ROMÂNIA
MINISTERUL ADMINISTRAŢIEI ŞI INTERNELOR
ACADEMIA DE POLIŢIE „ALEXANDRU IOAN CUZA”
ŞCOALA DOCTORALĂ ORDINE PUBLICĂ ŞI SIGURANŢĂ NAŢIONALĂ

TEZĂ DE DOCTORAT

CONDUCĂTOR DE DOCTORAT:
Prof.univ.dr.
Ştefania-Georgeta UNGUREANU

DOCTORAND:
IONIŢĂ Alexandru Cătălin

BUCUREŞTI
- 2012 -

R O M Â N I A **Nesecret**
MINISTERUL ADMINISTRAŢIEI ŞI INTERNELOR **Exemplar nr.**
ACADEMIA DE POLIŢIE *„Alexandru Ioan Cuza*”
Nr. _____ din _____ 2012

Doctorand IONIŢĂ Alexandru Cătălin

TEZĂ DE DOCTORAT

CRIMINOGENEZA INFRACŢIUNILOR CIBERNETICE

CONDUCĂTOR DE DOCTORAT:

Prof.univ.dr.

ŞTEFANIA-GEORGETA UNGUREANU

Teză elaborată în vederea
obţinerii titlului ştiinţific
de Doctor în Ordine Publică
şi Siguranţă Naţională

BUCUREŞTI

- 2012-

CUPRINS

ARGUMENT

Noua tehnologie informatică a pătruns în activitatea cotidiană, a schimbat modul nostru de viaţă obişnuit şi ne-a făcut să privim cu mai multă încredere în viitor. Astăzi, pentru a putea cumpăra un bilet de tren sau un tichet de metrou, trebuie să accesezi automatul care face distribuirea acestora prin accesarea cod, activitate care banalizează în totalitate vechiul mod de distribuţie.

Nu de puţine ori informatica ne rezervă surprize de proporţii mult mai mari. Munca în administraţie a devenit mai eficientă; în economie procesul de producţie se realizează în paşi „uriaşi"; în telecomunicaţii informaţiile sunt parte indestructibilă a noilor tehnologii informatice în materie, iar în deciziile militare ne crează posibilităţi rapide, inedite, de conversaţie.

Acum, elevii învaţă din primii ani de şcoală cum să folosească un calculator, fiindcă astăzi, dar mai ales mâine, toate serviciile vor apela la generaţii sofisticate de tehnologie.

Incontestabil, în societatea românească, cât mai curând, calculatorul va face parte din familia fiecăruia dintre noi. El ne va ajuta să ne multiplicăm reţelele şi să facem conexiuni cu o rapiditate uluitoare. Reţelele vechi de cabluri sunt înlocuite cu fibre optice, liniile de comunicaţii au un debit mult mai mare, iar sateliţii şi autocomutatoarele constituie o imensă resursă pentru comunicare între oamenii aflaţi în direcţii opuse ale planetei.

Tranzacţiile comerciale se pot încheia cu viteza electronică, fapt care face să dispară noţiunea de spaţiu şi de timp între părţi, discuţiile putându-se purta prin telefon, prin televiziune sau cu ajutorul mijloacelor de comunicare portabilă.

Sistemele informatice ne ajută să ne administrăm în toate domeniile: distribuţia electricităţii, gestionarea resurselor, transporturi aeriene, alocaţii familiale, securitate socială, fiscalitate, gestiune bancară şi tranzacţii financiare, viramente de salarii, controale aeroportuare, cărţi de identitate, paşapoarte, permise de conducere etc.

Viaţa noastră cotidiană este în mod direct condiţionată de buna funcţionare a sistemelor de informatică. Noile sisteme sunt din ce în ce mai mult apreciate ca o forţă fundamentală pentru funcţionarea şi existenţa unui stat.

Informatica, cu o frontieră care constituie o forţă extraordinară de dialog şi de progres, prezintă din păcate o formidabilă vulnerabilitate. Societatea devine de la o zi la alta total dependentă de acest spaţiu informatic. De aceea, conştientizând importanţa pătrunderii noilor tehnologii în viaţa cotidiană, trebuie să ne luăm măsuri de protejare a sistemelor informatice, noua tehnologie fiind la fel de vulnerabilă cât ne este de necesară. De exemplu, să ne imaginăm ce ar prezenta pentru viaţa social-economică a ţării afectarea sistemului naţional de electricitate de indivizi care au pătruns fraudulos în reţeaua informatică, profitând de vulnerabilitatea sistemului şi de lipsa de pregătire a celor abilitaţi să acţioneze pentru prevenirea unor astfel de evenimente.

