UNIVERSITATEA ECOLOGICĂ DIN BUCUREŞTI

FACULTATEA DE DREPT

Program de studii universitare de masterat

DREPTUL INFORMAȚIILOR ȘI AL SECURITĂȚII PRIVATE

Forma de învăţământ: învăţământ cu frecvenţă

PREVENIRE ȘI COMBATEREA CRIMINALITĂȚII INFORMATICE

- Suport de curs -

Titular de disciplină:
Prof. univ. dr. Emil STAN

Bucureşti

Introducere

Cursul este destinat studenţilor din cadrul programului de studii universitare de masterat Dreptul informațiilor și al securității private din cadrul Facutății de Drept – Universitatea Ecologică din București.

a. Date privind titularul de disciplină

Nume şi prenume:	Prof. univ. dr. Stan Emil
E-mail:	emil.stan@ueb.education

b. Date despre disciplină

Anul de studiu:	I
Semestrul:	2

c. Obiectivele disciplinei

Obiectivul general al disciplinei	Cunoaşterea, înţelegerea şi aprofundarea instituţiilor specifice criminalităţii informatice, precum şi a jurisprudenţei relevante în materie, în scopul creşterii securităţii în faţa atacurilor informatice.
Obiectivele specifice	Sistematizarea cunoştinţelor dobândite ca urmare a prelegerilor susţinute; Aprofundarea celor mai importante noţiuni şi concepte în domeniu; Verificarea nivelului de cunoştinţe dobândite de către masteranzi atât prin participarea la cursuri/seminarii, cât şi prin studiu individual.

d. Competenţe acumulate după parcurgerea cursului

Competenţe profesionale	Cunoaşterea, înţelegerea şi utilizarea noţiunilor, a principalelor metode şi tehnici privind prevenirea, detectarea, investigarea şi combaterea infracţiunilor informatice; Interpretarea şi explicarea legislaţiei internaţionale, regionale şi naţionale care incriminează criminalitatea informatică; Cunoaşterea posibilităţilor pe care le oferă internetul şi IT-ul în domenii precum comerţul electronic, internet banking, documentarea asistată; Aplicarea legislaţiei care reglementează diferite forme de manifestare ale criminalităţii informatice; Acordarea asistenţei sau consultanţei de specialitate referitoare la evitarea riscurilor ale sistemelor informatice; Formularea unor propuneri de lege ferenda privind modificarea, completarea sau perfecţionarea legislaţiei în materia criminalităţii informatice.
Competenţe transversale	Utilizarea eficientă a surselor informaţionale atât în limba română, cât şi într-o limbă de circulaţie internaţională; Dobândirea unor abilităţi de lucru şi comunicare în echipă, facilitând rezolvarea unor probleme specifice domeniului şi luare unor decizii, precum şi implicarea în alte activităţi.

e. Resurse şi mijloace de lucru

Pentru o pregătire temeinică vă sugerăm să consultaţi bibliografia recomandată.

f. Structura cursului

Cursul Prevenirea și combaterea criminalității informatice este structurat pe capitole, așa cum rezultă din cuprins și poate fi studiat atât în întregime, potrivit ordinii prestabilite a capitolelor, dar se poate şi fragmenta în funcţie de interesul propriu mai accentuat pentru anumite teme. Însă, în vederea susţinerii examenului este obligatorie parcurgerea tuturor capitolelor.

g. Evaluarea

Înainte de examen este indicat să parcurgeţi din nou toată materia, cu atenţie, durata estimată pentru această activitate fiind de aproximativ o săptămână.

Tip activitate	10.1.Criterii de evaluare	10.2. Metode de evaluare	10.3. Pondere din nota finală
10.4. Curs	Prezenţa la minim 40% la orele alocate cursului. Un test de evaluare a cunoştinţelor.	Verificarea prezenţei. Punctaj acordat testului de evaluare a cunoştinţelor.	20%
10.5. Seminar/ laborator/ lucrări practice / proiect	Prezenţa la minim 60% din orele alocate seminarului. Două referate cu studiu de caz şi atitudine participativă.	Verificarea prezenţei. Susţinerea referatelor şi acordarea unui punctaj pentru implicarea în desfăşurarea seminarului.	40 %
10.6. Evaluare finală	Nivelul de înţelegere şi capacitatea de explicare şi interpretare a aspectelor teoretice şi practice în materia protecţiei drepturilor omului.	Examen scris	40 %
10.7. Modalitatea de notare (calificativ sau notă): Notă de la 1 la 10.			
10.8 Standard minim de performanţă: Elaborarea şi prezentarea unui referat, urmărindu-se acurateţea ideilor prezentate în susţinerea acestuia.			

CUPRINS

INTRODUCERE

Valorile, principiile şi normele pe care comunitatea europeană le promovează şi le susţine este necesar a fi aplicate şi în **mediul online**, pentru ca Internetul să rămână liber şi deschis. Drepturile fundamentale ale cetăţenilor, democraţiei şi ale statului de drept trebuie să fie protejate şi în mediul DIGITAL.

Libertatea Internetului necesită siguranţă şi securitate. Internetul ar trebui să fie protejat de activităţile cu intenţii răuvoitoare, abuzuri şi incidente. Pentru realizarea acestor deziderate, *guvernele* tuturor statelor au un rol important în asigurarea unui spaţiu cibernetic liber şi de impunere a condiţiilor de siguranţă.

Pe lângă toate acestea, guvernele au sarcina de a proteja accesul şi de a respecta **drepturile fundamentale online**, de a menţine fiabilitatea şi interoperabilitatea internetului.

Totusi, *sectorul privat* deţine şi operează segmente semnificative din Internet. Insa, orice iniţiativă trebuie să recunoască rolul de lider al statului în domeniul securităţii informatice, chiar dacă scopul acestuia este in principal de crea cadrul legislativ necesar desfăşurării activităţilor în acest spaţiu.

Comunicaţiile şi tehnologia informaţiei au devenit coloana vertebrală a creşterii noastre economice. Acestea constituie o **resursă esenţială** pe care toate sectoarele economice se bazează. Baza sistemelor complexe care păstrează economiile noastre, funcţionarea sectoarelor cheie, cum ar fi finanţele, sănătatea, energia şi transportul, multe modele de afaceri sunt construite pe disponibilitatea neîntreruptă dată de internet şi de buna funcţionare a sistemelor de informare.

