INSTITUTUL DE CERCETĂRI JURIDICE ŞI POLITICE
Al ACADEMIEI DE ŞTIINŢE A MOLDOVEI

Cu titlu de manuscris
C.Z.U. 343 6 (043.2)

DRĂGAN Alin Teodorus

FRAUDA INFORMATICĂ: ANALIZA JURIDICO-PENALĂ A INFRACŢIUNII

Autoreferatul tezei de doctor în drept

Specialitatea: 554.01 – Drept penal şi execuţional penal

CHIŞINĂU, 2017

Teza a fost elaborată în cadrul Institutului de Cercetări Juridice şi Politice al Academiei de Ştiinţe a Moldovei.

CONDUCĂTOR ŞTIINŢIFIC:

CUŞNIR Valeriu, doctor habilitat în drept, profesor universitar

REFERENŢI OFICIALI:

1. ULIANOVSCHI Xenofon, doctor habilitat în drept, profesor universitar
2. COJOCARU Radion, doctor în drept, conferenţiar universitar

COMPONENŢA CONSILIULUI ŞTIINŢIFIC SPECIALIZAT:

1.BARBĂNEAGRĂ Alexei, preşedinte, doctor habilitat în drept, profesor universitar

2.BERLIBA Viorel, secretar ştiinţific, doctor habilitat în drept, conf. universitar

3.BRINZĂ Sergiu, doctor habilitat în drept, profesor universitar

4.MORARU Victor, doctor în drept, profesor universitar

5.STATI Vitalie, doctor în drept, conferenţiar universitar

6.IANCU Elena, doctor în drept, profesor universitar, România

7.CĂPĂŢANĂ Gheorghe, doctor habilitat în informatică, profesor universitar

Susţinerea va avea loc la data de 12 mai 2017, ora 11-00, în şedinţa Consiliului Ştiinţific Specializat D 18 554.01 – 03 din cadrul Institutului de Cercetări Juridice şi Politice al AŞM (MD 2001, Republica Moldova, mun. Chișinău, bd. Ștefan cel Mare, 1, aud. 408).

Teza de doctor şi autoreferatul pot fi consultate la Biblioteca Naţională a Republicii Moldova, Biblioteca Academiei de Științe a Moldovei și pe pagina web a CNAA (www.cnaa.asm.md).

Autoreferatul a fost expediat la 11.04.2017.

Secretar ştiinţific al
Consiliului Ştiinţific Specializat,
dr. hab. în drept, conf. univ. **BERLIBA Viorel**

Conducător ştiinţific,
dr. hab., prof. univ. **CUŞNIR Valeriu**

Autor **DRĂGAN Alin Teodorus**

REPERELE CONCEPTUALE ALE CERCETĂRII

Actualitatea temei. Provocările pe care epoca modernă le pune practicianului in domeniul juridic derivă din răspândirea deja exponențială a instrumentelor tehnologice şi de capacitatea lor de a influenţa viaţa oamenilor.

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 esenţiale ale vieţii noastre de zi cu zi.

Societatea de azi se bazează pe tehnologii noi pentru a se administra, a oferi servicii cetatenilor şi 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 telecomunicaţiilor la serviciul militar. În acelaşi timp, economia globală este şi ea consolidată de noile tehnologii care oferă mari oportunităţi pe piaţa internaţională. Multinaţionalele, dar şi întreprinderile mici si mijlocii, îşi desfaşoară comerţul şi afacerile lor mult mai uşor, fără bariere de spaţiu. Noile tehnologii permit, într-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.

Realitatea „virtuală” ce s-a creat a deschis, de asemenea, noi spaţii pentru activitatile ludice şi a generat competente profesionale specifice, revoluţionând categoria serviciilor tradiţionale şi 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 şi 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 infracţionalitate 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 naştere o nouă formă de criminalitate, şi anume criminalitatea informatică.

Actualitatea demersului ştiinţific este conferită de creşterea exponenţială a infracţiunilor informatice o dată cu progresul tehnologiei, fapt confirmat şi de datele statistice. Astfel, în România, Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică care este o instituţie publică aflată în coordonarea Ministerului pentru Societate informaţională, în raportul privind alertele de securitate cibernetică procesate în anul 2015 a oferit următoarele date îngrijorătoare: pentru perioada de referinţă, respectiv 01.01.2015 – 31.12.2015, şi anume: s-au colectat 68.206.856 de alerte de securitate cibernetică; 26% (2.3 mil.) din totalul I.P. –urilor unice alocate spaţiului cibernetic naţional au fost implicate în cel puţin o alertă de securitate cibernetică: 78% (53. mil) din alertele colectate şi 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 [1].

