaţiilor fictive sau vânzarea „produselor momeală”**, rezidă în ademenirea potenţialilor clienţi prin postarea de publicităţi fictive, oferindu-se spre vânzare produse costisitoare la un preţuri avantajoase. În speţă, produsele fie că nu există în realitate, fie că sunt ulterior schimbate cu produse aparent similare, dar cu calităţi ned inferioare. Caracteristic pentru această formă de fraudare este faptul că în nici un moment autorul nu are de gând să vândă „produsul momeală” [40, p.225];

- **escrocheria cu ajutorul telefonului mobil,** se practică în diferite modalităţi, precum ar fi, spre exemplu, expunerea spre comercializare a unor programe fictive, ce ar face posibilă efectuarea fără plată a convorbirilor telefonice. De regulă, schema de fraudare este deosebit de ingenioasă presupunând lansarea pe pagina *web* a unor oferte atractive (este dată publicităţii lista operatorilor cu

care asemenea programe pot fi puse în funcţiune; sunt afişate modelele telefoanelor mobile utilizarea cărora permite funcţionarea programei respective etc.). O altă metodă de săvârşire a escrocheriilor informaţionale cu utilizarea telefoanelor mobile constă în scanarea cod-pinurilor de pe cartelele telefonice, urmată de folosirea frauduloasă a timpul de convorbire, cu expunerea ulterioară a cartelelor în vânzare;

- **oferte fictive de afaceri**, de regulă, pe pagina *web* este descrisă rentabilitatea afacerii, făcând-o să devină, astfel, atractivă pentru victimă. Participarea propriu-zisă la afacere sau oferirea unor date suplimentare pentru realizarea ei, este condiţionată de transferarea pe un cont indicat de către făptuitor a unor mijloace băneşti, care, de regulă poartă un caracter simbolic, fiind nesemnificative (de exemplu, victimei i se propune achitarea unei sume de bani pentru obţinerea unor mostre de contracte pe care urmează să le încheie cu viitori clienţi). După operarea transferului de bani victima nu mai poate accesa pagina *web*, aceasta fiind distrusă de către făptuitor.

Urmarea imediată în cazul reglementării din Codul penal român constă în producerea unui rezultat, reprezentat de un prejudiciu material pentru partea vătămată, indiferent de valoarea acestu prejudiciu. Este suficient să se dovedească faptul că patrimoniul persoanei vătămate a suferit o micşorare ca urmare a faptei comise de făptuitor. aceasta în timp ce Codul penal al Republicii Moldova cere ca ca în momentul săvârşirii infracţiunii valoarei pagubei să depăşească a 20 de salarii medii lunare pe economie prognozate, stabilite prin Hotărârea de Guvern în vigoare la momentul săvârşirii faptei.

În ceea ce priveşte **legătura de cauzalitate**, pentru realizarea laturii obiective a infracţiunii de fraudă informatică este necesar să se constate că există un raport de cauzalitate între acţiunea incriminată şi urmarea imediată (prejudicial material). Dacă situaţia păgubitoare este urmarea altei cause (spre exemplu, căderi temporare de tensiune), şi nu a activităţii descries de legiuitorul penal, ea nu constituie urmarea imediată a acestei acţiuni, lipsind legătura de cauzalitate [61, p.603].

Astfel, în fapt, s-a reţinut că la data de 24.04.2008 BCCO Craiova s-a sesizat din oficiu în legătură cu faptul că pe raza Municipiului Craiova, s-a constituit un grup infracţional organizat compus din mai multe persoane dintre care au fost identificaţi T.M.R, P.D.M , D.R.M, P.S.D şi V.R.G, care au comis înşelăciuni în dauna unor cetăţeni străini prin intermediul internetului, astfel:

1 . La data de 19.02.2008, partea civilă C.M din S.U.A. a sesizat faptul că o persoană cu numele de T.M.R din Craiova, i-a oferit spre vânzare un laptop contra sumei de 1000 de dolari solicitând transmiterea preţului bunului pe care urma să-l vândă printr-o metodă de plată nesigură.

2. La data de 16.06.2007 partea civilă Sue Wade din S.U.A. a comandat un laptop APPLE utilizând serviciile e.-Bay şi a găsit pe acest site o listă cu computere.

Utilizând zona “Buy now” partea civilă Sue Wade a fost direcţionată către o adresă de e-mail a unei persoane cu numele P.S.D (spavel@gmailcom). şi şi-a manifestat dorinţa de a cumpăra

computerul respectiv achitând în schimb suma de1000 de dolari, bani pe care vânzătorul i-a solicitat să îi transmită prin serviciul Western Union .

În baza înţelegerii intervenite partea civilă a trimis suma solicitată însă nu a primit bunul pentru care a achitat suma de 1000 de dolari .

3. La data de 24.11.2008 partea civilă J.S din S.U.A. a sesizat faptul că, în ziua de 10.10. 2007 a găsit pe e-Bay o listă care făcea reclamă la laptop-uri Dell XPS şi că, vânzătorul a spus că lucrează la o companie de computere şi poate să achiziţioneze astfel de bunuri cu reducere însă cineva îi furase ID -ul e-Bay şi nu putea realiza o licitaţie cu opţiunea buy it now.

Suma de 900 de dolari solicitată de vânzătorul D.R.M a fost trimisă prin serviciul Western Union, însă partea civilă nu a primit bunul pe care l-a achitat.

4. La data de 17.07.2008 partea civilă C.M din S.U.A. a sesizat faptul că o persoană care avea adresa de e.mail thxbay @ gmail.com. a oferit spre vânzare un computer Dell XPS M 2010 pe site-ul e-Bay la preţul de 1000 de dolari şi că a dat asigurări că tranzacţia este sigură. Deşi partea vătămată a achitat suma solicitată prin Western Union nu a primit bunul al cărui preţ l-a achitat .

5. La data de 18.07.2006 partea civilă M.C.S din S.U.A a sesizat faptul că a intenţionat să cumpere un laptop şi că a fost înşelată cu suma de 1000 de dolari cu ocazia unei licitaţii organizate pe internet.

6. Partea civilă R.S din S.UA. a sesizat faptul că la data de 01.07.2006 a fost înşelată cu ocazia unei licitaţii care a avut loc pe internet cu suma de 1193 dolari .

Potrivit rechizitoriului întocmit începând cu anul 2005 inculpatul P.D.F a organizat în mod fraudulos licitaţii prin intermediul internet-ului oferind spre vânzare diverse bunuri pe care nu le deţinea şi solicitând trimiterea banilor prin serviciul Western Union. A fost sprijinit în activitatea desfăşurată de către inculpaţi P.S.D, T.M.R, V.R.G, Ş.M.C, D.M.A şi G.C.M, care au ridicat banii trimişi de persoanele prejudiciate prin intermediul serviciului Western Union .

În expozitivul rechizitoriului s-a arătat totodată că din declaraţiile date de inculpaţii P.D.F şi P.S.D rezultă că, fiecare dintre inculpaţii care ridicau bani, primeau un procent de 20 la sută din suma ridicată şi că, în acest mod P.D.F a obţinut aproximativ 100.000 de dolari, iar din declaraţiile inculpaţilor D.MA, Ş.M.C , T.M.R, V.R.G, reiese fie că nu au fost sinceri cu ocazia audierii (D.M.A) fie că au recunoscut că inculpatul P.D.F le-a solicitat să ridice nişte bani pe care urma să îi primească din străinătate, însă nu au cunoscut iniţial, proveniența ilicită a acestora (T.M).

În expozitivul rechizitoriului s-a arătat totodată că, la data de 25.08.2009, au fost efectuate percheziţii domiciliare la inculpaţii P.D.F zis "Pono" şi P.S.D precum şi la învinuiţii D.R.M zis "Gexy", T.M.R , V.R.G, Ş.M.C, V.E.M, D.M.A, G.C.M şi M.C.D Zis "Bădărică", conform autorizaţiilor emise de Tribunalul Dolj.

În urma efectuării percheziţiilor domiciliare au fost ridicate de la domiciliile inculpaţilor şi învinuiţilor sisteme informatice şi mijloace de stocarea a datelor pentru care DIICOT Serviciul Teritorial Craiova a solicitat şi obţinut de la Tribunalul Dolj autorizaţia de percheziţie informatică cu nr. 150/02.09.2009.

Conform materialului probator ataşat în vol.4 (proces - verbal 14.02.2009), în urma percheziţiei informatice efectuate la mediile de stocare a datelor informatice ridicate de la inculpatul P.D.F zis "Pono", în hard disk-ul marca MAXTOR a fost identificată corespondenţa electronică în limba engleză purtată prin intermediul unor adrese de e-mail ce conţin în denumire numele "D" respectiv "G", corespondenţa referitoare la vânzarea unor produse prin intermediul site-ului e-bay, dar şi a altor asemenea pagini web precum şi anunţuri postate în acelaşi sens.

De asemenea, cu ocazia percheziţionării DVD-ului marca COPIME ridicat tot de la inculpatul P.D.F zis "Pono", în folder-ul denumit "1111" ce conţine un număr de 24 de foldere şi 354 de fişiere, au fost descoperite fişiere tip imagine reprezentând laptop-uri, fişiere reprezentând pagini pentru anunţuri de vânzare laptop-uri, în limba engleză, însoţite de datele şi performanţele tehnice în varianta cunoscută sub denumirea "Buy it now"(cumpără acum), adresa de e-mail pentru contactarea vânzătorului fiind thxebav@gmail.com.

Au fost descoperite şi fişiere conţinând instrucţiuni referitoarea la schimbarea IP-ului, fişiere conţinând documente de vânzare -cumpărare laptop-uri ce par a fi emise de către Centrul de Securitate al site-ului de Comerţ Electronic de tip e-bay, fişiere reprezentând sume de bani în lei, euro şi dolari ale inculpatului P.D.F zis "Pono", şi un alt tânăr, fişiere cu texte în limba engleză prin care se oferă explicaţii privitoare la diverse impedimente întâmpinate cu ocazia tranzacţiilor prin e-bay ori asigurări cu privire la starea produsului, un folder conţinând 27 imagini reprezentând diverse produse electronice (maşini de cusut, sisteme audio, aparate foto, etc), un folder cu 14 imagini reprezentând laptop-uri de diverse mărci, un fişier document conţinând date de identificare şi preţuri ale unor produse electronice, un fişier document conţinând date cu privire la sume expediate prin Western Union, două fişiere conţinând texte în limba engleză referitoare la tranzacţii on-line având denumiri sugestive"vrăjeala să-ţi dea adresa şi să vadă şi preţu care a bidat "şi" şi după ce scoţi MTCN urmează poza", două fişiere document conţinând texte în limba engleză referitoare la tranzacţii on-line în regim de second chance mai precis se explica faptul că datorită unor probleme personale ale cumpărătorului iniţial, acesta nu poate plăti, motiv pentru care îi oferă interlocutorului şansa de a cumpăra respectivul produs la un preţ mai ieftin.