În ultimii ani s-a observat că în timp ce **lumea digitală** aduce beneficii enorme, ea este, de asemenea, vulnerabilă. Incidentele din Internet, fie intenţionate, fie accidentale, sunt în creştere la un nivel alarmant şi ar putea perturba furnizarea de

servicii esenţiale, cum ar fi cele de apă, sănătate, energie electrică sau serviciile de telefonie mobilă. Ameninţări ce pot avea origini diferite, inclusiv penale, motivate politic, atacuri teroriste sau sponsorizate de state, precum si fel de fel de dezastre naturale sau greşeli neintenţionate se constituie in amenintari reale, care trebuie prevenite si combatute.

Economia statelor este deja afectată, în proporţii diferite, de activităţile de criminalitate informatică îndreptate împotriva persoanelor fizice şi a sectarelor publice şi private. **Infractorii din mediul virtual** folosesc metode din ce în ce mai complexe pentru pătrunderea în sistemele informatice, avand scopuri diverse cum ar fi furtul de date critice, urmat de cereri de răscumpărari.

Creşterea spionajului economic si militar reprezintă o nouă categorie de ameninţări pentru guvernele şi companiile din întreaga lume. Guvernele ar putea abuza, de asemenea de spaţiul virtual pentru supravegherea şi controlul propriilor lor cetăţeni.

Uniunea Europeana poate contracara această situaţie prin promovarea libertăţii online şi asigurarea respectării drepturilor fundamentale în mediul cibernetic. Toţi aceşti factori explică de ce guvernele din întreaga lume au început să dezvolte strategii proprii de securitate cibernetică şi să ia în considerare Internetul ca o problemă internaţională din ce în ce mai importantă.

A sosit timpul ca Uniunea Europeană să-şi intensifice acţiunile în acest domeniu, în vederea elaborării unei strategii de **securitate cibernetică** a mediului virtual, care să prezinte viziunea sa în acest domeniu, clarificând rolurile şi responsabilităţile statelor membre şi stabilind acţiunile viitoare necesare, bazate pe o protecţie puternică şi eficientă şi pe promovarea drepturilor şi libertăţilor cetăţenilor, care să facă din mediul online al Uniunii Europene cel mai sigur spaţiu cibernetic din lume.

Securitatea în mediul cibernetic a devenit o componentă a securităţii tuturor statelor, care potrivit convenţiilor şi tratatelor internaţionale se poate realiza prin,

cunoaşterea, prevenirea şi contracararea atacurilor şi ameninţărilor, precum şi prin diminuarea vulnerabilităţilor infrastructurilor cibernetice.

Toate acestea sunt luate în scopul gestionării eficiente a tuturor riscurilor la adresa securităţii statelor, pentru prevenirea şi combaterea criminalităţii informatice şi nu în ultimul rând in scopul apărarii cibernetice.

Date fiind premisele şi efectele fenomenului în discuţie, in continuare vom efectua o analiza a fenomenului în toata complexitatea sa, în vederea realizării, la finalul cercertării, a unui set de **cai de actiune menit să prevină şi să limiteze criminalitatea informatică**.

Dintre toate ameninţările sfârşitului de secol XX si inceput de secol XXI, putem afirma că fenomenul criminalităţii informatice este cel care progresează cu paşii cei mai semnificativi, evoluând prin sine însuşi în forme din ce în ce mai surprinzătoare, dar servind şi ca **modus operand**i pentru alte tipuri de infracţiuni, ca pornografia infantilă sau furtul de identitate. Internetul, ca instrument principal al criminalităţii informatice, prezintă o infinitate de utilizări, ceea ce duce în mod inevitabil la diversificarea formelor de manifestare a fenomenului. Astfel, apare ca o necesitate realizarea de cercetări la zi, care să conveargă spre o radiografie cât mai exactă şi actuală a dimensunilor acestui tip de criminalitate, cu o structură clară, documentată şi cu propuneri viabile pe un termen cât mai îndelungat.

CAPITOLUL I. NOŢIUNI GENERALE

Prevenirea şi combaterea infractionalitatii informatice sunt concepte complexe şi pluridisciplinare care comportă **abordări multidisciplinare** atat conceptuale, cat şi operaţionale, din perspectivă socială, juridică, politică, criminologică, filozofică, logico-sistemică, etică etc.

Criminalitatea sau infracţionalitatea reprezintă o formă particulară a devianţei sociale, acest fenomen afectând relaţiile interumane cu efect negativ asupra ordinii publie şi a comunităţilor de persoane, violând valorile sociale caracteristice unei societăţi şi nu numai.

În prezent în România, fenomenul criminalităţii informatice se manifestă – în principal – în următoarele domenii:

- infracţiuni privitoare la comerţul electronic – sunt reprezentate (în principiu) de achiziţionarea de bunuri sau de servicii prin Internet (acestea fiind plătite cu ajutorul unor mijloace de plată electronică, folosite în mod fraudulos), precum şi oferirea spre vânzare prin Internet, a unor bunuri (unicul scop fiind acela de a înşela eventualul cumpărător);

- infracţiuni privitoare la sistemele informatice – sunt reprezentate de atacurile împotriva sistemelor informatice, atacuri ce pot urmări perturbarea bunei funcţionări a unui sistem informatic;

- pornografia infantilă prin sisteme informatice. Internetul şi în general noua tehnologie asigură infractorilor o cale deosebit de uşoară şi rapidă pentru racolarea de persoane, indiferent de vârstă, producerea şi răspândirea de imagini cu caracter pornografic, în unele dintre ele fiind implicaţi minori.

La nivel internaţional/regional nu se manifestă un consens în ceea ce privește terminologia fenomenului; sunt folosiţi (alternativ) o serie de termeni pentru a descrie infracţiunile comise prin intermediul/asupra calculatoarelor - „criminalitate în legătură cu (utilizarea) calculatorul (ui)” (“computer-related crime”), “criminalitate

informatică” (“cyber crime”), “criminalitatea de înaltă tehnologie” (“high-tech crime”), “criminalitate electronică” (“electronic crime”, “e-crime”).