Pentru a sublinia actualitatea tezei, putem menţiona un fapt foarte recent de o gravitate deosebită care se încadrează în rândul criminalităţii informatice, şi anume faptul că rezervele de valută şi aur ale Bangladeshului care se aflau în custodia Băncii Federela de Rezerve din New York, erau pe cale să aibă aceeaşi soartă ca şi sistemul bancar al Moldovei datorită acţiunilor unor hackeri. Aceştia 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 totuşi uriaşă, de 81 milioane de dolari, din cauza unei greşeli 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” (aşa cum era corect), ”fandation”. Acest fapt a stârnit suspiciuni şi a dus la anularea virării următoarelor tranşe de bani [2].

Prin prezentarea amănunţită a fenomenului criminalităţii informatice, a originilor acestuia, a formelor pe care le îmbracă, precum şi a modurilor în care sunt săvârşite infracţiunile informatice, prezenta teză se constituie într-un instrument util atât pentru teoreticieni dar şi pentru practicieni, de contracarare a acestui flagel.

Descrierea situaţiei în domeniu şi determinarea problemei cercetării. La cercetarea științifică a fenomenului infracțional de fraudă informatică au contribuit un șir de autori, care au analizat problemele existente la calificarea acesteia și au înaintat propuneri de soluționare a lor. Printre aceștia se numără: M. Dobrinoiu, Gh. Iu. Ioniță, C. Moise, I. Vasiu, L. Vasiu, I. A. Barbu, F. Encescu, O. Vară, G. Zlati (*România*), S. Brînză, V. Stati, Gh. Alecu, A. Barbăneagră (*R. Moldova*), Айков Д.А., Зыков Д.С., Карабаналов С.С.,Тропина Т.Н.,Черных А.В. (Federaţia Rusă), 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.

Nepunând la îndoială valoarea teoretico-ştiinţifică şi aplicativă a studiilor în cauză, precizăm, că prezenta lucrare este o încercare de actualizare a unor concepte, idei şi soluţii vizavi de interpretarea juridico-penală a infracţiunii de fraudă informatică, identificarea unor incoerențe, probleme și formularea unor propuneri de depășire a acestora. Totuşi, analiza și evaluarea acestor materiale a arătat că în dreptul penal au rămas neatinse un şir de subiecte ce vizează răspunderea penală pentru faptele de fraudă informatică, incriminate în legislaţia penală a României şi a Republicii Moldova. Aceste premise, deloc neglijabile ne-au direcționat spre o investigare fundamentală a tuturor aspectelor privitoare la răspunderea penală pentru frauda informatică.

Scopul şi obiectivele tezei. Scopul tezei constă în abordarea complexă a infracțiunii de fraudă informatică prin prisma reglemăntărilor din România, Republica Moldova, 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 infracţional în domeniul informatic şi caracterizarea acestuia; conturarea şi tratarea modalităţilor tipice de comitere şi a făptuitorilor în cazul infracţiunilor informatice; abordarea sediului normativ-preventiv de incriminare a fraudei informatice: actelor internaţionale de referinţă; normelor de incriminare a fraudei informatice din legislaţia altor state; reglementărilor antifraudă informatică şi incriminarea faptei în legea penală a României şi Republicii Moldova; analiza juridico-penală a conţinutului legal, condiţiilor preexistente, conţinutului juridic şi agravantelor infracţiunii 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 ştiinţifice. Bazele metodologice ale cercetării juridico-penale a infracţiunii de fraudă informatică au fost instituite dintr-o pluralitate de metode și procedee, atât teoretice dar şi practice, de cunoaştere a acestui fenomen. Astfel, pentru efectuarea acestui studiu au fost folosite o gamă de metode analitice de cercetare ştiinţifică, inclusiv: - metoda analizei comparative, constând în sesizarea elemenelor identice sau diferite în ceea ce priveşte reglementarea infracţiunii de fraudă informatică în legislaţia României, Republicii Moldova şi altor state; - metoda clasificării, care a permis clasificarea infracţiunilor informatice după anumite criterii; - metoda analizei istorice, constând în trecerea în revistă a apariţiei şi evoluţiei infracţiunilor informatice; - metoda analizei logice, constând în folosirea raţionamentelor logice pentru sintetizarea opiniilor doctrinare ale diverşilor autori.