Informaţia constituie un element esenţial în bătălia pentru cunoaştere, dar cine o deţine are şi supremaţia deciziei.

Pentru a combate criminalitatea comisă cu ajutorul noii tehnologii trebuie şi o dotare pe măsură, însă, mai ales, trebuie să ne formăm specialişti care să poată acţiona în acest sensibil domeniu.

La momentul actual, în lume, inamicii de ieri au devenit parteneri şi aliaţi, noile posibilităţi oferite de tehnologie făcând extreme de dificilă stabilirea unei frontiere între bine şi rău, şi, practice, aceasta făcându-i pe toţi agresori şi agresaţi.

Nu vor fi înlăturate aceste noi vulnerabilităţi dacă nu vor fi identificate foarte bine riscurile, motiv care duce la faptul că, în viitor, cercetarea criminologică şi criminologia în general, va avea un rol foarte important în identificarea cauzelor şi condiţiilor care favorizează criminalitatea informatică.[1]

[1] Tudor Amza, Tudor-Petronel Amza, Criminalitatea informatică, Ed. Lumina Lex, Bucureşti, 2003.

CAPITOLUL I
STATUTUL CRIMINALITĂŢII CIBERNETICE ÎN SOCIETATEA CONTEMPORANĂ

Cu privire la definirea criminalităţii informatice, găsirea unei definiţii unice, atotcuprinzătoare, e imposibil de realizat problema definiţiei fiind punct de pornire în orice încercare de uniformizare – raport la planul cooperări internaţionale – a incriminărilor în această materie.

Legislaţia statelor lumii este în continuă schimbare datorită dezvoltării tot mai accelerate a tehnologiei informatice, iar cooperarea internaţională este pusă în faţa unei provocări continue produsă de creşterea criminalităţi informatice transnaţionale. Din ce în ce mai multe state au procedat la armonizarea propriilor legislaţii în vederea combaterii fenomenului în discuţie, însă rezultatele sunt doar mulţumitoare şi nu se va putea vorbi de o eradicare a fenomenului.

CAPITOLUL II

PRINCIPALELE FORME DE MANIFESTARE A CRIMINALITĂŢII CIBERNETICE

În legea 161/2003 exista trei categorii de infracţiuni, incriminate, astfel:

Infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice.

Infracţiunea de acces ilegal la un sistem informatic;

Infracţiunea de interceptare ilegală a unei transmisii de date informatice;

Infracţiunea de alterare a integrităţii datelor informatice;

Infracţiunea de perturbare a funcţionării sistemelor informatice;

Infracţiunea de a realiza operaţiuni ilegale cu dispozitive sau programe informatice.

Infracţiuni informatice

Infracţiunea de fals informatic;

Infracţiunea de fraudă informatică.

*Pornografia infantilă prin intermediul sistemelor informatic*e

CAPITOLUL III

ALTE FORME DE MANIFESTARE A CRIMINALITĂŢII CIBERNETICE

Legea cadru în materie de comerţ electronic, Legea nr. 365/2002, *are ca scop stabilirea condiţiilor de furnizare a serviciilor societăţii informaţionale, precum prevederea ca infracţiuni a unor fapte săvârşite în legătura cu securitatea domeniilor utilizate în comerţul electronic, emiterea şi utilizarea instrumentelor de plată electronică şi cu utilizarea datelor de identificare în vederea efectuării de operaţiuni financiare, pentru asigurarea unui cadru favorabil liberei circulaţii şi dezvoltării în condiţii de securitate a acestor servicii.*

TERORISMUL INFORMATIC (sau cyberterorismul) reprezintă *convergenţa nefastă dintre spaţiul cibernetic şi terorismul clasic*[2]. Sunt incluse aici:

- operaţiunile de penetrare şi perturbare gravă a sistemelor informatice;
- operaţiunile de alterare sau furt a datelor şi informaţiilor stocate în maşinile de calcul cu scopul declarat de a produce pagube importante, în plan economic şi social;
- operaţiunile de a influenţa deciziile politice ori ca răspuns la acţiuni ostile.