Plecând de la definiția criminalității, dar adaptând-o particularităţilor proprii acestei forme de manifestare a criminalităţii, s-a considerat ca fiind criminalitatea informatică, ansamblul infracţiunilor comise, prin intermediul sau în legătură cu utilizarea sistemelor informatice sau reţelelor de comunicaţii. **Sistemele informatice și reţelele de comunicaţii** pot fi instrumentul, ţinta sau locaţia acestor infracţiuni.

Uşurinţa în utilizare, costul scăzut, rapiditatea şi asigurarea unui caracter anonim fac din Internet un mediu propice infracţiunilor. Datorită caracterului global al reţelei şi uriaşei complexităţi, posibilităţile „de **ascundere**” ale autorului sunt practic nelimitate, încurajând şi din acest motiv săvârşirea de infracţiuni.

Dezvoltarea tehnologiilor informaţionale a sporit considerabil eficienţa afacerilor în cele mai diferite sfere de activitate (economie, medicină, drept etc.). Reţelele de telecomunicaţii permit efectuarea tranzacţiilor în regim real de timp, viteza de procesare a sporit considerabil, iar companiile sunt capabile să păstreze şi să prelucreze masive enorme de date. Însă, pe lângă aspectele pozitive, a apărut un şir de fenomene negative – infracţiunile informatice, adică realizarea unor acţiuni directe sau indirecte, fizice sau logice, premeditate sau nepremeditate, ce au scop modificarea uneia sau mai multor stări (**confidenţialitate, integritate, accesibilitate, non-repudiere**) ale unui sistem sau subistem informaţional.

Acest fapt a dus la apariţia unei noi ramuri a dreptului, care necesită elaborarea concepţiei de infracţiune informatică, definirea noţiunii şi elucidarea tipurilor infracţiunilor, clasificarea lor şi stabilirea măsurilor de constrângere, elaborarea metodelor, tehnicilor şi metodologiilor de cercetare a infracţiunilor şi, nu în ultimul rând, elaborarea programelor de studiu pentru pregătirea specialiştilor în domeniu.

Dezvoltarea fără precedent în domeniul tehnologiei informatice, la nivel mondial, are, din păcate, o parte negativă:

S-a deschis o poartă către producerea unor fapte antisociale, "criminale", penalizate atât în dreptul internaţional penal, cât şi în rapoartele prezentate de specialişti din IT, fapte care nu ar fi putut exista în condiţiile tehnice existente acum 15 ani, de exemplu. Sistemele de calculatoare oferă, în prezent, **oportunităţi noi**, unele chiar sofisticate, de încălcare a legilor şi creează un potenţial ridicat de comitere a unor tipuri de infracţiuni realizate altfel decât în modurile cunoscute, tradiţionale.

Deşi societatea, în ansamblul ei, plăteşte pentru toate daunele economice cauzate de "criminalitatea informatică", aceasta continuă să se bazeze pe sistemele computerizate în aproape toate domeniile vieţii sociale: controlul traficului aerian, al trenurilor şi metrourilor, coordonarea serviciului medical sau al securităţii naţionale.

Dezvoltarea fără precedent a tehnologiei informaţiei (IT) şi pătrunderea acesteia în toate sectoarele de activitate, a determinat schimbări majore în societate.

Astfel s-a impus stabilirea de **norme juridice** apte să răspundă necesităţii de a menţine preocupările comunităţii internaţionale de **a preveni si a lupta împotriva criminalităţii informatice**. Cu prioritate trebuie raspuns necesitatii de a stabili

1. faptele care trebuie să fie incriminate în legislaţiile naţionale,
2. normele procedurale aplicabile în domeniul criminalităţii informatice
3. mijloacele de cooperare internaţională rapidă, care sunt impuse de specificul infracţiunilor săvârşite prin intermediul sistemelor informatice.

Toate acestea au fost concretizate în Convenţia europeană privind criminalitatea informatică, semnată de România la 23 noiembrie 2001. Convenția privind criminalitatea informatică impune statelor membre adoptarea unei legislații penale care să include reglemetări specifice acestui domeniu. În România, cele mai importante reglementări juridice în materie de criminalitate informatică au fost prevăzute în Legea nr.161/2003 privind unele măsuri pentru asigurarea transparenţei şi exercitarea demnităţilor publice, a funcţiilor publice şi mediul de afaceri, prevenirea şi sancţionarea corupţiei. 4 EXPUNERE DE MOTIVE la Legea privind

unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei.

CAPITOLUL II. PRINCIPALELE INFRACŢIUNI DIN SFERA CRIMINALITĂŢII INFORMATICE

Sancţiunile referitoare la faptele de criminalitate informatică sunt prevăzute în noul Cod Penal art.249 „Frauda informatică”, art.360-364, infracţiunile „Accesul ilegal la un sistem informatic”, „Interceptarea ilegală a unei transmisii de date informatice”, „Alterarea integrităţii datelor informatice”, Perturbarea funcţionării sistemelor informatice”, „Transferul neautorizat de date informatice”, iar infracţiunea de „Pornografie infantilă prin intermediul sistemelor informatice” este prevăzută în art. 374.

Prin “sistem informatic” se înţelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic. Prin “program informatic” se înţelege un ansamblu de instrucţiuni care pot fi executate de un sistem informatic în vederea obţinerii unui rezultat determinat. Prin “date informatice” se înţelege orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. Prin “măsuri de securitate” se înţelege folosirea unor proceduri, dispozitive sau programe informatice specializate, cu ajutorul cărora accesul la un sistem informatic este restricţionat sau interzis pentru anumite categorii de utilizatori.

Următoarele infracţiuni sunt cele mai des intalnite:

Accesul ilegal la un sistem informatic,

Interceptarea ilegală a unei transmisii de date informatice,

Alterarea integrităţii datelor informatice,

Perturbarea funcţionării sistemelor informatice,

Transferul neautorizat de date informatice,

Operaţiuni ilegale cu dispozitive sau programe informatice,

Falsul informatic,

Frauda informatică

Pornografia infantilă,

conform reglementărilor din Noul Cod Penal.

Conservarea imediată a datelor informatice se dispune de procurorul care supraveghează sau efectuează urmărirea penală, din oficiu sau la cererea organului de cercetare penală, pe o durată de maximum 60 de zile, prin ordonanţă, dacă sunt îndeplinite cumulativ următoarele condiţii:

-există o suspiciune rezonabilă cu privire la pregătirea sau săvârşirea unei infracţiuni;

-măsura este necesară în scopul strângerii de probe ori identificării făptuitorului , suspectului sau a inculpatului;

-datele informatice, inclusive datele referitoare la traficul informaţional, au fost stocate prin intermediul unui sistem informatic;

-aceste date se află în posesia sau sub controlul unui furnizor de servicii de comunicaţii electronice destinate publicului;

-există pericolul pierderii sau modificării acestora.