Totodată, au fost descoperite 10 fişiere conţinând documente în care sunt descrise diverse produse precum şi 16 fişiere reprezentând documente de vânzare - cumpărare, laptop-uri, telefoane mobile, prin intermediul e-bay vânzător:" pavelsoare(a).vahoo.com, metoda "buy it now" însoţite de alte 35 fişiere imagine reprezentând produse oferite la vânzare.

Conform materialului probator ataşat în vol.5 cu rezultatul percheziţiei informatice efectuate la sistemele informatice ridicate tot de la inculpatul P.D.F zis "Pono", în hard disk-ul marca MAXTOR a fost identificată corespondenţa electronică în limba engleză cu diverşi cetăţeni din străinătate, referitoare la vânzarea prin intermediul site-ului e-bay a unor produse electronice. în această corespondenţă, sunt identificate ca destinatare a sumelor de bani reprezentând preţul bunurilor, D.M.A şi N.G.C.. De asemenea a fost identificat postul telefonic cu nr. 0723 383 565 asociat numelui inculpatului P.D.F zis "Pono", formular în format electronic prin care echipa SQUARE TRADE şi SEIF HARBOR asigura cumpărătorul M.A din SUA, de siguranţa tranzacţiei.

Pe parcursul cercetării judecătoreşti la termenul din data de 11.01.2010 au fost audiaţi inculpaţii P.D.F, P.S, D.M.A, G.C.M, T.M, Ş.M.C şi V.R.

Inculpatul P.D.F a declarat că a organizat licitaţii pe internet începând cu anul 2005 introducând datele personale pe pagina de vânzări a e-Bay şi a dat anunţuri oferind spre vânzare diverse bunuri pe care nu le avea. Potrivit declaraţiilor sale, la început ceilalţi inculpaţi nu ştiau de unde provin banii, dar apoi şi-au dat seama şi au primit un comision de 20 la sută pentru fiecare dintre operaţiunile de ridicare efectuate . În legătură cu inculpata G a precizat că a ridicat bani o singură dată şi că nu ştie ce este cu celelalte două ridicări .

Inculpatul P.S.D. a recunoscut că a ridicat bani pentru inculpatul P aproximativ un an şi jumătate şi că după a treia ridicare şi-a dat seama de unde provin banii .A relatat totodată că, a primit un procent de 20 la sută din sumele ridicate.

Inculpata D.M a recunoscut că a ridicat bani de 4,5 ori arătând însă că nu a ştiut de unde provin şi că nu a primit comision pentru sumele ridicate.

Inculpata G.C. a recunoscut că a ridicat bani de două ori, la interval de două zile, la cererea prietenului său T însă nu a primit în schimb nicio sumă de bani nici de la P şi nici de la T .Potrivit declaraţiei date ,două dintre formularele Western Union expediate pe numele său nu sunt semnate de ea.

Inculpatul T.M a recunoscut că a ridicat bani de 2, 3 ori şi că şi-a dat seama de unde provin, iar Ponovescu nu i-a ascuns acest lucru.

Inculpatul Ş.M a relatat că a ridicat bani de 5,6 ori la solicitarea lui Ponovescu şi că a primit în schimb un comision de 20 la sută. Potrivit declaraţiei date, nu ştia că banii provin din comiterea unor înşelăciuni întrucât P i-a spus că sunt trimişi de prieteni din străinătate şi nu îi poate ridica pentru că are probleme cu cartea de identitate.

Inculpatul V a declarat că a ridicat de 2,3 ori bani la rugămintea lui Ponovescu şi că şi-a dat seama că aceştia provin din fraudă. Nu ştia însă că şi ceilalţi coinculpaţi ridicau bani pentru P.

Se reţine că inculpatul P.D.F a intrat neautorizat pe site-ul e-Bay, a plantat propria listă cu produse (laptop - uri) şi a convenit cu părţile civile S.W, J.S, C.M, C.S.M şi R.S, să le vândă astfel de bunuri deşi cunoştea faptul că nu le deţine cu nici un titlu (proprietar, posesor , detentor).

Conform înţelegerii dintre inculpat şi părţile civile contravaloarea bunurilor a fost achitată de acestea prin intermediul serviciului Western Union şi a fost ridicată de la acest serviciu de transfer rapid de fonduri de către inculpatul P.S.D.

În raport de cele expuse mai sus, instanţa constată că faptele comise de inculpaţii P.D.F, P.S.D şi T.R.M realizează conţinutul constitutiv al următoarelor infracţiuni :

Faptele inculpatului P.D.F constând în aceea că în mod repetat şi în baza unei rezoluţii infracţionale unice a oferit spre vânzare părţilor civile S.W, J.S, C.M, C.S.M şi R.S, bunuri pe care nu le deţinea cu scopul de a obţine diverse sume de bani realizează conţinutul constitutiv al infracţiunii prev. de art. 215 al. 1, 2 şi 3 din C.pen. cu aplic.art.41 al. 2 din C.pen.

Faptele inculpatului P.D.F constând în aceea că în mod repetat şi în baza unei rezoluţii infracţionale unice a pătruns în mod neautorizat pe site-ul e-Bay introducând propria listă de bunuri oferită la vânzare în scopul obţinerii unor beneficii materiale întruneşte elementele constitutive ale infracţiunii prev. de art. 49 din Legea 161/2003 cu aplicarea art. 41 al. 2 C.pen.

Faptele inculpatului P.S.D constând în aceea că în mod repetat şi în baza unei rezoluţii infracţionale unice a ridicat de la Servicul Western Union, sumele de 1050 dolari, 1930 dolari, 1068 dolari respectiv 1193 dolari, trimise de părţile civile S.W, J.S, C.M, C.S.M şi R.S, realizează elementele constitutive ale infracţiunii prev. de art. 26 C.pen. rap. la art. 215 al.1,2 şi 3 din C.pen cu aplic. art. 41 al.2 din C.pen.

Faptele inculpatului P.S.D constând în aceea că i-a pus la dispoziţie datele de identitate inculpatului P.D.F, pentru a fi introduse pe site-ul e - Bay în scopul obţinerii unor beneficii materiale realizează conţinutul constitutiv al infracţiunii prev. de art. 26 C.pen. rap. la art. 49 din Legea 161/2003 cu aplic. art. 41 al.2 din C.pen.[201]

Putem remarca aici raportul de cauzalitate între acţiunea incriminată şi prejudiciul material, acest prejudiciu fiind suferit drept consecinţă a licitaţiilor fictive care au fost organizate de către făptuitor.

b) **Latura subiectivă**. Vinovăţia la aceasta infracţiune se prezintă numai cu intenţie directă calificată prin scop. Astfel, acţiunea făptuitorului se realizează în scopul de a obţine un beneficiu material pentru sine sau pentru altul. Nu este necesară realizarea efectivă a acestui beneficiu ci numai urmărirea realizării acestuia [189, p.298].

Mobilul şi scopul. Mobilul nu prezintă relevanţă pentru existenţa infracţiunii, însă va putea fi luat în considerare la individualizarea pedepsei. Scopul urmărit de făptuitor este acela de a obţine un beneficiu material pentru sine sau pentru altul.

4.4. Forme agravante ale infracţiunii

La art. 260^6 C.pen. al R. Moldova este dozată răspunderea penală pentru frauda informatică săvârşită în prezenţa a două circumstanţe agravante, frauda informatică săvârşită de *un grup criminal organizat sau de o organizaţie criminală* şi care a *cauzat daune în proporţii deosebit de mari*.

Cu referinţă la prima circumstanţă agravantă, prin raportare la norma definitorie prevăzută la art.46 C.pen. al R. Moldova, se poate deduce că săvârşirea acţiunilor prevăzute la art.260^6 C.pen. de un grup criminal organizat are loc în cazul în care acestea sunt comise de o reuniune stabilă de persoane, care s-au organizat în prealabil pentru a comite una sau mai multe infracţiuni.

Săvârşirea faptei de către un grup criminal organizat urmează a fi delimitată de frauda informatică comisă de două sau mai multe persoane. La delimitarea acestor două forme de activitate infracţională se va ţine cont, în mod prioritar, de legătura funcţională ce există între participanţii la infracţiune. Astfel, grupul criminal se caracterizează prin asemenea trăsături cum ar fi: stabilitatea, prezenţa în componenţa lui a unui organizator, existenţa unui plan dinainte elaborat al activităţii infracţionale comune, repartizarea obligatorie a rolurilor între membrii grupului criminal organizat, mai ales la etapa pregătirii infracţiunii.

Fiecare persoană care intră în grupul criminal organizat, nu este doar un simplu participant la acel grup, ci membru al grupului, indiferent de locul şi funcţiile de executare, ce ia-u fost încredinţate lui în cadrul desfăşurării planurilor de activitate infracţională.

În practica judiciară a R. Moldova prezintă interes delimitarea dintre infracţiunea comisă de două sau mai multe persoane, sub forma coautoratului simplu, de infracţiunea săvârşită de către un grup criminal organizat.

În acest sens, CSJ a statuat: „Săvîrşirea sustragerii de un grup criminal organizat are loc în cazul în care această faptă e comisă de o reuniune stabilă de persoane care s-au organizat în prealabil pentru a comite una sau mai multe infracţiuni. Spre deosebite de două sau mai multe persoane, care s-au înţeles în prealabil despre săvîrşirea sustragerii, grupul criminal organizat se caracterizează, în special, prin stabilitate, prin prezenţa în componenţa lui a unui organizator şi printr-un plan dinainte elaborat al activităţii infracţionale comune, precum şi prin repartizarea obligatorie a rolurilor între membrii grupului criminal organizat, în timpul pregătirii sustragerii” [85, p. 5].

Luându-se drept punct de reper prevederile art.47 C.pen., săvârşirea faptei de către o organizaţie criminală are loc în cazul în care aceasta este comisă de o reuniune de grupuri criminale organizate, formând o comunitate stabilă, a cărei activitate se întemeiază pe diviziune, între membrii organizaţiei şi structurile ei, a funcţiilor de administrare, asigurare şi executare a intenţiilor criminale ale organizaţiei în scopul de a influenţa activitatea economică şi de altă natură a persoanelor fizice şi

juridice sau de a o controla, în alte forme, în vederea obţinerii de avantaje şi realizării de interese economice, financiare sau politice.