[2] D. Denning, op. cit.

CAPITOLUL IV
CRIMINOGENEZA CRIMINALITĂŢII CIBERNETICE

Având în vedere diversitatea conduitelor criminale, raportul lor cu normele şi standardele sociale în baza cărora sunt taxate ca antisociale sau nu, faptul că, în general, infractorii aparţin tuturor categoriilor de vârstă, sex, pregătire socioprofesională şi culturală, aptitudini intelectuale, rol, statut social sau economic, tip temperamental şi caracterologic etc., apare destul de limpede determinarea lor multiplă. Propunându-şi ca obiectiv identificarea cauzelor şi condiţiilor în care un individ este susceptibil a se angaja în acte de agresiune antisociale, cercetările efectuate pun în evidenţă o „cauzalitate multiplă cumulativă".

Din evaluările grupărilor infracţionale care acţionează în domeniu s-au desprins următoarele caracteristici privind criminalitatea informatică produsă în România:

- caracter predominant financiar, se urmăreşte obţinerea unui produs financiar substanţial şi sunt vizate sisteme de plată, produse de credit şi plată oferite de instituţii financiare;

- organizarea grupărilor care acţionează; structurarea şi specializarea membrilor acestora;

- folosirea unor tineri cu abilităţi în a utiliza computerele şi noile tehnologii, care sunt organizaţi şi coordonaţi de către lideri ai grupărilor infracţionale;

- trecerea de la fraudele informatice în care încrederea era elementul primordial în realizarea tranzacţiilor, la fraude în care predomină folosirea de programe informatice în fraudare;

- caracterul transnaţional al acestor fapte, în sensul că sunt vizate victime din alte ţări, anumite activităţi sunt derulate de pe teritoriul altor state sau sunt folosite sisteme informatice din alte state;

- permanenta preocupare pentru identificarea de noi moduri de operare, de identificarea de produse ce pot fi fraudate, precum şi sisteme informatice ce pot fi compromise;

- reorientarea grupărilor infracţionale către fraudarea mijloacelor de plată electronică oferite de instituţiile financiare din România;

- reorientarea grupărilor infracţionale care comit fraude informatice, de la fraudele mărunte (prejudicii mici) îndreptate împotriva persoanelor, către fraudele mari (prejudicii mari – sute de mii/milioane de euro) împotriva companiilor;

- zonarea infractorilor pe tipuri de infracţiuni şi ţări de destinaţie, datorate specificului zonei (zone turistice, zone cu număr ridicat de grupări infracţionale bine organizate etc.).

În urma cazurilor soluţionate, a reieşit că infractorii care provin din judeţele vestice şi sud-vestice ale României (Satu Mare, Bihor, Timiş, Caraş-Severin, Hunedoara, Gorj, Dolj, Olt şi Teleorman) preferă să-şi desfăşoare activităţile infracţionale în Franţa. Infractorii din judeţele aflate în Moldova (Suceava, Iaşi, Bacău) folosesc ca ţări de desfăşurare a activităţilor Marea Britanie şi Germania. Germania apare ca ţară preferată şi pentru cei din judeţul Braşov. Alte două ţări unde desfăşoară activităţi infracţionale din domeniul criminalităţii informatice cetăţenii români sunt Spania şi Italia. Majoritatea celor care comit astfel de fapte provin din judeţele Vâlcea, Argeş, Constanţa şi Municipiul Bucureşti.

Principalii factori care au determinat reorientarea grupărilor criminale către infracţiuni informatice sunt:

- obţinerea de câştiguri materiale mari într-un timp relativ scurt şji cu riscuri relativ mici;

- caracterul transfrontalier al infracţiunilor face ca instrumentarea acestora de către autorităţile unui stat să fie mult mai dificilă întrucât, pentru probarea faptelor este nevoie, de cele mai multe ori, de obţinerea unor informaţii de la

autorităţile competente din mai multe state, pe calea cererilor de asistenţă juridică internaţională, procedură ce este costisitoare şi lentă;

- accesul facil la echipamente moderne care permit desfăşurarea de activităţi ilicite şi complexe;

- posibilitatea deplasării rapide a membrilor unei grupări criminale de pe teritoriul unui stat pe teritoriul altui stat, urmărirea activităţii desfăşurate de către aceştia fiind, de cele mai multe ori, foarte greu de realizat de către autorităţile competente.