Conform Noului Cod de Procedură Penală, organele judiciare (organele de urmărire penală sau instanța) au obligația de a ridica obiectele și înscrisurile ce pot servi ca mijloc de probă în procesul penal.

Conform art. 168 alin. (1) NCPP, prin percheziţie în sistem informatic sau a unui suport de stocare a datelor informatice se înţelege procedeul de cercetare, descoperire, identificare şi strângere a probelor stocate într-un sistem informatic sau suport de stocare a datelor informatice, realizat prin intermediul unor mijloace tehnice şi proceduri adecvate, de natură să asigure integritatea informaţiilor conţinute de acestea. În cursul urmăririi penale, competenţa şi procedura de soluţionare a cererii de autorizare a percheziţiei informatice este identică cu cea referitoare la percheziţia domiciliară.

CAPITOLUL III. PRINCIPALII FACTORI CARE INFLUENŢEAZĂ DEZVOLTAREA CRIMINALITĂŢII INFORMATICE

Chiar dacă nu ne place să recunoaștem, depindem din ce în ce mai mult de tehnologia informației și comunicațiilor (ICT). Astfel, comunicațiile zilnice, controlul și gestionarea funcționalităților în clădiri, transportul (aerian, feroviar, naval, etc.), furnizarea de energie, apă, etc. Depind de tehnologia informației și comunicațiilor iar integrarea continuă a tehnologiei informației și comunicațiilor în viața de zi cu zi este posibil să continue și să dobândească valențe noi.

Popularitatea Internetului și a serviciilor sale, este în continuă ascensiune, depășind 2,5 miliarde de utilizatori (în prezent). Dar, odată cu creșterea numărului de utilizatori conectați la Internet, a crescut și numărul potențialelor ținte și infractori. Este dificil de estimat cât de mulți oameni folosesc Internetul pentru activități ilegale. Chair dacă numai 0,1% din utilizatori ar comite infracțiuni, numărul total al infractorilor ar depăși 1,5 milioane.

Comiterea infracțiunilor din sfera criminalității informatice este relativ ușoară, fiind necesare echipamente (hardware), programe de utilizare a echipamentelor (software) și acces la Internet.

Internetul conține, în prezent, aproape 940 milioane de pagini **web** de informații, la zi. Un infractor care plănuiește un atac poate găsi informații detaliate pe Internet, de la cum să construiască o bombă folosind substanțe și produse comerializate liber, până la planurile unei clădiri sau ale unei rețele de utilități. Deși astfel de informații erau disponibile chiar înainte de dezvoltarea Internetului, accesul la aceste informații era (oricum) mult mai greu de obținut.

Toate rețelele de comunicare în masă, de la rețelele de telefonie utilizate pentru apeluri de voce, la Internet, au nevoie de administrare centrală și standarde tehnice pentru a asigura operabilitatea. Internetul trebuie de asemenea, să fie guvernat de legi și leguitori iar organele de aplicare a legii ai început să se dezvolte standarde legale car neceită un anumit grad de control central.

Multe procese de transfer de date pot dobândi caracter transnațional datorită faptului că protocoalele utilizate pentru transferurile de date pe Internet se bazează pe o dirijare optimă dacă legăturile directe sunt temporar blocate.

Pentru comiterea infracțiunilor, infractorii nu trebuie să fie prezenți în aceeași locație cu ținta. Aceesul la Internet le permite comiterea infracțiunilor de aproape oriunde în lume.

Una dintre cele mai mari avantaje ale tehnologiei informației și comunicațiilor este abilitateade a automatiza anumite procese, automatizare care are multe consecințe majore: mărește viteza proceselor, crește amploarea și impactul proceselor, limitează implicarea oamenilor.

Nu doar o creștere a puterii calculatoarelor folosite de un singur utilizator este singura caracteristică care ridică probleme pentru investigații; în aceiași măsură, creșterea capacităților rețelei poate ridica probleme majore.

Trimiterea unui mesaj de poștă electronica oriunde în lume durează doar câteva secunde. Acest transfer rapid lasă foarte puțin timp organelor de aplicare a legii pentru a cerceta infracțiunea sau pentru a colecta probele.

Internetul este într-o continuă dezvoltare. Începutul extinderii sale dramatice a fost marcat de creșterea unei **interfețe de utilizator grafice** (www) "prietenoasă" și ușor accesibilă. Crearea acestei interfețe (www) a permis dezvoltarea de noi aplicații, dar și de noi infracțiuni.

Anumite servicii Internet fac dificilă identificarea infractorilor. Posibilitatea comunicațiilor anonime este un produs/serviciu oferit cu intenția de a evita dezavantajele de utilizator; exemple de astfel de servicii: terminale publice de Internet (la aeroporturi, cafenele Internet), rețele fără fir, servicii detelefonie mobilă preplătite care nu necesită înregistrare, capaciățile de stocare oferite de pagini web fără înregistrare,sisteme tip server de comunicații anonime, retransmițători anonimi.

Un alt factor care poate complica investigarea criminalității informatice, dar care constituie soluția tehnică cheie în lupta împotriva criminalității informatice, este

tehnologia de criptare. Folosind criptarea, se reușește protejarea informațiilor împotriva accesului persoanelor neautorizate.

CAPITOLUL IV. CRIMINALITATEA INFORMATICĂ ŞI CRIMINALITATEA ORGANIZATĂ

Modul de operare care implică mai multe persoane putem afirma că este specific infracţiunilor din sfera criminalităţii informatice. În grupurile de infractori formate, fiecare membru are rolul său bine definit, grupul conlucrând pentru scopul final, respective obţinerea de bani sau alte foloase în mod illicit.