Reieşind din această noţiune legală în doctrina penală de specialitate moldovenească sunt identificate următoarele trăsături definitorii ale organizaţiei criminale:

1) organizaţia criminală reprezintă o reuniune de grupuri criminale;

2) consolidarea grupurilor criminale într-o comunitate stabilă;

3) divizarea activităţii organizaţiei între membrii organizaţiei ş structurile ei;

4) scopul organizaţiei criminale este de a influenţa activitatea economică şi de altă natură a persoanelor fizice ş juridice sau de a o controla, în alte forme, în vederea obţinerii de avantaje şi a realizării de interese economice, financiare sau politice.

Infracţiunea se consideră săvârşită de o organizaţie criminală dacă a fost comisă de un membru al acesteia în interesul ei sau de o persoană care nu este membru al organizaţiei respective, la însărcinarea acesteia.

Organizatorul şi conducătorul organizaţiei criminale poartă răspundere pentru toate infracţiunile săvârşite de această organizaţie, indiferent de faptul dacă au luat sau nu parte la săvârşirea acestor infracţiuni.

În cazurile în care organizaţia criminală şi-a început activitatea infracţională, iar membrii acesteia au săvârşit careva activităţi legate de frauda informatică, atunci acţiunile organizatorului sau conducătorului organizaţiei criminale trebuie calificate prin concurs, conform art.284 şi art.260^6 C.pen.

În situaţia săvârşirii de către membrii organizaţiei criminale a infracţiunilor care nu au fost prevăzute în planurile activităţii organizaţiei criminale răspunderea pentru aceste infracţiuni o vor purta numai cei care au comis nemijlocit aceste infracţiuni.

Infracţiunea de fraudă informatică, dată fiind mecanismul propriu de comitere cei este specific şi veniturile colosale pe care le obţin făptuitorii implicaţi în asemenea activităţi frauduloase de obţinere a profiturilor este susceptibilă să fie comisă la nivel transnaţional, putând îmbrăca fomra unei infracţiuni cu caracter transnaţional.

În general, criminalitatea organizată transnaţională reprezintă o totalitate de infracţiuni, săvârşite de grupări criminale organizate la diferite nivele, formate, de regulă, din cetăţeni a unor state diferite, infracţiuni ce sunt comise prin folosirea pe scară largă a coordonării activităţii criminale la nivel transnaţional şi care constau în răspândirea pe teritoriul a două sau a mai multor state a activităţii de pregătire, organizare, săvârşire şi de survenire a consecinţelor criminale, în scopul obţinerii unor profituri economice sau creării unor condiţii propice de majorare a acestora, prin recurgerea la utilizarea violenţei sau a legăturilor corupţionale, inclusiv la nivel politic.

Din această noţiune rezultă următoarele trăsături definitorii ale criminalităţii organizate transnaţionale: 1) existenţa unor grupări organizate criminale de diferite nivele, formate, de regulă, din

cetăţeni a unor state diferite sau persoane fără cetăţenie; 2) presupune folosirea pe scară largă a coordonării activităţii criminale la nivel transnaţional; 3) infracţiunile sunt săvârşite prin răspândirea pe teritoriul a două sau a mai multor state a activităţii de pregătire, organizare, săvârşire şi de survenire a consecinţelor criminale; 4) existenţa scopului de obţinere a unor profituri economice sau creării unor condiţii propice de majorare a acestora; 5) recurgerea la utilizarea violenţei sau a legăturilor corupţionale, inclusiv la nivel politic, pentru realizarea scopurilor sale [173, p. 47].

Cea de a două agravanată este prevăzută de art. 260^6 lit.b) şi constă în cauzarea unor daune în proporţii deosbeit de mari.

În conformitate cu art. 126 alin. (1^1) C.pen. se consideră proporţii deosebit de mari valoarea bunurilor sustrase, dobîndite, primite, fabricate, distruse, utilizate, transportate, păstrate, comercializate, trecute peste frontiera vamală, valoarea pagubei pricinuite de o persoană sau de un grup de persoane, care depăşeşte 40 de salarii medii lunare pe economie prognozate, stabilite prin hotărîrea de Guvern în vigoare la momentul săvîrşirii faptei.

Infracţiunea de fraudă informatică poate îmbrăca forma unei conduite infracţionale ce poate fi comisă în mod continuu sau prelungit.

În Codul penal în vigoare al României infracţiunea continuată este definită la art. 41alin. (2) C.pen. român, care prevede că „Infracţiunea este continuată când o persoană săvârşeşte la diferite intervale de timp, dar în realizarea aceleiaşi rezoluţii, acţiuni sau inacţiuni care prezintă, fiecare în parte, conţinutul aceleiaşi infracţiuni”.

Codul penal în vigoare al Republicii Moldova din 2002 defineşte infracţiunea continuată la art.30 alin. (1), sub denumirea de infracţiune prelungită. Potrivit textului de lege: „Infracţiunea prelungită se consideră fapta săvârşită cu intenţie unică, caracterizată prin două sau mai multe acţiuni infracţionale identice, comise cu un singur scop, alcătuind în ansamblu o infracţiune”.

Trăsătura definitorie care particularizează infracţiunea prelungită (continuate), ca formă a unităţii infracţionale o *constituie unitatea de rezoluţie sau, după cum se exprimă legiuitorul moldovean, unitatea de intenţie şi de scop*.

Într-adevăr, datorită pluralităţii de acte componente la care se referă, hotărârea infracţională proprie infracţiunii prelungite (continuate) reprezintă un proces psihic specific, caracterizat prin reprezentarea şi voinţa săvârşirii faptei prin acţiuni sau inacţiuni repetate, la intervale diferite de timp şi reprezentând fiecare în parte conţinutul aceleiaşi infracţiuni. Prin urmare, va exista „rezoluţia unică” sau „intenţia unică” caracteristică infracţiunii continuate (prelungite) există atunci când făptuitorul îşi dă seama de caracterul prejudiciabil al acţiunilor sau inacţiunilor săvârşite, inclusiv a realizării acestora la intervale diferite de timp, prevede urmarea prejudiciabilă unică ce poate surveni ca rezultat al săvârşirii acestora şi doreşte sau admite în mod conştient survenirea acestei urmări [119, p. 12-127].

Deci, se poate concluziona că în rezoluţia unică aferentă infracţiunii continuate, cuprinde în sine întreaga activitate complexă, realizată prin acţiuni sau inacţiuni succesive, fiecare fiind aptă să constituie o infracţiune autonomă şi nu doar asupra unei infracţiuni comise eşalonat, în rate.

Se poate constata existenţa unei legături de parte-întreg între **rezoluţia (intenţia) infracţională unică** caracteristică infracţiunii prelungite şi **poziţia subiectivă sau intenţia concretizată** faţă de fiecare dintre acţiunile-inacţiunile ce o compun.

Prin urmare, în cadrul acestui tip de unitate infracţională, pe lângă rezoluţia unică, caracterizată complexului constituit din totalitatea acţiunilor sau inacţiunilor, există tot atâtea poziţii subiective distincte raportate la numărul acţiunilor sau inacţiunilor care intră în compunerea sa.

4.5. Concluzii la Capitolul 4

Cercetare fraudei informatice, din perspectiva celor două legilsaţii penale – a Republicii Moldova şi a României - ca parte integrantă a criminalităţii informatice a fundamentat următoarele concluzii:

1. Similitudinea textelor normative dedicate incrimnării și pedepsirii fraudei informatice în legislaţia penală a Republicii Moldova şi a României este una vizibilă, sunt însă diferite criteriile de apreciere a gradului prejudicabil sau a pericolului social al faptei în legislaţiile penale de referință. În viziunea legiuitorului moldovean, gradul prejudiciabil al infracţiunii de fraudă informatică, incriminată la art. 260^6 C.pen. al Republicii Moldova, este determinat în mare parte de cuantumul evaluat în bani al urmării prejudiciabile, ce survine în rezultatul comiterii infracţiunii. În baza acestei abordări legislative pentru existenţa temeiului juridic al răspunderi penale, prevăzut de art. 51 alin. (1) C.pen. Republicii Moldova este necesar ca în rezultatul săvârşirii faptei victimei să i se provoace o daună materială care depăşeşte 20 de salarii medii lunare pe economie prognozate, stabilite prin hotărîrea de Guvern în vigoare la momentul săvîrşirii faptei.

2. În raport cu infracţiunile prevăzute de art. 190 şi 196 C.pen. al Republicii Moldova, infracţiunea specificată la art. 260^6 C.pen. al Republicii Moldova se distinge printr-un mecanism propriu de săvârșire, ce constă în recurgerea la mijloace informatice, aplicate într-un mediu informatic. Aceste mijloace speciale de săvârşire a infracţiunii au ca efect teza, potrivit căreia, cele stipulate la alin. (1) al art. 260 C.pen. al Republicii Moldova, reprezintă o normă specială, în raport cu norma de la art. 190 şi 196 C.pen. Prin urmare, aplicarea alin. (1) art. 260^6 C.pen.al R.Moldova, exclude reţinerea la încadrare a uneia dintre infracţiunile prevăzute la art. 190 sau 196 C.pen. al Republicii Moldova.

3. Considerăm neîntemeiată soluţia legiuitorului moldovean de a limita cercul subiecţilor activi ai fraudei informatice doar la persoanele fizice. În contextul progresului tehnico-ştiinţific,

succeptibilitatea persoanelor juridice de a fi implicate în activităţi infracţionale de fraudare informatică este una evidentă.

3. De *lege ferenda* propunem următoarea variantă a textului incriminator de la art. 260^6 C.pen. al Republicii Moldova:

Frauda informatică,

(1) Dobândirea ilegală a bunurilor altei persoane, a avantajelor materiale sau de altă natură prin introducerea, modificarea sau ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic,

se pedepsesc cu amendă în mărime de la 550 la 850 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare până la 4 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 1000 la 3000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(2) Aceleaşi acţiuni săvârşite:

a) de un grup criminal organizat sau de o organizaţie criminală;

b) în proporţii mari

se pedepsesc cu închisoare de la 4 la 8 ani cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de până la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 3000 la 5000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(3) Acţiunile prevăzute la alin. (1)-(2) săvîrşite în proporţii deosebit de mari

se pedepsesc cu închisoare de la 7 la 12 ani cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de până la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 5000 la 10000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea persoanei juridice.