Fraudele informatice, atacurile informatice, fraudele cu mijloace de plată electronică şi pornografia infantilă prin Internet sunt tipuri infracţionale care necesită investigaţii specializate, pregătire şi dotare corespunzătoare pentru structurile de aplicare a legii. Fraudele privind comerţul electronic sunt preocupări continue ale elementelor infractoare pentru identificarea de noi moduri de operare (licitaţii frauduloase, folosirea de site-uri false de escrow, site-uri de transport, site-uri de comerţ electronic, site-uri de phishing), organizarea şi specializarea membrilor grupărilor (atât asupra activităţilor desfăşurate în cadrul activităţii infracţionale, cât şi din punct de vedere tehnic);

- ascunderea urmelor prin Internet şi a circuitului produsului financiar;

- „extraneitatea" activităţilor infracţionale comise, astfel, parte din acestea sunt iniţiate din România, dar vizează victime din străinătate sau sunt finalizate în străinătate, unde se ridică produsul financiar;

- folosirea în comiterea acestor fapte a sistemelor de plată rapide oferite prin Internet (sistem escrow, conturi de paypal, conturi e-gold, conturi de internet-bancking) sau a celor de transfer rapid de bani;

- cele mai active zone ale ţării sunt cele deja cunoscute: Bucureşti, Alexandria, Râmnicu-Vâlcea, Craiova, Timişoara, Iaşi, Sibiu şi Constanţa;

- comerţul electronic începe să se dezvolte şi în România, atât în ceea ce priveşte site-urile de comerţ electronic, folosirea de instrumente de plată electronice

(cărţi de credit), dar şi numărul de persoane care achiziţionează produse prin acest sistem.

Fraudele cu cărţi de credit a cunoscut o creştere exponenţială, înregistrându-se numeroase cazuri de persoane depistate la bancomate în România care folosesc cărţi de credit în mod fraudulos. De asemenea, numeroase cazuri sunt semnalate de către autorităţi străine cu privire la cetăţeni români care sunt depistaţi comiţând astfel de fraude la bancomate.

CAPITOLUL V

ELEMENTE DE DREPT COMPARAT ÎN MATERIA CRIMINALITĂŢII CIBERNETICE

În ceea ce priveşte modul de reglementare a criminalităţii informatice, acesta este diferit datorita faptului ca infracţiunile din domeniu activităţilor informatice iar nivelul precar de dezvoltare al unor state in domeniu tehnologiilor informatice nu a impus introducerea reglementarilor in aceasta materie. Se constata existenţa unor prevederi şi sancţiuni penale neuniforme, care diferă de la ţară la ţară, în funcţie de tipul datelor manipulate. Doar câteva armonizări au fost realizate în domeniul protecţiei datelor cu caracter personal pentru protecţia vieţii private.

Astfel în dreptul penal al SUA exista prevederi care reglementează acţiuni ca refuzul de a da informaţii caracter personal sau furnizarea de informaţii false autorităţilor statului, refuzul de a permite accesul! şi inspecţia autorităţilor pe o proprietate personală (au fost incluse în definiţie şi calculatoarele personale), refuzul de a permite înregistrarea oficială a unor date caracter personal.

Observăm că legislaţia Africii de Sud respectă prevederile Convenţie' Ca o particularitate, faptele care aduc atingere integrităţii şi securităţii sistemelor

informatice sunt incriminate într-un singur articol. Separat, se prevede incriminarea falsului şi a fraudei informatice, precum şi a unor dispoziţii generale privind tentativa, participaţia şi sancţiunile aplicabile.

Observăm faptul că Australia sancţionează în special acele fapte care aduc atingere integrităţii şi confidenţialităţii datelor informatice şi se referă mai puţin (cu excepţia comunicaţiei electronice) la sistemul informatic în sine. De asemenea, din studiu Codului Penal reiese faptul că infracţiunile de fals informatic şi frauda informatică sunt asimilate infracţiunilor tradiţionale, calculatorul fiind considerat doar un mijloc de comitere a faptei.