Noutatea ştiinţifică a rezultatelor obţinute 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 soluționarea unor probleme privind aplicarea normelor în cauză, dar și întru perfecționarea cadrului normativ în domeniu.

Problema ştiinţifică de importanţă majoră soluţionată prin cercetarea realizată constă în fundamentarea ştiinţifică a elementelor şi semnelor constitutive ale infracţiunii de fraudă

informatică prin prisma legii penale şi practicii judiciare, având ca efecte favorizarea încadrării juridice şi aplicarea corectă a legii, precum şi perfecţionarea cadrului normativ de sancţionare, fapt de natură să contribuie la sporirea ansamblului preventiv şi de combatere a infracţiunilor în sfera tehnologiilor informaţionale.

Importanţa teoretică a lucrării. Valoarea teoretica a studiului se concretizează în efortul de a descrie, inventaria, analiza, interpreta şi sistematiza materia epistemologică, normativă şi praxiologică în domeniul fraudei informatice, dar şi a criminalităţii informatice în ansamblul ei. Totodată, în teză sunt concentrate viziunile doctrinare privind infracţiunea de fraudă informatică şi stabilirea elementelor constitutive a variantei tip şi agravantelor infracţiunii. Valenţele teoretice ale lucrării sunt reliefate şi de caracterul pluridisciplinar (informatic şi juridic) al cercetării, or fenomenul fraudei informatice se săvârşeşte 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. Teza oferă şi soluţii juridice adecvate pentru activitatea de interpretare şi aplicare a normei de incriminare a fraudei informatice, prevăzute la art.249 N.C.pen.român şi art. 260^6 C.pen. al Republicii Moldova. Lucrarea este utilă atât pentru teoreticienii dreptului, în special pentru instituţiile care pregătesc cadre profesionale antrenate în combaterea acestui fenomen, dar se constituie şi într-un autentic ghid de îndrumare, în special pentru cei ce aplică normele de drept, cum sunt ofiţerii de urmărire penală, procurorii şi judecătorii, dar oferă cunoştinţe şi utilizatorului obişnuit 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 şi comunicări la conferinţe ştiinţifice internaţionale, în speţă: conferinţa ştiinţifică internaţională a doctoranzilor şi tinerilor cercetători cu tema „Tendinţe contemporane în evoluţia patrimoniului istoric şi juridic al Republicii Moldova", Chişinău, 12 aprilie, 2012; Conferinţa ştiinţifică internaţională „Consolidarea statului de drept al Republicii Moldova în contextul evoluţiei sistemului internaţional şi proceselor integraţioniste", Chişinău, 3 iunie, 2014.

Implementarea rezultatelor ştiinţifice. Rezultatele ştiinţifice pot fi aplicate în procesul de instruire a studenţilor, masteranzilor din cadrul facultăţilor de drept a instituţiilor de învăţământ universitar, precum şi în activitatea practică a organelor de drept.

Publicaţii la tema tezei: 6 lucrări ştiinţifice.

Volumul şi structura tezei: Textul lucrării conţine 177 pagini ce cuprind: introducere; 4

capitole; concluzii generale și recomandări; bibliografia din 221 titluri; declarația privind asumarea răspunderii; CV-ul autorului.

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

CONŢINUTUL TEZEI

În **Introducere** sunt cuprinse importanţa şi actualitatea problemei abordate, scopul şi obiectivele tezei, obiectul cercetării, metodologia cercetării ştiinţifice, noutatea ştiinţifică a rezultatelor obţinute, problema ştiinţifică de importanţă majoră soluţionată prin conţinutul tezei de doctor elaborată, importanţa teoretică şi valoarea aplicativă a lucrării, aprobarea rezultatelor, sumarul compartimentelor tezei de doctor.

În **Capitolul I** ***„Analiza doctrinară a infracţiunii de fraudă informatică”*** se reliefează materialele ştiinţifice publicate la tema tezei de doctor (cursuri, tratate, monografii, studii de sinteză, articole ştiinţifice etc.), în România şi Republica Moldova dar şi în alte state.

Autorul Maxim Dobrinoiu sesizează că divergenţele care există între codurile penale ale statelor în ceea ce priveşte modul de reglementare al criminalităţii informatice se explică, pe de o parte, prin faptul că infracţiunile din domeniul activităţilor informatice nu au fost recunoscute pe plan mondial decât în ultimii ani şi au avut evaluări divergente, iar pe de altă parte, prin nivelul scăzut de dezvoltare al unor state în domeniul criminalităţii informatice şi al sistemelor de telecomunicaţii, nu s-a impus adoptarea reglementărilor în această materie [3, p.77].