(4) Cauzarea de pagube materiale prin introducerea, modificarea sau ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic săvârşită în proporţii mari, dacă fapta nu este o însuşire

se pedepsesc cu amendă în mărime de la 200 la 500 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare de până la 3 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 500 la 3000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(5) Acţiunile prevăzute la alin.(4) săvârşite în proporţii deosebit de mari

se pedepsesc cu închisoare de la 3 la 6 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 3000 la 5000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

CONCLUZII GENERALE ȘI RECOMANDĂRI

Problema științifică de importanţă majoră soluţionată prin cercetarea realizată constă în fundamentarea științifică a elementelor şi semnelor constitutive ale infracţiunii de fraudă informatică prin prisma legii penale şi practicii judiciare, având ca efecte favorizarea încadrării juridice și aplicarea corectă a legii, precum și perfecționarea cadrului normativ de sancționare, fapt de natură să contribuie la sporirea ansamblului preventiv și de combatere a infracțiunilor în sfera tehnologiilor informaționale.

Cercetarea problemelor teoretice şi practice ale fraudei informatice a determinat următoarele **concluzii generale:**

1. Criminalitatea informatică a crescut în sofisticare și prevalență, ajungând în a implica din ce în ce mai mult și crima organizată, motiv pentru care pagubele înregistrate, ca și consecință a acestui tip de activitate, sunt în continuă creștere.

2. Fenomenul criminalității informatice are o dimensiune internațională, caracterizată prin numeroase legături teritoriale, astfel încât infractorul din domeniul informatic, deși este sub jurisdicția unui anume stat, acțiunile sale ilegale pot avea drept țintă computere și persoane din alte țări. În astfel de împrejurări se impune cooperarea internațională în domeniul combaterii criminalității informatice între organele de ocrotire a normelor de drept în scopul colectării probelor în procesul de investigare.

3. Natura criminalității informatice este una planetară, în consecință și natura problemelor cadrului juridic în acest domeniu, impune necesitatea unui consens global în vederea armonizării, atât a legislației, cât și a procedurilor de investigare. Convenția Consiliului Europei privind criminalitatea informatică constituie un ghid pentru toate statele europene, dar și pentru alte țări, care au utilizat-o ca pe un model normativ la adoptarea măsurilor interne de prevenire și combatere a criminalității informatice.

4. *Frauda informatică*, în viziunea noastră, poate fi definită ca fiind *un act infracţional săvârşit prin intrarea, alterarea, ştergerea, sau supraimprimarea de date sau de programe pentru calculator sau orice alta ingerinţă într-un tratament informatic care îi influenţează rezultatul, cauzând prin aceasta un prejudiciu economic sau material, cu intenţia de a obţine un beneficiu nelegitim pentru sine însuşi sau pentru altul*.

5. Conţinutul obiectului juridic generic al fraudei informatice, incriminate în legislaţia penală românească, îl formează relaţiile sociale, a căror formare, existenţă şi dezvoltare sunt condiţionate de de necesitatea protejării relaţiilor sociale cu caracter patrimonial. Prin urmare, dintr-o atare abordare legislativă, frauda informatică este considerată drept o infracţiune patrimonială săvârşită prin utilizarea sistemelor informatice.

6. Obiectul juridic generic al fraudei informatice în legislaţia penală a Republicii Moldova îl formează un spectru specific de relaţii sociale a cărora existenţă şi desfăşare sunt condiţionate de necesitatea protejării informaticii şi telecomunicaţiilor. Prin urmare, dintr-o atare abordare legislativă, frauda informatică este considerată drept o infracţiune informaţională, care este săvârşită prin utilizarea sistemelor informatice în scopul obținerii de benficii materiale.

7. La baza poziționării locului incriminator al fraudei informatice în legislaţia penală stau două criterii: 1) obiectul juridic de atentare și 2) mijlocul de comitere a infracţiunii.

8. Din noţiunea fraudei informatice, reiese, în mod indubitabil, că scopul final al infractorului nu este de a perturba sistemul informaţional, ci cel de a obţine anumite bunuri, beneficii sau drepturi asupra bunurilor. Prin urmare, anume aceasta este raţiunea legiuitorilor care incriminează frauda informatică ca infracţiune patrimonială. În această viziune legislativă relaţiile patrimoniale prevalează în raport cu relaţiile ce condiţionează existenţa sistemului informaţional, fapt pentru care frauda informatică este incriminată în compartimentul ce se referă ocrotirea penală a patrimoniului.

9. Mijlocul de comitere al fraudei informatice este în măsură să perturbeze sau chiar să dăuneze în mod grav sistemul informaţional, afectându-se în acelaşi timp şi încrederea pe care persoanele o au în utilizarea acestora. În această abordare, deja relaţiile sociale referitoare la protejarea sistemului informaţional prevelază în raport cu relaţiile sociale din domeniul patrimonial, fapt pentru care infracţiunea este incriminată în acel compartiment al legii penale care se referă la ocrotirea relaţiilor sociale din domeniul informaticii.

10. Similitudinea textelor normative dedicate incrimnării și pedepsirii fraudei informatice în legislaţia penală a R. Moldova şi a României este una vizibilă, sunt însă diferite criteriile de apreciere a gradului prejudiciabil sau a pericolului social al faptei, în legislaţiile penale de referință. În viziunea legiuitorului moldovean, gradul prejudiciabil al infracţiunii de fraudă informatică, incriminată la art. 260^6 C.pen. al R. Moldova, este determinat, în mare parte, de cuantumul evaluat în bani al urmării prejudiciabile ce survine în rezultatul comiterii infracţiunii. În baza acestei abordări legislative pentru existenţa temeiului juridic al răspunderi penale, prevăzut de art. 51 alin. (1) C.pen. R. Moldova este necesar ca în rezultatul săvârşirii faptei victimei să i se provoace o daună materială care depăşeşte 20 de salarii medii lunare pe economie prognozate, stabilite prin hotărârea de Guvern în vigoare la momentul săvârșirii faptei.

11. În raport cu infracţiunile prevăzute de art. 190 şi 196 C.pen. al Republicii Moldova, infracţiunea specificată la art. 260^6 C.pen. se distinge printr-un mecanism propriu de săvârşire ce constă la recurgerea la mijloace informatice, aplicate într-un mediu informatic. Aceste mijloace speciale de săvârşire a infracţiunii au ca efect teza, potrivit căreia, norma de la alin. (1) al art. 260^6 C.pen. reprezintă o normă specială în raport cu norma prevăzută la art. 190 şi 196 C.pen. Prin urmare,

aplicarea alin. (1) art. 260^6 C.pen. exclude reţinerea, la încadrarea faptei, a uneia dintre infracţiunile prevăzute la art. 190 sau 196 C.pen. Republicii Moldova.

12. Considerăm neîntemeiată soluţia legiuitorului moldovean de a limita cercul subiecţilor activi al fraudei informatice doar la persoanele fizice. În contextul progresului tehnico-ştiinţific, succeptibilitatea persoanelor juridice de a fi implicate în activităţi infracţionale de fraudare informatică este una evidentă.

Totodată, reieșind din cercetarea fenomenului fraudei informatice, ținem să formulăm următoarele propuneri legislative:

1. De *lege ferenda* propunem următoarea variantă a textului incriminator de la art. 260^6 C.pen. al Republicii Moldova:

Frauda informatică,

(1) Dobândirea ilegală a bunurilor altei persoane, a avantajelor materiale sau de altă natură prin introducerea, modificarea sau ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic,

se pedepsesc cu amendă în mărime de la 550 la 850 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare până la 4 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 1000 la 3000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(2) Aceleaşi acţiuni săvârşite:

a) de un grup criminal organizat sau de o organizaţie criminală;

b) în proporţii mari

se pedepsesc cu închisoare de la 4 la 8 ani cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de până la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 3000 la 5000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(3) Acţiunile prevăzute la alin. (1)-(2) săvîrşite în proporţii deosebit de mari

se pedepsesc cu închisoare de la 7 la 12 ani cu privarea de dreptul de a ocupa anumite funcţii sau de a exercita o anumită activitate pe un termen de până la 5 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 5000 la 10000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea persoanei juridice.

(4) Cauzarea de pagube materiale prin introducerea, modificarea sau ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic săvârşită în proporţii mari, dacă fapta nu este o însuşire

se pedepsesc cu amendă în mărime de la 200 la 500 unităţi convenţionale sau cu muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau cu închisoare de până la 3 ani, iar

persoana juridică se pedepseşte cu amendă în mărime de la 500 la 3000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

(5) Acţiunile prevăzute la alin.(4) săvârşite în proporţii deosebit de mari

se pedepsesc cu închisoare de la 3 la 6 ani, iar persoana juridică se pedepseşte cu amendă în mărime de la 3000 la 5000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate.

2. De *lege ferenda*, pentru o mai bună prevenire a fraudei informatice se propune introducerea în legislația penală a Republicii Moldova și a României a unei noi incriminări cu denumirea marginală de ***furt de identitate*** *(phishing)*, cu următoarea formulare legislativă: ***acțiunea prin care făptuitorul obține în mod fraudulos identitatea altei persoane cu ajutorul sistemelor informatice sau de telecomunicație prin inducerea în eroare a utilizatorului sistemului informatic datorită creării unei stări de aparență menite a determina utilizatorul să furnizeze date personale în cadrul unei comunicări electronice.*** În C.pen. al României incriminarea ar urma să fie statuată în Titlul VII, Capitolul VI din Partea specială la art. 364^1, cu instituirea unei pedepse *de la 3 luni pînă la 2 ani sau cu amendă*. În C.pen. al Republicii Moldova incriminarea urmează să fie încorporată în Capitolul XI din Partea specială prin introducerea art. 260^7 și instituirea următoarei pedepse: *amendă în mărime de la 200 la 500 unităţi convenţionale sau muncă neremunerată în folosul comunităţii de la 150 la 200 de ore, sau închisoare de pînă la 2 ani, cu amendă, aplicată persoanei juridice, în mărime de la 1000 la 3000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate*.

Avantajele recomandărilor constau în:

a) evidențierea lacunelor de reglementare și elaborarea propunerilor de lege ferenda privind perfecționarea cadrului incriminatoriu din legislația României și a Republicii Moldova;

b) armonizarea legislației penale din România și Republica Moldova în conformitate cu prevederile și cu spiritul Convenției Consiliului Europei privind criminalitatea informatică;

c) conturarea unor linii directoare pentru organele de specialitate în vederea aplicării corecte și uniforme a normelor penale privind răspunderea pentru săvârșirea infracțiunii de fraudă informatică.