Un aspect-cheie subliniat în SOCTA UE 2017 este utilizarea de noi tehnologii de către infractori. Pentru aproape toate tipurile de criminalitate organizată, infractorii utilizează și adaptează, cu o abilitate din ce în ce mai mare, tehnologii al căror impact este tot mai important. Se constată o utilizare mult mai mare a internetului pentru toate tipurile de comerț ilicit cu bunuri și servicii. Aceasta impune ca autoritățile de aplicare a legii să dispună de instrumente adecvate pentru a combate acest tip de infracțiuni online și să se instruiască și să învețe împreună. Agenția Uniunii Europene pentru formare în materie de aplicare a legii joacă un rol esențial în asigurarea unei formări adecvate, în conformitate cu prioritățile de politică și amenințările identificate, pentru agenții de aplicare a legii din prima linie.

Prin însăși natura sa, criminalitatea informatică este internațională: victimele, infractorii și probele sunt adesea situate în țări diferite, fiind sub mai multe jurisdicții. Statele membre au arătat un interes deosebit pentru prioritatea pe care o constituie criminalitatea informatică, astfel cum o demonstrează numărul de planuri operaționale de acțiune instituite în domeniile atacurilor cibernetice, exploatării sexuale online a copiilor și fraudării cardurilor de plată.

CAPITOLUL V. IMPACTUL CRIMINALITĂȚII INFORMATICE ASUPRA ORDINII PUBLICE ȘI SIGURANȚEI NAȚIONALE

Spre exemplu, fortele de politie internationale au destructurat o grupare de romani care sunt acuzati ca stau in spatele a ceea ce oficialitatile au numit cea mai mare frauda cu carduri bancare din Australia, de la nivelul anului 2018. Un număr de şapte persoane din România au fost acuzate de furt informatic de pe 30.000 de carduri de credit australiene, potrivit politiştilor din acest stat. Fără cooperarea altor 13 state, împreună cu sectorul bancar al Australiei, nu am fi fost posibilă depistarea acestor tranzacţii ilegale în reţelele infracţionale din România. Informaţiile furate erau utilizate pentru a se crea carduri de credit false, folosite pentru retrageri frauduloase in Australia, Hong Kong, Europa si SUA.

Astfel cum am arătat şi anterior, caracterul pregnant transfrontalier, face ca linia dintre criminalitatea informatică de la nivel naţional şi cea de la nivel internaţional să fie foarte fină. Nu de puţine ori, cetăţeni români orchestrează reţele de crimă roganizată în alte state decât România, pentru a obţine foloase materiale în mod nelegal. Spre exemplu, **fortele de politie internationale** au destructurat o grupare de romani care sunt acuzati ca stau in spatele a ceea ce oficialitatile au numit cea mai mare frauda cu carduri bancare din Australia, de la nivelul anului 2018. Un număr de şapte persoane din România au fost acuzate de furt informatic de pe 30.000 de carduri de credit australiene, potrivit politiştilor din acest stat.

La data de 14 martie 2018, Comisia Europeană a definit o serie de acțiuni menite să combată în întreaga Uniune Europeană practicile comerciale agresive, cum ar fi falsele oferte „gratuite”, publicitatea de tip „capcană și deturnare” la produse care nu pot fi furnizate și îndemnurile adresate copiilor. La cinci ani de la intrarea în vigoare a Directivei privind practicile comerciale neloiale, Comisia a reexaminat aplicarea acesteia și a anunțat măsuri de intensificare a procesului de asigurare a respectării normelor, în vederea sporirii încrederii cetățenilor atunci când fac cumpărături pe piața internă a Europei.

Deşi este considerat mai degrabă un concept decât o realitate, **terorismul informatic** suscită din ce în ce mai mult interesul deopotrivă al mass-media şi al cercurilor guvernamentale. Studii in domeniu relevă faptul că pericolul există, însă se cunosc prea puţine informaţii despre fenomen sau sunt prea puţin conturate limitele acestuia. Ce este, însă, terorismul informatic? În prezent, atât în mediile academice, cât şi în cele circumscrise securităţii IT, există foarte multe definiţii, multe dintre acestea încercând un paralelism cu definiţia clasică a terorismului, respectiv totalitatea actelor intenționate de violență comise de un grup sau de o organizație pentru a provoca o teamă generalizată și pentru atingerea unor scopuri politice. În esenţă, potrivit definiţiei Biroului Federal de Investigatii al S.U.A. (FBI) avem de-a face cu "un atac premeditat, motivat politic, impotriva informatiilor, sistemelor de calculatoare, programelor si operarilor de date, ce conduce la violente impotriva obiectivelor civile si necombatantilor, atac exercitat de grupari subnaţionale sau agenţi clandestini".

În vederea studierii impactului pe care fenomenul criminalităţii informatice îl are asupra ordinii publice, în cadrul realizării prezentei teze am considerat utilă aplicarea unui chestionar la nivelul utilizatorilor de internet precum şi al posesorilor de card-uri de debit ori credit, având în vedere împrejurarea că şi aceste persoane pot deveni victime ale făptuitorilor care actionează pe Internet.

În acest sens, au fost chestionate un număr de 45 de persoane, cu vârste cuprinse între 20 şi 50 de ani, din mediul urban, care au abilitatea de a utiliza internetul şi care sunt deţinătoare de card-uri, considerând că aceste persoane prezintă cel mai însemnat potenţial de a deveni victime ale fenomenului în discuţie. Concluziile care se desprind ca urmare a adimistrării acestui **chestionar** se leagă de împrejurarea că utilizatorii români din mediul urban manifestă încă o reticenţă faţă de achiziţiile online şi deţin suficiente cunoştinţe despre mediul virtual încât să nu deschidă mesaje care par a nu avea legătură cu ei, ca destinatari.

CAPITOLUL VI. COOPERAREA INSTITUŢIONALĂ ÎN PREVENIREA ŞI COMBATEREA CRIMINALITĂŢII INFORMATICE

Pe linia prevenirii şi combaterii infracţiunilor din sfera criminalităţii informatice, principala structură specializată este Serviciul de prevenire şi combatere a criminalităţii informatice din cadrai Direcţiei de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism. Activitatea de cercetare a infracţiunilor din sfera criminalităţii informatice este desfăşurată de Serviciul de combatere a criminalităţii informatice din cadrul Direcţiei de Combatere a Criminalităţii Organizate din cadrul Inspectoratului General al Politiei Romane.