Gheorghe Iulian Ioniţă îşi asumă o definiţie proprie considerând criminalitatea informatică ca ansamblul infracţiunilor comise, prin intermediul sau în legătură cu utilizarea sistemelor informatice sau reţelelor de comunicaţii, într-un interval temporar şi spaţial determinat. Sistemul informatic şi reţelele de comunicaţii pot fi instrumentul, ţinta sau locaţia acestor infracțiuni [4].

Ioana Vasiu şi Lucian Vasiu arată că atacurile informatice vizează şi afectează persoane fizice din toate grupurile demografice (bărbaţii şi femeile raportând crime într-o proporţie aproape egală), firme mici şi mijlocii, instanţe de judecată, operatori bursieri, corporaţii globale, organisme guvernamentale, întregi industrii sau chiar ţări întregi. Impactul atacurilor informatice depinde de victimă şi poate consta în pagube financiare mari, încălcarea drepturilor de proprietate intelectuală, contaminarea sau copierea datelor informatice, blocarea accesului la date informatice, repudierea tranzacţiilor sau comunicaţiilor electronice, încetinirea vitezei de procesare a datelor ș.a. [5]

În Republica Moldova, autorii Gheorghe Alecu şi Alexei Barbăneagră fac o paralelă dintre criminalitatea informatică reală şi criminalitatea informatică aparentă, arătând că diferenţa reprezintă cifra neagră a acestui gen de crimă şi ea cuprinde toate acele fapte sancţionate de

legiuitor, dar care, din anumite motive, rămân nedescoperite de către organele abilitate ale justiţiei penale. Dacă în cadrul criminalităţii generale se apreciază că cifra neagră reprezintă un important segment de fapte penale nedescoperite, în cadrul criminalităţii informatice, procentul acesteia tinde tinde să fie în jur de de 90% [6].

Nicolae Ploteanu, Sergiu Maftea, Rodica Griniuc, Angela Coţofană avertizează asupra faptului că uneori, un eveniment care are loc pe un computer sau o reţea este parte a unei serii de paşi ce intenţionează să producă un acces neautorizat [7].

Autorii Sergiu Brînză şi Vitalie Stati apreciază că informaţia stocată nu are nici o valoare în sine. Valoarea ei devine evidentă în momentul în care o foloseşti, sau mai rău, o pierzi prin nefolosirea rapidă şi eficientă. Datorită spaţiului în care se poartă şi legislaţiei precare, războiul infracţional în acest caz implică riscuri mici şi posibile câştiguri mari [8, p.253].

În străinătate, Grainne Kirwan şi Andrew Power analizând printre altele şi conflictele de jurisdicţie încearcă 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 exploratorii acelui spaţiu [9].

John Sammons remarcă că pentru a contracara noile progrese ale criminalisticii în domeniul investigării infracţiunilor informatice, instrumente şi tehnici anticriminalistice apar în număr semnificativ de mare [10].

Felicia Donovan şi Kristin Bernier prezintă mai multe moduri de operare ale hackerilor, între care unele mai noi, realizate prin intermediul telefoniei celulare. 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 telefona şi a corecta situaţia. Când contactezi acel număr, este derulat un mesaj de bun venit care sună autentic, iar apoi eşti îndemnat să relatezi numărul de cont şi parola sau pin-ul [11].

Autoarea Susan W. Brenner reliefează dificultăţile de care se lovesc uneori anchetatorii atunci când infracţiunile cibernetice implică victime într-o ţară şi făptaşi în altă ţară, aceasta deoarece funcţionarii publici însărcinați cu supravegherea aplicării legii nu se pot baza pe procedurile pe care le folosesc de obicei pentru a găsi dovezi și/sau a prinde făptaşii [12].

Franco Barresi şi Michele Nigretti precizează că hackerii se consideră ca fiind un fel de eroi ai vremurilor noastre, cu obiectivul de bază de a elibera orice informaţie şi comunicare de împrejmuirile rigide ale controlului si ale pieţei, pentru posibilitatea ca oricine să aibă acces în mod liber la informaţie, iar dreptul de a fi informat si de a informa să poată fi exercitat în orice moment [13].

Aceste cercetări sunt, mai mult sau mai puţin, sumative, impunându-se în acest spaţiu, o investigație tematică, complexă și aprofundată. Interesul faţă de această temă s-a dovedit a fi unul

deosebit în literatura de specialitate de peste hotare, ceea ce a contribuit esenţial la ridicarea patrimoniului doctrinar în vederea cercetării infracţiunii de fraudă informatică.