Subiecte pentru cercetare științifică de perspectivă:

Deoarece prezenta teză de doctorat se focusează pe studiul exhaustiv al fraudei informatice în contextul criminalității informatice, viitoarele demersuri științifice vor fi făcute pentru analiza juridico-penală și a celorlalte infracțiuni informatice prevăzute în Codul penal român și Codul penal al Republicii Moldova și analiza lor comparativă. Astfel, se vor avea în vedere infracțiuni precum: 1) accesul ilegal la un sistem informatic, 2) interceptarea ilegală a unei transmisii de date informatice, 3) alterarea integrității datelor informatice, 4) perturbarea funcționării sistemelor informatice, 5)

transferul neautorizat de date informatice, 6) operațiuni ilegale cu dispozitive sau programe informatice, 7) pornografia infantilă săvârșită prin sisteme informatice iar rezultatele cercetării vor fi înfățișate în lucrări distincte. Având în vedere că fenomenul infracțional în domeniul informatic se marchează și prin caracterul specific al probatoriului penal, al urmelor produse, sunt de perspectivă și cercetările științifice privind:

- particularitățile investigării infracțiunii de fraudă informatică;
- particularitățile expertizei judiciare în cauzele privind fraudă informatică.

BIBLIOGRAFIE

1. Adrian Cristian Moise, Analysis of Directive 2013/40/EU on atack against information systems in the context of approximation of law at the Europen level, în Journal of Law and Administrative, Special Issue, 2015, p.374-383.
2. Adrian Cristian Moise, *Metodologia investigarii criminalistice a infractiunilor informatice*, Ed. Universul Juridic, Bucuresti, 2011,442 p.
3. Adrian-Cristian Moise, *Dimensiunea criminologică a criminalității din cyberspațiu*, Ed. C.H. Beck, București, 2015, 423 p.
4. Alexandru Boroi, *Drept penal. Partea specială*, Ed. C.H. Beck, București, 2011, 734 p.
5. Alexandru Ionaș, Alexandru Florin Măgureanu, Cristina Dinu, *Drept penal. Partea specială,* Ed. Universul Juridic, București, 2015, 784 p.
6. Alexei Barbăneagră, Gheorghe Alecu, Viorel Berliba, Vitalie Budeci, Trofim Carpov, Valeriu Cușnir, Radion Cojocaru, Alexandru Mariț, Tudor Popovici, Gheorghe Ulianovschi, Xenofon Ulianovschi, Nicolae Ursu, Victor Volcinschi, *Codul penal al Republicii Moldova: Comentariu*, Tipografia Reclama, Chișinău, 2009, 859 p.
7. Alin Teodorus Drăgan, *Criminalitatea informatică; aspecte generale și moduri de operare a infractorilor*, în Materialele Conferinței științifice internaționale anuale a doctoranzilor și tinerilor cercetători, Vol. II, Ediția a VI-a, 12 aprilie 2012, Chișinău, p.179-189.
8. Alin Teodorus Drăgan, *Falsul informatic în viziunea Noului Cod penal român și a Codului Penal al Republicii Moldova*, în Revista Națională de Drept nr. 1/2015, p.44-48.
9. Alin Teodorus Drăgan, *Hacking and computer crimes. Computer fraud – a comparative look at the new criminal Code and the criminal Code of the Republic of Moldova,* Agora International Journal of Juridical Sciences, nr. 1/2014, p.29-34.
10. Alin Teodorus Drăgan, *Particularities regarding computer search and field research for online crimes,* Agora International Journal of Juridical Sciences, nr. 2/2013, p.85-90.
11. Alin Teodorus Drăgan, *Procedural aspects of cybercrimes investigations,* Journal of legal studies, vol. XVI, december, 2015, p.55-67.
12. Alin Titus Pîrcălab, Sorin Fildan, *Informatică juridică*, Ed. Cordial Lex, Cluj-Napoca, 2012, 312 p.
13. Alina Letiția, *Metode de investigare a criminalității informatice*, în Dreptul, nr. 12/2013, p. 250-266.
14. Anastasiu Crișu, *Drept procesual penal. Partea generală*. Ed. Hamangiu, București, 2016, 583 p.
15. Anca-Lelia Lorincz, *Drept procesual penal, Vol. I*, Ed. Universul Juridic, București, 2015, 347 p.

16. Andrei Ionuț Barbu, *Infracțiuni săvârsite prin internet*, în Revista de investigare a criminalității, anul V, numărul 1/2012, p.100-106.
17. Andrei Zarafiu, *Procedură penală. Partea generală. Partea specială*. Ed. C.H. Beck, București, 2014, 492 p.
18. Camil Suciu, *Criminalistică*, Ed. Didactică și Pedagogică, București, 1972, 656 p.
19. Chuck Easttom, Jeff Taylor, *Computer Crime, Investigation, and the Law*, Cengage Learning, 2011, 499 p.
20. Codruț Olaru, *Mijloace specifice de investigare a infracțiunilor de criminalitate organizată*, Ed. Hamangiu, București, 2014, 130 p.
21. Codruț Olaru, *Particularitățile criminalității organizate în România*, Ediția a 2-a, Editura Hamangiu, București, 2015, p. 323.
22. Codul de procedură penală a României, în M. Of. din 486 din 15 iulie 2010, în vigoare de la 1 februarie 2014.
23. Codul de procesură penală al Republicii Moldova, în M. Of. nr. 104-110, art. nr. 447.
24. Codul penal al Republicii Moldova, în M. Of. nr. 72-74 din 14.04.2009, art. nr. 195.
25. Codul penal al României, în M. Of. nr. 510 din 24 iulie 2009, în vigoare de la 1 februarie 2014.
26. Cojocaru R. Escrocherii informaţionale: forme şi clarificări conceptuale ale cadrului normativ-penal de incriminare. În: Probleme de prevenire şi combatere a criminalităţii de către organele afcerilor interne în perioada recesiunii economice. Chişinău, 2010. p. 17-22.
27. Constantin Drăghici, Adrian Iacob, Ciprian Iftimie, *Metode și tehnici moderne de cercetare și identificare criminalistică*, Ed. Lumina Lex, București, 2006, 256 p.
28. Convenția Consiliului Europei privind criminalitatea informatică, în M. Of. nr. 343 din 20.04.2004.
29. Cristian Drăghici, Cristian Eduard Ștefan, *Tactica efectuării percheziției și a ridicării de obiecte și inscrisuri,* Ed. Sitech, Craiova, 2006, 251 p.
30. Cristian Nedelcu, *Criminalistică. Tehnica și tactica criminalistică,* Ed. Hamangiu, *București,* 2014, 448 p.
31. Cristinel Ghigheci, Principiile procesului penal în noul Cod de procedură penală, Ed. Universul Juridic, București, 2014, 340 p.
32. Dan Cimpoeru, *Dreptul internetului*, Ed. C.H. Beck, București, 2012, 504 p.
33. Dan Voinea, Vasile Lăpuși, *Unele considerente privind probele și mijloacele de probă*, în Revista română de criminalistică, nr. 3/2015, p. 1945-1947.
34. Daniela Gărăiman, *Dreptul și informatica*, Ed. All Beck, București, 2003, 350 p.
35. Dave Kleiman, *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensics Investigations*, Ed. Syngress, Burlington, Massachusetts, 2007, 960 p.

36. David D'Agostini, *Diritto penalle dell'Informatica – dai Computer Crimes alla Digital Forensics,* Experta, Forli, 2007, 327 p.
37. Delia Littlejohn Shinder, *Scene of the cybercrime. Computer Forensics Handbook*, Syngress Publishing, Rockland Massachusetts, 2002, 744 p.
38. Denis Gabriela Ghervase, *Securitatea informațiilor și internetul – criminalitatea informatică*, Ed,Unniversitaria Craiova, 2013, 124 p.
39. Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului, disponibilă pe site-ul data.consilium.europa.eu/doc/document/PE-38-2012-REV-1/ro/pdf (vizitat la 11.08.2015).
40. Dobrinoiu M. Infracţiuni în domeniul informaticii. Ed. C.H.Beck, Bucureşti, 2006. 401 p.
41. Dorin Ciuncan, *Dicționar de procedură penală*, Ed. Universul Juridic, București, 2015, 472 p.
42. Dorothy E. Denning, Cyberterrorism, Testimony before the Special Oversight Panel on Terorism, The Terrorism Research Center, Committee an Armed Services, U.S. House of Representatives, 23 May, 2000, p. 1, publicat pe www.nato.int/structur/.../cyberterrorism.pdf (vizitat la 17.03.2013) .
43. Douglas Schweitzer, *Incident Response: Computer Forensics Toolkit*, Wiley Publishing Inc., Indianapolis, Indiana, 2003, 345 p.
44. Dumitru Dumbravă, *Agresiunile în spațiul cibernetic*, în Revista Română de Studii de Inteligence nr. 6/2011, 650 p.
45. Dumitru Oprea, *Protecția și securitatea informațiilor*, Ed. Polirom, București, 2007, 448 p.
46. Dumitru Rădoiu, *Noua ordine informațională*, BYTE România, octombrie 1995, 200 p.
47. Duşa Adrian. Elemente de analiză comparativă. Bucureşti: Tritonic, 2014. p. 74. 220 p
48. Emilian Stancu, Adrian Cristian Moise, *Criminalistica. Elemente de tehnică și de tactică a investigării penale*, Ed. Universul juridic, București, 2014, 307 p.
49. Emilian Stancu, Carmina - Elena Aleca, *Elemente de criminologie generală*, Ed. Pro Universitaria, București, 2014, 261 p.
50. Emilian Stancu, *Tratat de criminalistică*, ed. a III-a, Ed. Universul juridic, București, 2004, 736 p.
51. Emilian Stancu, *Tratat de criminalistică*, Ed. Universul Juridic, București, 2010, 840 p.
52. Eoghan Casey, *Digital evidence and computer crime, third edition,* Academic Press, 2011, 807 p.
53. Ernesto U. Savona, *Crime and Technology – New Frontiers for regulation, law, enforcement and research*, Springer, Massachusetts, 2004, 140 p.