Prin Legea nr. 508/2004 s-a înfiinţat Direcţia de Investigare a Infracţiunilor de CriminalitateOrganizată şi Terorism, în cadrul Parchetului de pe lângă Înalta Curte de Casaţie şi Justiţie, prin reorganizarea Secţiei de Combatere a Criminalităţii Organizate şi Antidrog, ca unica structură din cadrul Ministerului Public, specializată în combaterea şi investigarea infracţiunilor decriminalitate organizată şi terorism. Serviciul de prevenire şi combatere a criminalităţii informatice este condus de un procuror şef şi are în structură 3 birouri, conduse de procurori şefi. Serviciul de prevenire şi combatere a criminalităţii informatice efectuează urmărirea penală, în condiţiile prevăzute în Codul de procedură penală, în Legea nr. 508/2004, cu modificările şi completările ulterioare, precum şi în alte legi speciale care prevăd infracţiuni de competenţa Direcţiei de Investigare a Infracţiunilor de Criminalitate Organizată si Terorism.

Direcţia de Combatere a Criminalităţii Organizate (DCCO) este unitatea specializată din structura Inspectoratului General al Poliţiei Române, cu competenţă teritorială generală, care desfăşoară şi coordonează activitatea de combatere a criminalităţii organizate la nivel naţional, în conformitate cu actele normative în vigoare.

În Statele Unite ale Americii, la nivelul Departamentului de Justiţie a fost creată Secţiunea privind criminalitatea informatică şi proprietatea intelectuală („The Computer Crime and Intellectual Property Section”), care se ocupă cu implementarea

strategiei naţionate de combatere a criminalităţii informatice şi protejează proprietatea intelectuală în legătură cu acest stat la nivel global.

În ceea ce priveşte raportarea faptelor ilegale ce privesc sfera informaticii, principala structură de punere în aplicare a legislaţiei naţionale este F.B.I. (Federal Bureau of Investigation – Biroul federal de Investigaţii), la care se adaugă the United States Secret Service (Serviciul Secret al Statelor Unite), the United States Immigration and Customs Enforcement (ICE – Direcţia de Imigrări şi Vămi a Statelor Unite), United States Postal Inspection Service (Serviciul de Inspecţie Poştală a Statelor Unite) şi the Bureau of Alcohol, Tobacco and Firearms (ATF – Biroul pentru Alcool, Tutun şi Arme de foc al Statelor Unite).

Statele europene au dobândit, de-a lungul timpului, o bogată experienţă în ceea ce priveşte conlucrarea între instituţii naţionale similare, în vederea combaterii faptelor din sfera criminalităţii informatice de la nivel transfrontalier. La data de 4 iulie 2018, Parlamentul European a adoptat noua legislaţie a Uniunii Europene cu privire la criminalitatea informatică. Noua Directivă se doreşte a întări răspunsul Uniunii Europene faţă de criminalitatea informatică, astfel contribuind la creşterea nivelului de securitate informatică de care se bucură fiecare cetăţean U.E. Cu această ocazie, a fost înfiinţat şi Centrul European pentru Criminalitate Informatică (European Cybercrime Center), în cadrul Europol.

Europol este o organizaţie de combatere a criminalităţii la nivel european, având sediul la Haga (Olanda). Această organizaţie preia sarcinile poliţiei naţionale din fiecare stat al Europei, în caz că activitatea criminală, depăşeşte limita graniţelor naţionale. Centrul European pentru Criminalitate Informatică a fost creat în cadrul Europol, după realizarea unui studiu de fezabilitate comandat de Comisia Europeană către Rand Corporation Europe. Centrul se doreşte a fi punctul de focalizare a luptei împotriva criminalităţii informatice de la nivelul Uniunii Europene, contribuind la creşterea vitezei de reacţie a autorităţilor europene împotriva infracţiunilor din această arie.

CAPITOLUL VII. MĂSURI DE PREVENIRE SI COMBATERE A FENOMENULUI CRIMINALITATII INFRACTIONALE

În literatura de specialitate se evidenţiază faptul că definirea şi evaluarea conceptului de politică penală de prevenire a criminalităţii trebuie să ţină seama de trei dimensiuni:

a) prima se referă la legislaţia penală în vigoare privind sistemul de sancţiuni aplicate indivizilor delincvenţi;

b) cea de a doua include instituţiile specializate de prevenire şi control social specializat împotriva criminalităţii;

c) cea de a treia include reacţia socială faţă de crimă şi criminalitate.

Orice măsură întreprinsă în sensul limitării viitoare a acestui fenomen trebuie să ţină seama de diversitatea faptelor penale săvârşite, precum şi a situaţiilor în care diverse persoane sau instituţii devin victime ale unor astfel de infracţiuni. Considerăm că direcţiile pe care măsurile de prevenire şi combatere a fenomenului criminalităţii informatice ca parte a criminalităţii organizate trebuie să se îndrepte către o aplicare mai eficientă a legislaţiei existente şi completarea, îmbunătăţirea acestei, precum şi către o cooperare mai bună între instituţiile responsabile în vederea limitării activităţii infracţionale. De asemenea, considerăm că aceste direcţii ar trebui să vizeze și crearea unor programe complexe de consiliere şi asistenţă a victimelor dar şi a celor care au avut calitatea de autor al unei infracţiunii, în vederea reintegrării acestora în societate, dar și a unor programe/cursuri de perfecționare a anchetatorilor și magistraților în ceea ce privește modul de investigare a infracțiunilor informatice.

În vederea garantării unei securități cât mai mari pentru utilizatori, Uniunea Europeană a instituit Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA), al cărei rol este de a consilia Comisia și statele UE, precum și de a coordona măsurile pe care acestea le iau pentru a asigura securitatea sistemelor și rețelelor de informații.20 Centrul Naţional de Răspuns la Incidente de Securitate

Cibernetică (CERTRO), ca structură independent de expertiză şi cercetare în domeniul protecţiei infracstructurilor cibernetice.

Scopul măsurilor tehnice de protecție constă în protejarea resurselor informaționale contra amenințărilor sau vulnerabilităților. Securizarea sistemelor are drept scop îngreunarea accesului infractorilor la computer, dar și de a-i putea detecta în cazul în care aceștia reușesc să pătrundă. Pentru un rezultat cât mai bun, procedurile de securitate fizică a unui sistem, ar trebui combinate cu procedurile de securitate a operării.