Capitolul II „***Fenomenul infracţional în domeniul informatic: definire şi caracterizare”*** este consacrat fenomenului de criminalitate informatică, relevându-se trăsăturile definitorii şi caracteristicile specifice, fraudă informatică fiind poziţionată în contextul apartenenţei sale de criminalitatea informatică în ansamblul ei.

Iniţial, criminalitatea informatică a reprezentat o atitudine teribilistă de sfidare a securităţii reţelelor informatice, treptat ea a devenit un instrument în săvârşirea celor mai grave infracţiuni, dând naştere unei veritabile pieţe negre ale informaţiilor piratate, ale furtului de identitate şi ale violării dreptului de proprietate intelectuală, ale fraudării cardurilor bancare.

Noile categorii de infracţiuni care formează acum un nou tip de criminalitate, sunt comise tot de oameni, tot cu vinovăţie, şi urmărind, de regulă, realizarea unor beneficii patrimoniale.

Infractorii cibernetici eludează limitările fizice care guvernează infracţiunile din lumea reală, aceasta deoarece nu este necesară proximitatea fizică între victimă şi făptaş. Infracţiunea cibernetică este o infracţiune fără limitări, victima şi făptaşul putând fi în oraşe, state sau chiar ţări diferite. Infracţiunea cibernetică este automatizată, iar cu ajutorul automatizării infractorii pot comite mii de infracţiuni cu maximă rapiditate şi minim de efort.

Infracţiunea cibernetică este automatizată, iar cu ajutorul automatizării infractorii pot comite mii de infracţiuni cu maximă rapiditate și minim de efort, și pot obține un profit destul de însemnat cu riscuri mai reduse.

Viteza cu care este săvârşită o infracţiune informatică, volumul datelor sau sumele implicate, distanţa în raport cu locul comiterii infracţiunii sunt elementele care o diferenţiază în comparaţie cu criminalitatea tradiţională. Specific infracţiunilor informatice sunt următoarele caracteristici esenţiale care se transformă în avantaje reale conferite făptuitorilor:

- caracterul transfrontalier - acest fenomen nu ia în considerare graniţele convenţional stabilite;
- anonimitatea - făptuitorul nu trebuie să fie prezent la locul faptei;
- credibilitatea - făptuitorul creează aparenţa unei afaceri legale şi corecte;
- rapiditatea - conferită de transmiterea aproape instantanee a datelor prin sistemele informatice;
- costurile foarte reduse în comparaţie cu beneficiile ce pot fi obţinute.

Într-o accepţiune generală *infracţiunea informatică* ar fi *infracţiune care implică un computer în următoarele moduri*:

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

- computerul ca focalizare a infracţiunii. Aici, computerul este folosit ca ţintă urmărită de activitatea criminală şi nu este neapărat folosit în comiterea actului. Cel mai bun exemplu în acest caz îl constituie individul care intră prin efracţie într-un magazin de computere, după orele de program, cu intenţia de a fura computere şi echipamente conexe;

- computerul ca loc de stocare a dovezilor. Aici, persoana implicată in actul infracţional nu a furat computerul şi nici nu l-a folosit ca mijloc de a comite vreo infracţiune, dar a stocat dovezi pe computer, cum ar fi păstrarea evidenţelor asupra infracţiunilor comise pe hard-disk.

De-a lungul timpului ***hacking-ul*** – o primă modalitate tipică de comitere a infracţiunilor informatice, inclusiv a fraudei informatice - a parcurs patru etape: prima generaţie (anii 1970) ce a fost condusă de nevoia de cunoaştere, a doua generaţie (începutul anilor 1980) a fost determinată de curiozitate şi de nevoia de cunoaştere, iar mai târziu (1985-1990), hacking-ul a devenit o tendinţă; a treia generaţie (anii 1990) a devenit o activitate obişnuită, condusă de curiozitate, stabilind reţele şi schimbând informaţii; a patra generaţie (începând cu anul 2000 şi până în prezent) condusă de dorinţe şi bani, în această etapă hacking-ul întâlnindu-se cu activitatea politică şi cu activitatea criminală.

Următorul 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).

Un alt mod de operare al făptuitorilor este ***phishing-ul*** *(furtul de identitate)*. Furtul de identitate a fost definit ca fiind furtul identității cuiva prin intermediul unei informații de identificare care este apoi utilizata in activitatea de fraudare. Acest termen descrie actele criminale prin care infractorul obţine şi utilizează în mod fraudulos identitatea altei persoane. De cele mai multe ori, furtul de identitate reprezintă o etapă pregătitoare în comiterea infracţiunii de fraudă informatică [14].