54. Felicia Donovan, Kristyn Bernier, *Cyber Crime Fighters: Tales from the trenches,* QUE, Indianapolis, Indiana, 2009, 308 p.
55. Francesca Bosco, *The New Cybercriminals HPP: Hackers Profiling Project,* United Nations Interregional Crime and Justice Research Institute, 23 October 2012, 58 p.
56. Francesco Baressi, Michele Nigretti, *Fenomeno hacking: analisi sociocriminalistica dell intrusione informatica,* Iris 4 Edizioni, Roma, 2012, 178 p.
57. Gabriel Naghi, *Criminalistică - fundamente*, Ed. Universul Juridic, București, 2014, 276 p.
58. George Antoniu și colab, *Explicații preliminare ale noului Cod penal*, vol. III, Ed. Universul Juridic, București, 2013, 656 p.
59. George Antoniu, *Infracțiuni contra patrimoniului. Generalități*, în Revista de Drept penal, anul VII, NR. 4, București, 2000.
60. George Antoniu, Tudorel Toader (coordonatori), Verșavia Brutaru, Constantin Duvac, Ion Ifrim, Daniela Iuliana Lămășanu, Ilie Pașcu, Marieta Safta, Constantin Sima, Ioana Vasiu, *Explicațiile noului Cod penal*, vol. III, Ed. Universul Juridic, București, 2015, 600 p.
61. George Antoniu, Tudorel Toader (coordonatori), Verșavia Brutaru, Ștefan Daneș, Constantin Duvac, Ioan Griga, Ion Ifrim, Gheorghe Ivan, Gavril Paraschiv, Ilie Pascu, Ion Rusu, Marieta Safta, Iancu Tănăsescu, Ioana Vasiu, *Explicațiile noului Cod penal,* vol. IV, Ed. Universul Juridic, București, 2016, 896 p.
62. George Curtis, *The law of cybercrimes and their investigations*, CRC Press, Florida, 2012, 414 p.
63. George Zlati, *Legitima apărare și starea de necesitate în domeniul criminalității informatice (II),* în Dreptul, nr. 5/2015, p. 143-171.
64. George Zlati, *Unele considerații cu privire la infracțiunile prevăzute de art. 5 lit. b) și e) din Legea nr. 11/1991 privind combaterea concurenței neloiale*, Pandectele Române, nr. 9/2012.
65. Gheorghe Alecu, Alexei Barbăneagră, *Reglementarea penală și investigarea criminalistică a infracțiunilor din domeniul informatic*, Ed. Penguin Book, București, 2006, 271 p.
66. Gheorghe Iulian Ioniță, *Infracțiunile din sfera criminalității informatice*, Ed. Universul Juridic, București, 2012, 344 p.
67. Gheorghe Iulian Ioniță, *Accesul la un sistem informatic și recursul în interesul legii formulat în această materie,* în Revista de drept penal, nr. 4/2013, p.111-125.
68. Gheorghe Iulian Ioniță, *Aspecte procesual penale și tehnice referitoare la percheziția informatică,* în Dreptul, nr. 12/2014, 456 p.
69. Gheorghe Iulian Ioniță, *Infracțiunile din sfera criminalității informatice*, Ediția a II-a revăzută și adăugită, Ed. Pro Universitaria, București, 2013, 338 p.
70. Gheorghe Iulian Ioniță, *Principalii factori care influențează dezvoltarea criminalității informatice, provocări ale combaterii fenomenului*, în Instituții juridice contemporane, în

contextul integrării României în Uniunea Europeană, ed. a III-a, Ed. Pro Universitaria Bucureti, 2009.

71. Gheorghe Ivan, Mari – Claudia Ivan, *Drept penal. Partea specială*, Ed. C.H. Beck, 2015.
72. Gheorghe Nistoreanu și colab., *Drept penal. Partea specială*, Ed. Europa Nova, București, 1999, 650 p.
73. Gheorghe Vizitiu, *Delapidarea*, Ed. Lumina Lex, București, 2001, 96 p.
74. Gheorghiță Mateuț, *Procedură penală, Partea generală*, vol. II, Ed. Chemarea, Iași, 1996, 550 p.
75. Grainne Kirwan, Andrew Power, *Cybercrime. The Psichology of Online Offenders*, Cambridge Universidy Press, 2013, 256 p.
76. Grigore Gr. Theodoru, *Drept procesual penal*, Ed. Cugetarea, Iași, 1996, 265 p.
77. Grigore Gr. Theodoru, *Tratat de Drept procesual penal*, ed. a 3-a, Ed. Hamangiu, București, București, 2013, 896 p.
78. Grigore Nicolae Labo, *Cercetarea Criminalistică*, Ed. Pro Universitaria, București, 2014, 235 p.
79. Grigore Theodoru, Lucia Moldovan, *Drept procesual penal*, Ed. Didactică și Pedagogică, București, 1979, 352 p.
80. Guinka Hristova, *Le phenomene "cybercriminalite". Strategie pour combattre la cybercriminalite et mesures concrets*, Editions universitaires europeennes, 2011, 78 p.
81. Hotărârârea Guvernului Republicii Moldova nr. 811 din 29.10.2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, publicată în M. Of. nr. 306-310, art. nr. 905.
82. Hotărârea Guvernului Moldovei 857 din 31.10.2013, publicată în M. Of. nr. 306-310, art. nr. 905.
83. Hotărârea Guvernului Republicii Moldova nr. 808 din 07.10.2014 cu privire la aprobarea Planului național de acțiuni pentru implementarea Acordului de Asociere Republica Moldova – Uniunea Europeană în perioada 2014-2016, publicată în M. Of. nr. 297-309, art. nr. 851.
84. Hotărârea nr. 271/2013 privind aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind mplementarea Sistemului național de securitate cibernetică, publicată în Publicată în M. Of. Partea I nr. 296 din 23.05.2013.
85. Hotărârea Plenului Curţii Supreme de Justiţie a R. Moldova din 28.06.2004, nr.23, cu privire la practica judiciară în procesele penale despre sustragerea bunurilor. În: Buletinul CSJ a R. Moldova, nr. 8, 2004.
86. http//dexonline.ro/definiție/investigație (vizitat la 08.10.2014).
87. http://etalonline.by (accesat la 1.10.2016).
88. http://www.competentedigitale.ro/ (vizitat la 17.05.2014).

89. http://www.comunic.ro/article/raport-kaspersky-lab-rom%C3%A2nia-se-afl%C4%83-%C3%AEn-categoria-de-risc-moderat-privind-infectarea-online (vizitat la 23.01.2016).
90. http://www.consultant.ru/document (accesat la 1.10.2016).
91. http://www.securitate-informatica.ro/ (vizitat la 30.05.2014).
92. http://www.softsystems.ro/ (vizitat la (10.07.2014).
93. https://www.cert-ro.eu/ (vizitat la 11.03.2014).
94. https://www.fbi.gov/.../terrorism/terrorism-defin (vizitat la 12.05.2012).
95. Ilie Pașcu, Mirela Gorunescu. *Drept penal. Partea specială*, ed. a 2-a, Ed. Hamangiu, București, 2009, 824 p.
96. Ioan Doltu, *Probele și mijloacele de probă cu privire specială la declarațiile învinuitului sau ale inculpatului, ca mijloace de probă și apărare în procesul penal*, Ed. Dobrogea, Constanța, 1997, 210 p.
97. Ioana Vasiu, *Criminalitatea informatică*, Ed. Nemira, București, 1998, 239 p.
98. Ioana Vasiu, Lucian Vasiu, *Criminalitatea in cyberspațiu*, Ed.. Universul Juridic, Bucuresti, 2011, 390 p.
99. Ioana Vasiu, Lucian Vasiu, *Informatica juridică și drept informatic*, Ed. Albastră, Cluj-Napoca, 2009, 225 p.
100. Ioana Vasiu, *Totul despre Hackeri*, Ed. Nemira, București, 2001, 185 p.
101. Ion Coman, *Aspecte privind cercetarea la fața locului în infracțiunile de omor*, I.G.M., București, 1975, 350 p.
102. Ion Craiovan, *Tratat de teoria generală a dreptului*, ediția a iii-a revăzută și adăugită, Ed. Universului Juridic, București, 2015, 600 p.
103. Ion Dogaru, Sevastian Cercel, *Drept civil. Teoria generală a drepturilor reale*, Ed. All Beck, București, 2003, 371 p.
104. Ion Gabriel Olteanu, Adrian Iacob, Mirela Gorunescu ș.a., *Metodologie criminalistică - structurile infracționale și activitățile ilicite desfășurate de către acestea,* Ed. AIT Laboratories, București, 2008, 560 p.
105. Ion Mircea, *Importanța și modul determinării modului de tragere*, în Studia Universitatis Babeș-Bolyai, Oeconomica et jurisprudential, Cluj, 1961, 155 p.
106. Ion Neagu, *Drept procesual penal, Partea specială*, vol. I, Ed. Oscar Print, București, 1994, 272 p.
107. Ion Neagu, Mircea Damaschin, *Tratat de procedură penală. Partea generală - În lumina noului Cod Cod de procedură penală,* Ed. Universul Juridic, București, 2014, 743 p.
108. Ion Neagu, Mircea Damaschin, *Tratat de procedură penală. Partea specială,* Ed. Universul Juridic, București, 2015, 676 p.