În contextul dezvoltării rapide a tehnologiilor moderne de informații și comunicații fiecare țară este nevoită să-și dezvolte o strategie proprie de securizare a spatiului cibernetic. Prin adoptarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, țara noastră urmărește atât dezvoltarea unui mediu informaţional dinamic bazat pe interoperabilitate şi servicii specifice societăţii informaţionale, cât şi asigurarea respectării drepturilor şi libertăţilor fundamentale ale cetăţenilor şi a intereselor de securitate naţională, într-un cadru legal adecvat.

CAPITOLUL VIII. CAI DE ACTIUNE IN VIITOR

Dezvoltarea tehnicii și a tehnologiei a reprezentat o adevărată revoluție în societatea umană, având ca principală consecință tranziția de la Societatea Industrială la Societatea Informațională. Apariția calculatoarelor și a Internetului a ușurat foarte mult munca oamenilor, dându-le posibilitatea efectuarii într-un timp extrem de scurt a unei multitudini de tranzacții, de afaceri și de comunicări.

Calculatorul a devenit o component vitală a activității noastre zilnice iar tehnologia comunicațiilor și posibilitățile oferite de Internet au produs transformări în întreaga societate, pătrunzând în toate sectoarele vieţii economice, sociale şi culturale.

În aceste condiţii, criminalitatea informatică, este o problemă majoră în societăţile care folosesc pe scară largă tehnologia informatică, iar în condiţiile absenţei unei definiţii standardizate şi unanim acceptate şi a lipsei unor statistici credibile în domeniu, studierea şi examinarea din punct de vedere juridico-penal a acestui nou gen de infracţiuni, care a cuprins întreg mapamondul, este foarte importantă.

În România, fenomenul criminalităţii informatice se manifestă prin creşterea numărului de cazuri înregistrate şi organizarea celor ce comit astfel de fapte, în adevărate grupări infracţionale, precum şi reorientarea grupărilor criminale care, în trecut, comiteau infracţiuni din sfera traficului de persoane, traficului internaţional de autoturisme şi traficului de droguri, către infracţiuni de natură informatică.

Principalii factori, care au determinat reorientarea grupărilor criminale, către infracţiuni informatice, sunt legaţi de obţinerea de câştiguri materiale mari, într-un timp relativ scurt şi cu riscuri relativ mici În prezent, asistăm nu doar la o explozie, diversificare și specializare a criminalității, ci și la o congruență între infracțiunile din sfera criminalității informatice și infracțiunile „clasice”.

Având în vedere dinamica şi ritmul rapid de evoluţie a spaţiului cibernetic, precum şi obiectivele ţării în procesul de dezvoltare a societăţii informaţionale,

pentru implementarea pe o scară cât mai largă a serviciilor electronice, se întrevede nevoia ca legislaţia internă să se adapteze din mers şi continuu, la oportunităţile şi provocările generate de un mediu de securitate cibernetică în permanentă schimbare.

Asigurarea securităţii şi a spațiului cibernetic trebuie să se bazeze pe cooperarea la nivel naţional şi internaţional, prin coordonarea demersurilor naţionale în concordanţă cu orientările şi măsurile adoptate la nivel internaţional. Numeroase studii arată că doar o mică parte din faptele penale legate de utilizarea sistemelor informatice ajung la cunoştinţa organelor de cercetare penală, iar investigaţiile în domeniul infracţionalităţii informatice sunt, prin natura lor, complexe şi implică utilizarea de tehnologii și echipamente sofisticate.

Aplicarea eficientă a legislaţiei interne existente, precum şi armonizarea legislaţiei interne la cea de la nivel european şi internaţional este o directie care trebuie urmata in continuare. Criminalitatea informatică şi Internetul sunt două elemente aflate într-o continuă evoluţie, ceea ce face dificil pentru autorităţile publice crearea unui pachet legislativ adaptat celor mai noi metode de comitere de fapte penale. Totodată, având în vedere că legislaţia internaţională este realizată de cele mai multe ori în limba engleză, este necesar a se realiza traduceri cât mai fidele la transpunerea acesteia în legislaţia internă, pentru a se evita situaţii de confuzie între anumiţi termeni ori situaţii descrise în normele legale adoptate.

În strânsă legătură cu aplicarea eficientă a legislaţiei şi adaptarea acesteia la realitatea cibernetică, un alt punct important considerăm că este înființarea unor centre de pregătire periodică atât a anchetatorilor, cât și a magistraților. Nu de puține ori, practica ne-a arătat că polițiștii, dar și procurorii nu știu de unde să înceapă o investigație cu privire la o infracțiune informatică. De cele mai multe ori asemenea cauze sunt plasate “băiatului cu calculatorul.”

Având în vedere amploarea fenomenului criminalității informatice, computerele devinind din ce în ce mai mult obiectul crimelor tradiționale, este absolut necesar și util ca atât magistrații,cât și organele de cercetare penală să devină

“experți” în calculatoare, să cunoască cele mai noi metode de investigare a infracțiunilor.

De asemenea, având în vedere faptul că fraudele din sfera criminalităţii informatice sunt, uneori, în strânsă legătură cu infracţiuni de tip economic, ar fi utile stagii de practică pentru reprezentanţii Ministerului Public, organelor de poliţie şi magistraţi – judecători care să conţină şi predarea unor elemente de economie.

Intensificarea activităţilor de cooperare între stucturile publice care au atribuţii în ceea ce priveşte prevenirea şi combaterea criminalităţii informatice, prin creşterea numărului de persoane care să-şi desfăşoare activitatea de investigare a faptelor din sfera criminalităţii informatice, precum şi organizarea de stagii de practică comune, astfel cum am arătat şi mai sus, la care să participe personal din diverse structuri ori autorităţi publice, în vederea dezvoltării de echipe interspecializate, care să coopereze în mod eficient la viitoare acţiuni comune. Creşterea efectivelor de investigatori reprezintă o necesitate ce persistă de mult timp în practică, multe cauze fiind soluţionate cu întârziere, din lipsa personalului specializat în realizarea de percheziţii şi/sau culegeri de date informatice.

Cooperarea dintre autortiăţile publice şi membrii societăţii civile, în vederea aducerii la cunoştinţa acestora din urmă a pericolelor la care se expun când accesează Internetul ori contul personal, precum şi cu privire la metodele de protecţie pe care le au la dispoziţie pentru a evita statutul de victime.