Astfel, frauda informatică nu înseamnă doar o nouă titulatură în ceea ce priveşte abordarea fenomenului infracţional în spațiul virtual, or nfractorii digitali, ca de altfel şi faptele comise de aceştia, reprezintă o transformare fundamentală în felul nostru de a aborda problema crimei şi a criminalității.

Capitolul III ***Sediul normativ-preventiv de incriminare a fraudei informatice: reglementări internaţionale şi naţionale*** cuprinde trei secțiuni, în care sunt analizate succesiv asemenea probleme, precum: cadrul juridic internațional în materia incriminării fraudei informatice, elemente de drept penal comparat privind incriminarea fraudei informatice în legislația penală altor state, reglementări antifraudă informatică și locul incriminării fraudei informatice în legea penală a României și Republicii Moldova.

Este o realitate incontestabilă că atât în România cât şi în Republica Moldova, legiuitorul care a incriminat frauda informatică s-a inspirat din **Convenţia Consiliului Europei asupra criminalităţii informatice**, practic reproducând prevederile acestui act. Convenţia Consiliului Europei privind criminalitatea 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 în vedere 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 prevăd măsuri pentru cooperarea internaţională, în Capitolul III.

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.

Tot la nivelul Uniunii Europene, un alt document important îl reprezintă **Directiva 2013/40/UE a Parlamentului European şi a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice** şi de înlocuire a deciziei-cadru 2005/222/JAI a Consiliului [15].

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 Uniunea Europeană 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.

Concluziile desprinse din analiza comparativă a legislaţiilor penale ale diferitor state, aparţinând 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, aparţinând diferitor sisteme de drept, în privinţa infracţiunii de fraudă informatică ne permite să efectuăm o clasificare a acestora, după cum urmează:

1. **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);

2. **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 conținutului constitutiv al fraudei informatice, mai ales în ceea ce ţine de conținutul laurii obiective a infracțiunii, pune în evidenţă o particularitate specifică doar legislației penale a Republicii Moldova comparativ cu legislaţiile penale ale altor state, şi anume consacrarea în structura laturii obiectivă a infracţiunii analizate în calitate de subelement obligatoriu 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. Acest aspect, deloc neglijabil poate fi luat în considerație de către legiuitorul autohton în eventualul proces de perfecționare a normei incriminatorii privitoare la frauda informatică la standardele statelor care fac parte din familia statelor europene.

În cadrul altui compartiment al tezei a fost relevat şi caracterizat sediul normativ aferent legislației României şi a celeia din Republica Moldova, care stă la baza prevenirii fraudei informatice ca fenomen infracţional. O primă precizare care sa impus cu pregnanță este că mecanismul preventiv, cu caracter juridic, în afară de normele incriminatorii, încorporate în legislaţia penală, mai include şi alte legi, care stabilesc măsuri de altă natură necesare prevenirii eficiente a criminalităţii informatice (instituționale, politice, administrative, economice, tehnice etc.).

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 acest proces, fiecare dintre ele asigurînd acoperirea problematicii respective pe segmentul său de activitate. În acest sens, urmează a fi acoperit golul existent, pe segmentul legislativ-normativ, în domeniul asigurării securităţii cibernetice.

Constatăm, că se resimte necesitatea dezvoltării culturii de securitate cibernetică a utilizatorilor sistemelor informatice şi de comunicaţii, adesea aceştia fiind insuficient informaţi în legătură cu potențialele riscuri, amenințări, 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 cibernetică a infrastructurilor naţionale (instituţii publice, reţele de comunicaţii electronice, apeducte, reţele de transport etc.); creşterea gradului de conștientizare 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 legislativ naţional în domeniul securităţii cibernetice; formarea profesională adecvată a persoanelor care îşi desfăşoară activitatea în domeniul securităţii cibernetice etc.

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 stabilirii 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 subsumează relaţiile sociale a căror formare, existenţă şi dezvoltare sunt condiţionate de protejarea raporturilor cu caracter patrimonial. Prin urmare, dintr-o atare abordare legislativă frauda informatică este considerată drept o infracţiune patrimonială săvârşită prin utilizarea sistemelor informatice.

Cu referire la legislaţia penală a R. 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 R. 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 beneficii materiale.