109. Ion Neagu, *Tratat de procedură penală. Partea generală, ed. a II-a, revăzută și adăugită*, Ed. Universul Juridic, București, 2010, 680 p.
110. Ion P. Filipescu, Andrei I. Filipescu, Drept civil. *Dreptul de proprietate și alte drepturi reale*, Ed. Actami, București, 2000, 415 p.
111. Ion Poiană, Ioana Păcurariu, *Drept procesual penal, partea generală*, Ed. Universul juridic, București, 2014, 268 p.
112. Ion Ristea, *Drept penal. Partea specială*, vol. I, Ed. Universul Juridic, București, 2014, 550 p.
113. Ionuț Andrei Barbu, *Introducere în criminalitatea informatică*, Ed. Sitech, Craiova, 2014, 224 p.
114. Jaime J. Triquell, *Role d enqueteur specialise*, Revue de la Gendarmerie Nationale, nr. 159/2000, Paris, 2008, 250 p.
115. Jason Anders, Steve Winterfeld, *Cyber Warfare. Techniues, Tactics and Tools for Security Practioners*, Second Edition, Syngress, 2013, 324 p.
116. John Sammons, *The basics of digital forensics*, Syngress, Waltham, Massachusetts, 2012, 177 p.
117. Ken Fenstein, *Antispam, viruși, pop-up, spyware*, Ed. Rosseti Educational, București, 2006, 248 p.
118. Ketty Guiu, *Infracțiunile contra patrimoniului. Considerații generale*, în Dreptul nr. 3/2004, 350 p.
119. Larii Iu., Cojocaru R. ș.a. Infracţiunea continuată (prelungită) în dreptul penal – legislaţie, teorie şi practică judiciară. Chişinău, 2016, 193 p.
120. Larry J. Siegel, *Criminology: Theories, Patterns, and Typologies*, 10th Edition, Cengage Learning, 2007, 640 p.
121. Laura Codruța Kovesi, *Accesul și supravegherea sistemelor de telecomunicații sau informatice. Mijloace de probă*, în Dreptul nr. 7/2003.
122. Lazăr Cârjan, *O abordare modernă a investigării locului faptei*, în Revista de investigare a criminalității nr. 2/2008.
123. Legea nr. 187/2012 pentru punerea în aplicare a Legii nr. 286/2009, art. 298.
124. Legea nr. 20 din 03.02.2009 privind prevenirea și combaterea criminalității informatice, publicată în M.l Of. nr. 11-12 din 26.01.2010, art. nr. 17.
125. Lidia Barac, *Drept penal. Partea specială*, Ed. Universul Juridic, București, 2014, 281 p.
126. Linda Bird, *Internet ghid complet de utilizare*, Ed. Corint, București, 2008, 548 p.
127. Lucaci Iosif, Martin Robert, *Investigarea fraudelor informatice*, Ed. M.I., 2002, 207 p.
128. Lucian Mihăescu, *Sisteme informaționale și aplicații informatice în adminisrarea afacerilor*, Ed. Universității ”Lucian Blaga”, 2009, 214 p.
129. Luigi Cuomo, Ranieri Razzante, *La disciplina dei reati informatici*, Giappichelli, Torino, 2007, 362 p.

130. Magdalena Iordache, *Camera preliminară în noul Cod de procedură penală*, Ed. Universul Juridic, București, 2014, 198 p.
131. Magdalena Iordache, *Judecata în primă instanță în noul Cod de procedură penală*, Ed. Universul Juridic, București, 2014, 214 p.
132. Magdalena Iordache, *Nulitățile în noul Cod de procedură penală*, Ed. Universul Juridic, București, 2015, 270 p.
133. Marian Drilea-Marga, *Urmărirea penală în noul Cod de procedură penală*, Ed. Universul Juridic, București, 2014, 241 p.
134. Mariana Zainea, Raluca Simion, *Infractiuni in domeniul informatics - culegere de practica judiciara*, Ed. C. H. Beck, Bucuresti, 2009.
135. Marije T. Britz, *Computer Forensics and Cyber Crime: An Introduction*, 3rd Edition, Prentice Hall, 2013, 408 p.
136. Marin Ruiu, *Metodologia investigării criminalistice a unor genuri de infracțiun*i, Ed. Universul Juridic, București, 2014, 188 p.
137. Marius Pantea, Ion. Cosmin Mihai, Gheorghe Dorobantu, *Investigarea fraudelor informatice*, Ed. Sitech, Craiova, 2008, 188 p.
138. Matei Cantacuzino, *Elementele dreptului civil*, Ed. Cartea Românească, București, 1921, 760 p.
139. Maxim Dobrinoiu, *Infractiuni in domeniul informatic*, Ed. C.H.Beck, Bucuresti, 2006.
140. Maxim Dobrinoiu, *Infracțiunea de alterare a integrității datelor informatice*, Revista Română de Dreptul Proprietății Intelectuale, nr. 3/2006, 325 p.
141. Michael G. Solomon, K. Rudolph, Ed Titlel and Neil Broom, *Computer Forensics Jump Start*, 2 edition, Sybex, Indianapolis, 2011, 316 p.
142. Mihai Drăgănescu, Societatea informațională și a cunoașterii. Vectorii societății cunoașterii, p. 6, articol disponibil pe site-ul www.academiaromana.ro/pro_pri/doc/st_a01a.doc (vizitat în 08.03.2015).
143. Mihai Olariu, Cătălin Marin, *Drept procesual penal. Partea generală*, Ed. Universul Juridic, București, 2015, 275 p.
144. Mihai-Adrian Hotca, Mirela Gorunescu, Norel Neagu, Maxim Dobrinoiu, Radu-Florin Geamănu, *Infracțiuni prevăzute în legi speciale. Comentarii și explicații*, Ediția 3, Ed. C.H. Beck, București, 2013, 1080 p.
145. Mihail Gheorgiță, *Tratat de metodică criminalistică*, CEP USM, Chișinău, 2015, 531 p.
146. Mihail Udroiu (coordonator), Amalia. Andone Bontaș, Georgina Bodoroncea, Marius Bulancea, Victor Constantinescu, Daniel Grădinaru, Claudia Jderu, Irina Kuglay, Cristinel Meceanu, Lucreția. Postelnicu, Isabelle Tocan, Andra Trandafir, *Codul de procedură penală. Comentariu pe articole*, Ed. C.. H. Beck, București, 2015, 1712 p.

147. Mihail-Silviu Pocora, Monica Pocora, *Infracțiuni contra patrimoniului prin nesocotirea încrederii*, Ed. Universul Juridic, București, 2014, 213 p.
148. Mircea Damaschin, *Drept procesual penal: partea generală*, Ed. Universul Juridic, București, 2013, 450 p.
149. Nicolae Ploteanu, Sergiu Maftea, Rodica Griniuc, Angela Coțofană, *Pasul II în ciberspațiu: Securitatea Informațională*, Academia MAI ”Ștefan cel Mare”, Tipografia ”Elena VI” Chișinău 2008, 335 p.
150. Nicolae Volonciu (coordonator), Andreea Simona Uzlău, Raluca Moroșanu, Victor Văduva, Daniel Atasiei, Cristinel Ghicheci, Corina Voicu, Georgiana Tudor, Teodor-Viorel Gheorghe, Cătălin Mihai Chiriță, *Noul cod de procedură penală comentat*, ediția a 2-a, Ed. Hamangiu, București, 2015, 1542 p.
151. Nicolae Volonciu, *Tratat de procedură penală. Partea generală, vol. I*, Ed. Paideia, București, 1999, 450 p.
152. Nicolae Volonciu, *Tratat de procedură penală. Partea specială*, vol. II, Ed. Paideia, București, 1994, 504 p.
153. Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar. What Everyoone needs to know*, Oxford University Press, 2014, 320 p.
154. Peter Warren, Michael Streeter, *Cyber crime and warfare*, McGraw-Hill Educational, first edition, Great Britain, 2012, 148 p.
155. Petre Dungan, Tiberiu Medeanu, Viorel Pașca, *Drept penal. Partea specială*, Ed. Universul Juridic, București, 2014, 554 p.
156. Potrivit Hotărârii Consiliului Superior al Magistraturii nr. 140/2014 pentru aprobarea Regulamentului privind accesul judecătorilor, procurorilor și magistraților asistenți ai Înaltei Curți de Casație și Justiție la informații clasificate, secrete de stat și secrete de serviciu (www.csm1909.ro).
157. Publicată în Monitorul Oficial al României, Partea I, nr. 343 din 20.04.2004; Legea R. Moldova nr. 6 din 02.02.2009 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică Publicat: 20.02.2009 în Monitorul Oficial Nr. 37-40.
158. Radu Constantin, Pompil Drăghici, Mircea Ioniță, *Expertizele mijloc de probă în procesul penal,* Ed. Tehnică, București, 2000, 275 p.
159. Radu Mârșanu, *Sisteme de calcul*, Ed. Didactică și Pedagogică, București, 1995, 136 p.
160. Raluca Diaconu, *Tehnici de investigare a infracțiunilor informatice*, în Noi instituții ale dreptului penal și dreptului procesual penal în dialogul interprofesional între judecători și avocați, Ed. Universul Juridic, București, 2015, 560 p.

161. Raoul Chiesa, Stefania Ducci, Silvio Ciappi, *The Science of Criminal Profiling as Applied to the World of Hacking, Auerbach Publications*, 2008, 279 p.
162. Remus Jurj-Tudoran, *Metode speciale de supraveghere şi protecţia martorilor în cauzele penale complexe*, Ed. C.H. Beck, București, 2014, 232 p.
163. Richard Nolan, Colin O Sullivan, Jake Branson, Cal Waits, *Firsr Responders Guide to Computer Forensics*, CERT Training and Education, Handbook, Carnegie Mellon Software Engineering Institute, 2005, 216 p.
164. Robert Moore, *Cybercrime-investigating high-technology computer crime,* second edition, Anderson Publishing, Oxford, 2011, 318 p.
165. Rodica, Aida Popa, *Aspecte teoretice și practice referitoare la metodele speciale de supraveghere sau cercetare prevăzute în Codul de procedură penală*, în Dreptul, nr. 6/2015.
166. Sandra Grădinaru, *Supravegherea tehnică în Noul Cod de procedură penală*, Ed. C.H. Beck, București, 2014, 389 p.
167. Serge Le Doran, Philippe Rosse, *Cyber – mafia*, Ed. Antet, București, 1998, 256 p.
168. Sergiu Bogdan, Doris Alina Șerban, George Zlati, *Noul Cod penal. Partea speială. Analize, explicații, comentarii*. Ed. Uiversul Juridic, București, 2014, 880 p.
169. Sergiu Brînză, Vitalie Stati, *Drept penal. Partea specială, vol. I*, Tipografia Centrală, Chișinău, 2011, 1062 p.
170. Sergiu Brînză, Vitalie Stati, *Drept penal. Partea specială, vol. II*, Tipografia Centrală, Chișinău, 2011, 1311 p.
171. Simona Lungu, Mihaela Tilea, Dan Voinea, *Cercetarea la fața locului în cazul infracțiunilor săvârșite prin mijloace electronice,* articol apărut în volumul „Investigarea criminalistică a locului faptei", Asociația Criminaliștilor din România, Ed. Luceafărul, București, 2004.
172. Sputnik.md/world/20160311/5164998.html (vizitat la 06.04.2016).
173. Sterschi Florena Esther. Criminalitatea transnaţională: normativul penal de sancţionare şi politici de prevenire şi combatere. Teză de doctor în drept, Chişinău, 2015. 180 p.
174. Steve Johnson, *Microsoft Windows 7*, Ed. NICULESCU, BucureȘti, 2010, 554 p.
175. Susan W. Brenner, *Cybercrime: Criminal threats from cyberspace*, ABC-CLIO, Santa Barbara, California, 2010, 281 p.
176. Ștefan Prună, Ioan Cosmin Mihai*, Criminalitatea informatică*, Ed. Sitech, Craiova, 2008, 190 p.
177. Theodor Mrejeru, Bogdan Mrejeru, *Competența penală*, Ed. Nomina Lex, București, 2010, 295 p.
178. Traian Anghel, *Dicționar de informatică*, Ed. Corint, București, 2010, 448 p.
179. Traian Anghel, *Tot ce trebuie să știi despre internet*, Ed. Polirom, Bucuresti 2011, 232 p.