Existenţa unor instituţii specializate la nivel intern şi internaţional precum şi existenţa unei cooperări dintre aceste instituţii reprezintă aspecte pe care le-am arătat anterior, în prezenta lucrare. Însă, având în vedere şi concluziile chestionarului aplicat utilizatorilor, rezultă că fenomenul criminalăţii informatice rămâne perceput ca ceva abstract, care are loc doar la un nivel superior vieţii cotidiene, căruia le cad victime doar companiile mari şi faţă de care populaţia sau firmele de mici dimensiuni adoptă atitudinea „mie nu mi se poate întâmpla”.

La momentul la care o persoană devine victima unui furt de date personale sau află că i s-a clonat cardul de credit, de exemplu, se adresează fie instituţiei bancare, iar de cele mai multe ori este sfătuită să nu facă publică lipsa sumelor din cont, pentru a nu ştirbi imaginea băncii, fie se adresează unui site (de exemplu de poştă electronică sau de cumpărături), fără a primi un răspuns clar într-un termen rezonabil.

De aceea, considerăm utilă desfăşurarea unor campanii de aducere la cunoştinţă a riscurilor pe care activitatea online le poate purta, dar şi de expunere clară către populaţie şi mediul de afaceri, a unor paşi legali cre sunt la dispoziţia potenţialelor victime, în caz de nevoie.

Deşi legislaţia internă din România este cosacrată principiului „Nemo legem ignorare censetur" – Nimeni nu poate invoca necunoaşterea legii, în practică trebuie să acceptăm că anumite părţi ale legislaţiei sunt mai puţin accesibile decât altele.

Şi pentru acest motiv, considerăm că între membrii societăţii civile şi reprezentanţii autorităţilor trebuie să se dezvolte o cooperare de durată, care să producă periodic informaţii sub forma unor ghiduri care să fie aduse la cunoştinţa unor grupuri ţintă bine determinate, în concordanţă cu nivelul fiecăruia de înţelegere a riscurilor de a deveni victime ale criminalităţii informatice.

Lumea criminalității informatice nu se limitează doar la fraude bancare, fraude cu cărți de credit, fraude economico-financiare, ci merg mai departe până la săvârșirea de acte teroriste. Din ce în ce mai mult, în zilele noastre grupările teroriste utilizează Internetul pentru a-și atinge scopurile, în sensul că își propagă ideologiile pe care le îmbrățișează, trimit mesaje de ură și incitare la violență, pregătesc atacuri teroriste, etc. În plus, spre deosebire de acum câţiva ani - o caracteristică a criminalităţii informatice din zilele noastre o reprezintă nivelul de dezvoltare a instrumentelor utilizate şi automatizarea atacurilor şi a infectării sistemelor informatice pentru a prelua controlul acestora.

Retelele de computere ale utilizatorilor casnici şi din firme şi instituţii, infectate şi care pot fi programate să atace simultan din nenumărate colţuri ale lumii

un serviciu sau o retea conectata la internet au o capacitate de atac demonstrată deja în numeroase ocazii. Pentru a intra la categoria terorismului informatic, doar motivaţia politică mai este necesara - o organizatie teroristă putând închiria cu uşurinţă o astfel infrastructură ce poate fi utilizată ca arma cibernetică.

Cel mai des oferit exemplu care poate fi încadrat la **ciberterorism** este atacul asupra Estoniei în 2007. Mai sunt şi alte exemple de situaţii în care a existat o urmare deosebit de gravă cu impact la nivel social. Având în vedere aceste aspecte, dar și multe alte activități pe care grupările teroriste le întreprind prin intermediul Internetului, dar și gravitatea acțiunilor lor, de lege ferenda propunem introducerea unor noi articole în legislația penală care să prevadă incriminarea terorismului informatic.

Alternativ, ar fi utilă şi introducerea unui alineat suplimentar pentru infracţiunile din sfera criminalităţii informatice prevăzute de Codul Penal, respectiv Accesul ilegal la un sistem informatic, Interceptarea ilegală a unei transmisii de date informatice, Alterarea integrităţii datelor informatice, Perturbarea funcţionării sistemelor informatice, Transferul neautorizat de date informatice, Operaţiuni ilegale cu dispozitive sau programe informatice, Falsul informatic, Frauda informatică şi Pornografia infantilă prin sisteme informatice. Respectivul alineat ar fi necesar să cuprindă sancţiuni penale cu limite mai mari, dacă infracţiunea este comisă în scopul întreprinderii unor acţiuni teroriste. În acest sens, considerăm că este necesară introducerea de către leguitor şi a unei definiţii unitare a acestui nou concept, în acord cu legislaţia în vigoare.

Definiţia dată „**terorismului informatic**” de F.B.I. este una completă: „un atac premeditat, motivat politic, impotriva informatiilor, sistemelor de calculatoare, programelor si operarilor de date, ce conduce la violente impotriva obiectivelor civile si necombatantilor, atac exercitat de grupări subnaţionale sau agenţi clandestini”. Aceasta întrucât terorismul reprezintă o ameninţare la nivel global, iar legislaţia în acest domeniu este necesar a fi una unitară.

BIBLIOGRAFIE

1. D. Cimpoeru, Dreptul internetului, Ed. C.H. Beck, București, 2017;

2. V. Coman, Infractiuni privind criminalitatea in cyberspatiu. Volumul I. Practica judiciara recenta adnotata, Ed. Universul Juridic, București, 2020;

3. M. Cross, Scene of the cybercrime, ediţia a II-a, Ed. Syngress Publishing Inc, Rockland Massachusetts, 2018;

4. Goodman S.E., Sofaer A.D. - The Transnational Dimension of Cyber Crime and Terrorism, Hoover Press, Standford, CA, 2011

5. I.-C. Mihai, L. Giurea, Criminalitatea informatică, Ediţia a II-a revizuită şi adăugită, Editura Sitech, 2014;

6. M. C. Scheau, Criminalitatea informatica privind transferurile financiare, Ed. Economică, București, 2018;

7. E. Stan. Războiul informatic, Ed. Argument, Bucuresti, 2012;

8. E. Străinu, E. Stan, Războiul informatic. Războiul epocii informaţionale, Ed.Triumf, Bucureşti, 2009;

9. C. Voicu, E. Stan, Investigarea infractiunilor informatice, editia a II-a, Ed. Triumf, Bucuresti, 2014;

10. Gh. Zlati, Tratat de criminalitate informatică, vol. I, Ed. Solomon, București, 2020.