În lumina celor prezentate mai sus se poate concluziona că la baza instituirii 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 informațional, ci cel de a obţine anumite bunuri, beneficii sau drepturi asupra bunurilor. Prin urmare, anume aceasta este raţiunea legiuitorului care incriminează frauda informatică ca infracţiune contra patrimoniului. 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 la 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 abordare deja relaţiile sociale referitoare la protejarea sistemului informaţional prevalează 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.

Capitolul IV, intitulat ***Infracţiunea de fraudă informatică în lega penală a României şi Republicii Moldova,*** înserează în sine patru paragrafe, destinate analizei elementelor şi a subelementelor constitutive ale infracţiunii de fraudă informatică prin prisma normelor incriminatorii din legislaţiile de referinţă, interpretărilor doctrinare şi de practică judiciară.

În conformiatte cu art. 249 C.pen. al României, din punct de vedere al conţinutulu legal, prin fraudă infomatică se are în vedere *introducerea, modificarea sau ştergerea de date informatice, restricţionarea accesului la aceste date ori împiedicarea on orice mod a funcţionării unui sistem informatic, on scopul de a obţine un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane, se pedepseşte cu onchisoarea de la 2 la 7 ani*.

După cum s-a menţionat anterior, în ceea ce priveşte Codul penal al R. 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*. Astfel, prin fraudă informatică se înţelege i*ntroducerea, 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 mar*i [16].

Potrivit art. 126 alin. (1) din C.pen. al R. Moldova *se consideră proporţii mari valoarea bunurilor sustrase, dobândite, 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 hotărârea de Guvern în vigoare la momentul săvârşirii faptei*.

În ceea ce priveşte conţinutul legal al infracţiunii de fraudă informatică, norma incriminatoare este relativ identică cu cea din N.C.pen. român, art.249, singura divergență constând în faptul, că spre deosebire de C.pen. al României, unde nu contează valoarea acestui prejudiciu, suficient fiind să se dovedească faptul că patrimoniul persoanei vătămate a suferit o micşorare ca urmare a faptei comise de făptuitor, în C.pen. al Republicii Moldova este necesară cauzarea de daune în proporţii

mari [17].

Deci, în cazul fraudei informatice, Codul penal al R. Moldova cere ca în momentul săvârşirii infracţiunii valoarea pagubei să depăşească 20 de salarii medii lunare pe economie prognozate, stabilite prin Hotărârea de Guvern în vigoare la momentul săvârşirii 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 privind criminalitatea informatică.

În legătură cu textele normative comparate s-au făcut două constatări de bază.

În primul rând, deşi similitudinea textelor normative dedicate incriminării şi pedepsirii fraudei informatice în legislaţia penală a R. Moldova şi a României este una vizibilă, aprecierea gradului prejudiciabil sau a pericolului social al faptei în legislaţiile penale de referinţă este diferit.

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 Hotărârea de Guvern în vigoare la momentul săvârşirii faptei.

Cea de a doua constatare ţine de aprecierea naturii juridice a fraudei informatice în raport cu alte infracţiuni, precum ar fi, de exemplu, sustragerea de bunuri, mai ales cea comisă prin escrocherie.

În acest sens a fost acceptat şi promovat 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. 260^6 C.pen. reprezintă o normă specială în raport cu cea de la art. 190 şi 196 C.pen. În consecinţă, aplicarea alin. (1) art. 260^6 C.pen. exclude reţinerea, la încadrare, a uneia dintre infracţiunile prevăzute la art. 190 sau 196 C.pen. [8, p.139].

Deşi ne-am solidarizat cu această opinie, au fost făcute două precizări referitoare la natura juridică a 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 soluţie calificativă rezultă mai mult din substanţa lucrurilor, necunoscând,

totodată, şi o consacrare legală.

În al doilea rând, regimul sancţionator al infracţiunii de escrocherie este cu 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 Hotărârea de Guvern în vigoare la momentul săvârşirii 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 [18].

De *lege lata* nu se pare a fi 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, s-a propus textul 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 în raport cu frauda informatică comisă prin cauzarea de daune materiale sau abuz de încredere, iar pe de altă parte, 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 calificat persoana juridică în calitate de subiect activ al fraudei informatice.

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 [19, p.576].

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.

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 ce serveşte anumite funcţii sau obiective. Pe de altă parte, dintr-o perspectivă funcţională, un sistem informatic 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 [20, 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, procedură 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 funcţii 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 dispozitive portabile utilizate ca mediu de stocare a informaţiei (memory stick) etc.

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 [21, 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.

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 [22, p.44-48].

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.

Ştergerea 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.