180. Tratatul privind funcționarea Uniunii Europene (JOUE C. 326/47 din 26 octombrie 2012), disponibil pe site-ul (http://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:12012E/TXT&from=en), (accesat la 03.01.2015).
181. Tudor Amza, Cosmin Amza, *Criminalitate informatică*, Ed. Lumina Lex, București, 2003, 520 p.
182. Tudorel Butoi și colab., *Victimologie*, Ed. Pinguin Book, București, 2004, 504 p.
183. Tyler Cohen Wood, *Depistarea impostorilor virtuali*, Lifestyle Publishing, București, 2015, 216 p.
184. Valeriu Cușnir, *Locul și rolul organelor de urmărire penală în statul de drept*, în Reforme instituționale în Republica Moldova în contextul integrării europene, Chișinău, 2006, 116 p.
185. Valeriu Manea și colab., *Curs de tehnică criminalistică, vol. I*, Academia de poliție Al. I. Cuza, București, 1983, 357 p.
186. Vasile Bercheșan, *Cercetarea penală - îndrumar complet de cercetare penală*, Ed. Icar, București, 2001, 420 p.
187. Vasile Bercheșan, Ion N. Dunitrașcu. *Probele și mijloacele de probă – mic îndrumar de cercetare penală*, Ed. Ministerului, București, 1994, 290 p.
188. Vasile Dobrinoiu, Mihai Adrian Hotca, Mirela Gorunescu, Maxim Dobrinoiu, Ilie Pascu, Ioan Chiș, Costică Păun, Norel Neagu, Mircea Constantin Sinescu, *Noul Cod penal comentat. Partea specială*, Ed. a II-a, revăzută și adăugită, Ed. Universul Juridic, București, 2014, 1154 p.
189. Vasile Dobrinoiu, Norel Neagu, *Drept penal. Partea specială*, Ed. Universul Juridic, București, 2014, 731 p.
190. Victor-Valeriu Patriciu, *Criptografia în Cyberspace*, BYTE România, octombrie 1995, 350 p.
191. Victor-Valeriu Patriciu, Ioana Vasiu, Șerban George Patriciu, *Internetul și dreptul*, Ed. All Beck București, 1999, 454 p.
192. Vintilă Dongoroz, George Antoniu, Siegfried Kahane, Rodica Mihaela Stănoiu, Constantin Bulai, *Explicații teoretice ale Codului de procedură penală român, Partea specială, vol. II*, Ed. Academiei, București, 1976, 436 p.
193. Vintilă Dongoroz, Iosif Fodor, Nicoleta Iliescu, *Explicații teoretice ale codului penal român*, Ed. All Beck, București, 2003, 1035 p.
194. Virgil Rămureanu, *Sesizarea organelor judiciare în reglementarea noului Cod de procedură penală,* în Revista Română de Drept nr. 3/1969.
195. www.crime.vl.ru/index.php (accesat la 1.10.2016).
196. www.juridice.ro/.../REZUMAT-TEZA-DE-DOCTORAT-VARA-OCTAVIAN (vizitat la 05.02.2016).
197. www.nato.int/structur/.../cyberterrorism.pdf (vizitat la 17.03.2013).

198. www.portal.just.ro, Curtea de Apel Bacău, Secția penală și pentru cauze cu minori și de familie, Decizia penală nr. 124 din 28.10.2009 (vizitat la 05.08.2015).
199. www.portal.just.ro, Judecătoria Drăgășani, sentința penală nr. 250 din 5 decembrie 2013 (vizitat la 03.08.2015).
200. www.portal.just.ro, Judecătoria Pitești, Secția penală, Sentința penală nr. 2253 din 18.11.2011.
201. www.portal.just.ro, Tribunalul Dolj, sentința penală nr. 350 din 04.07.2011 (vizitat la 30.08.2015).
202. www.portal.just.ro, Tribunalul Vâlcea, sentința penală nr. 20 din 15.02.2012 (vizitat la 08.08.2015).
203. www.univnt.ro/...doctorat/index.php?...Encescu_Florin (vizitat la 01.02.2016).
204. http://www.legislation.gov.uk/ukpga/1990/18 (accesat la 15.11.2016).
205. http://www.legislation.gov.uk/ukpga/2006/35/contents (accesat la 15.11.2016.
206. https://www.gracefulsecurity.com/uk-cyber-crime-law/ (accesat la 15.11.2016).
207. Айков Д.. Компьютерные преступления. Москва: Мир, 1999.
208. Зыков Д. Понятие компьютерного мошенничества. www.crime-research.org (accesat la 07.10.2016).
209. Карабаналов С.С., Компьютерное мошенничество при торговле ценными бумагами с использованием сети Интернет в США // http://skyglobe.ru (accesat la 12.10.2016).
210. Крымінальный кодэкс Рэспублікі Беларусь № 275-З від 09.07.1999 г. В: Ведамасці Нацыянальнага сходу Рэспублікі Беларусь, 1999 г., № 24.
211. Тропина Т. Компьютерное мошенничество»: вопросы квалификации и законодательной техники // www.connect.ru/article.
212. Уголовное право России. Части общая и особенная. А.В.Брилиантова, Москва: Проспект, 2014. стр.500.
213. Уголовное уложение (Уголовный кодекс) Федеративной республики Германия: текст и научно-практ. комментарий. Под ред. А. И. Рарога. Москва: Проспект, 2010. 280 с.
214. Уголовный Кодекс Бельгии от 08.06.1867 г. Пер. с фр. Г. И. Мачковский. Санкт-Петербург: «Юридический центр Пресс», 2004.
215. Уголовный кодекс Испании от 23.11.1995 г. Под ред. Н.Ф. Кузнецовой, Ф.М. Решетникова. Москва: Зерцало, 1998. 219 с.
216. Уголовный кодекс Республики Болгария. Науч. ред.: Лукашов А.И., Милушев Д.В., Айдаров Й.И. Санкт-Петербург: «Юрид. центр Пресс», 2001. 298 с.
217. Уголовный кодекс Республики Польша. Закон от 6 июня 1997 г. Научное редактирование А.И. Лукашева, Н.Ф. Кузнецовой, Д.А. Барилович. Санкт-Петербург: «Юридический центр Пресс», 2001. 234 с.

218. Уголовный кодекс Рооссийской Федерации № 63-Ф3 от 13.06.1996. В: «Собрание законодательства Рооссийской Федерации», № 25 от 17.06.1996.
219. Уголовный кодекс Франции. Науч. ред. Л. В. Головко, Н. Е. Крыловой; пер. с фр. и предисл. Н. Е. Крыловой. Санкт-Петербург: «Юридический центр Пресс», 2002. 650 с.
220. України Кримінальний кодекс, Закон № 2341-III від 05.04.2001. В: Відомості Верховної Ради України (ВВР), 2001, № 25-26.
221. Черных А.В. Некоторые вопросы уголовно-правовой квалификации компьютерных мошенничеств. În: Советское государство и право, 1989, № 6 . p. 65-78.

DECLARAȚIA PRIVIND ASUMAREA RĂSPUNDERII

Subsemnatul Alin Teodorus Drăgan, declar pe proprie răspundere că materialele prezentate în teza de doctorat se referă la propriile activităţi şi realizări, în caz contrar urmând să suport consecinţele, în conformitate cu legislația în vigoare.

Alin Teodorus DRĂGAN

22.06.2016

CV AL AUTORULUI

Date personale: Alin Teodorus DRĂGAN

Data și locul nașterii: 05.06.1968, loc. Arad, jud. Arad, România

Studii:

1986 – absolvent al liceului Elena Ghiba Birta din Arad

1991-1995 – Facultatea de Științe Juridice din cadrul Universității de Vest „Vasile Goldiș" din Arad

2008 – absolvent al masteratului cu specializarea Drept comunitar și administrarea justiției antidrog

2011 - până în prezent – doctorand, Institutul de Cercetări Juridice și Politice al Academiei de Ştiinţe a Moldovei

Activitate profesională: din 1995 până în prezent, asist. univ. Facultatea Drept, Universitatea Arad

Domeniul de cercetare științifică: drept penal

Participări la conferințe științifice internaționale:

- Conferința științifică internațională a doctoranzilor și tinerilor cercetători cu genericul: „Tendințe contemporane în evoluția patrimoniului istoric și juridic al Rebublicii Moldova", Chișinău, 12 aprilie, 2012;

- Conferința științifică internațională cu genericul: „Consolidarea statului de drept al Republicii Moldova în contextul evoluției sistemului internațional și proceselor integraționiste", Chișinău, 3 iunie, 2014

Lucrări publicate:

1. Protecția națională și internațională a drepturilor omului. Curs universitar, Ed. Concordia, Arad, 2003;
2. Dreptul proprietății intelectuale. Ccurs universitar, Ed. Viața arădeană, Arad, 2007;
3. Criminalitatea informatică; aspecte generale și moduri de operare a infractorilor. În: Materialele Conferinței științifice internaționale anuale a doctoranzilor și tinerilor cercetători, Vol. II, Ediția a VI-a, 12 aprilie 2012, Chișinău;
4. Particularities regarding computer search and field research for online crimes. În: Agora International Journal of Juridical Sciences, No. 2 (2013);
5. Hacking and computers crime computer fraud – a compararative look at the new criminal Code and the Criminal code of the Republic of Moldova. În: Agora International Journal of Juridical Sciences, No 1 (2014);
6. Procedural aspects of cybercrime investigations, În: Journal of legal studies,vol. XVI/2015, ISSN 2457-9017;
7. Falsul informatic în viziunea Noului Cod penal român și a Codului penal al Republicii Moldova, În: Revista Națională de drept, Chișinău, nr. 1/2015;
8. Frauda informatică în sistemul infracţiunilor. contra patrimoniului în noul cod penal român. În: Revista Națională de drept, Chișinău, nr. 6/2016;

Date de contact: str. Simion-Popa nr. 28, bl. 224, ap. 11, loc. Arad, jud Arad, România
telefon mobil: 0040765656300; e-mail: alinteodorus@ yahoo.co.uk