Urmarea imediată în cazul reglementării din C.pen. al României 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 în momentul săvârşirii infracţiunii valorii pagubei să depăşească echivalentul 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

cauze (spre exemplu, căderi temporare de tensiune), şi nu a activităţii descrise de legiuitorul penal, ea nu constituie urmarea imediată a acestei acţiuni, lipsind legătura de cauzalitate.

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.

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.

CONCLUZII GENERALE ŞI 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 obținerii de rezultate concrete 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 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 beneficii 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 prevalează 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 incriminării 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 săvârșire 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) săvârşite 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 până 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 până 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 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. https://www.cert-ro.eu/ (vizitat la 11.05.2016);
2. sputnik.md/world/20160311/5164998.html (vizitat la 06.04.2016);
3. Maxim Dobrinoiu, *Infracțiuni în domeniul informatic*, Ed. C.H. Beck, București, 2006, p. 77;
4. Gheorghe Iulian Ioniță, *Infracțiunile din sfera criminalității informatice*, Ed. Pro Universitaria, București, 2013, p. 50;
5. Ioana Vasiu, Lucian Vasiu, *Criminalitatea în cyberspațiu*, Ed. Universul Juridic, București, 2011, p. 13-14;
6. Gheorghe Alecu, Alexei Barbăneagră, *Reglementarea penală și investigarea criminalistică a infracțiunilor din domeniul informatic*, Ed. Pinguin Book, București, 2006, p. 20.
7. Nicolae Ploteanu, Sergiu Maftea, Rodica Griniuc, Angela Coțofană, *Pasul II în ciberspațiu: Securitatea Informațională*, Academia MAI ”Ștefan cel Mare”, Tipografia ”Elena VI” Chișinău 2008, p. 16;
8. Sergiu Brînză, Vitalie Stati, *Drept penal. Partea specială*, vol. II, Tipografia Centrală, Chișinău, 2011, p. 253;
9. Grainne Kirwan, Andrew Power, *Cybercrime. The Psichology of Online Offenders*, Cambridge Universidy Press, 2013, p. 32;
10. John Sammons, *The basics of digital forensics*, Syngress, Waltham, Massachusetts, 2012, p. 81;
11. Felicia Donovan, Kristyn Bernier, *Cyber Crime Fighters: Tales from the trenches*, QUE, Indianapolis, Indiana, 2009, p. 183;
12. Susan W. Brenner. *Cybercrime: Criminal threats from cyberspace*, ABC-CLIO, Santa Barbara, California, 2010, p. 141;
13. Francesco Baressi, Michele Nigretti, *Fenomeno hacking: analisi sociocriminalistica dell intrusione informatica*, Iris 4 Edizioni, Roma, 2012, p. 99.
14. Robert Moore, *Cybercrime-investigating high-technology computer crime, second edition*, Anderson Publishing, Oxford, 2011, p. 27;
15. 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 Europei. https://www.data.consilium.europa.eu/doc/document/PE-38-2012-REV-1/ro/pdf (vizitat la 11.08.2015).
16. Codul penal al Republicii Moldova, în M. Of. nr. 72-74 din 14.04.2009, art. nr. 195;
17. Drăgan A. T., *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;

18. Victor-Valeriu Patriciu, Ioana Vasiu, Șerban George Patriciu, *Internetul şi dreptul*, Ed. All Beck Bucureşti, 1999, p.9.
19. 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, Chişinău, 2009, p. 567;
20. 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, p. 841;
21. Ioana Vasiu, Lucian Vasiu. *Informatica juridică și drept informatic*. Ed. Albastră, Cluj-Napoca, 2009, p. 144;
22. Drăgan A. T. *Falsul informatic în viziunea Noului Cod penal Român şi a Codului penal al Republicii Moldova*. În: Revista Națională de Drept, nr. 1, 2015. p. 44-48.
23. Карабаналов С.С., *Компьютерное мошенничество при торговле ценными бумагами с использованием сети Интернет в США* // http://skyglobe.ru (accesat la 12.10.2016);

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 perfecţionarea 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 a 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.

Keywords: 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.

DRĂGAN Alin Teodorus

Frauda informatică: analiza juridico-penală a infracţiunii

Specialitatea: 554.01 – Drept penal şi execuţional penal

Autoreferatul tezei de doctor în drept

Hârtie ofset. Tipar ofset. Formatul hârtiei 60x84 1/16
Coli de tipar: 1,0 Tirajul: 60 ex.

Institutul de Cercetări Juridice şi Politice al AŞM
Mun. Chişinău, bd. Ştefan cel Mare, 1, MD 2001