Specific legislaţiei bulgare este incriminarea extensivă a faptelor îndreptate împotriva integrităţii şi securităţii sistemelor informatice. Legislaţia bulgară nu incriminează în schimb falsul informatic, considerând că este acoperită de prevederile dreptului comun. Frauda informatică este prevăzută ca o variantă agravată a infracţiunii de alterare a integrităţii datelor informatice.

Canada manifestă tendinţa unei reglementări proprii infracţiunilor îndreptate împotriva integrităţii şi securităţii datelor informatice şi nu se preocupă de falsul şi frauda informatică, considerându-le acoperite de prevederile de drept comun.

Observăm că în legislaţia statului Chile nu sunt reglementate ca infracţiuni producerea sau procurarea de viruşi ori obţinerea unor parole, în vederea accesului ilegal la un sistem informatic ori pentru alterarea integrităţii datelor informatice ori chiar a integrităţii sistemului.

Legislaţia chineză acoperă prevederile Convenţiei în ceea ce priveşte recomandările acesteia în domeniul infracţiunilor îndreptate împotriva confidenţialităţii, integrităţii şi securităţii datelor şi sistemelor informatice. De asemenea, sunt incriminate infracţiuni de drept comun săvârşite prin intermediul sistemelor informatice, cum ar fi falsul, înşelăciunea, furtul, faptele de corupţie, şantajul.

Legislaţia Croaţiei respectă prevederile Convenţiei, incriminând, la fel Ca în cazul Africii de Sud, faptele care aduc atingere integrităţii şi securităţii

sistemelor informatice într-un singur articol. Legislaţia croată nu incriminează în schimb falsul şi frauda informatică, considerând că sunt acoperite de prevederile dreptului comun.

Danemarca incriminează numai accesul ilegal, celelalte fapte putând fi acoperite în legislaţia daneză de prevederile de drept comun.

Legislaţia elveţiană prevede fără sistematizare atât infracţiuni de drept comun săvârşite prin intermediul sistemelor informatice, cât şi infracţiuni îndreptate împotriva confidenţialităţii, integrităţii şi securităţii datelor şi sistemelor informatice, acoperindu-se însă prevederile Convenţiei.

Codul Penal estonian, modificat, a intrat în vigoare la 1 septembrie 2002. Estonia a ratificat Convenţia Europeană asupra Criminalităţii Informatice la 12 mai 2003.

CAPITOLUL VI
MODALITĂŢI DE PREVENIRE ŞI COMBATERE A CRIMINALITĂŢII ORGANIZATE

Scara alarmantă a criminalităţii, aflată în continuă creştere, obligă la o mai bună organizare a efortului de apărare a valorilor sociale fundamentale, a drepturilor şi libertăţilor cetăţenilor.

Astfel, se impune cu necesitate ca prevenirea criminalităţii să devină o misiune permanentă a organelor de poliţie. Statul este cel care, în funcţie de ordinea prioritară stabilită prin politica sa în domeniul apărării sociale, combaterii criminalităţii şi realizării unui climat de ordine şi linişte publică, trebuie să realizeze un echilibru între munca de prevenire şi cea de combatere a criminalităţii. Acest echilibru trebuie privit sub aspect dinamic, în sensul deplasării accentului către o latură sau cealaltă, în funcţie de priorităţile stabilite prin politica statului respectiv.

Din cauza complexităţii Intemetului şi extinderii acestei reţele în ţări care, evident, sunt caracterizate de legislaţii diverse, este foarte dificilă incriminarea acestor infracţiuni informatice.

Eficienţa acţiunilor şi politicilor conturate în scopul întâmpinării acestui nou timp de criminalitate este pusă la îndoială de nesincronizarea prevederilor actelor normative ale statelor care reglementează acest segment al dezvoltării tehnologice.

Sistemele juridice din întreaga lume sunt puse să facă faţă acestor noi provocări prin elaborarea unor soluţii prin definirea clară a infracţiunilor ce decurg din folosirea abuzivă a spaţiului cibernetic. Importantă este şi stabilirea unor norme care să determine sub ce jurisdicţie intra delictul comis în acest mod atipic, ştiut fiind ca lumea virtuală nu cunoaşte aceleaşi frontiere delimitate din lumea fizică.

După o perioadă îndelungată în care s-a evitat o mobilizare generală a factorilor responsabili în vederea creării unui status al spaţiului virtual - tocmai din cauza scepticismului şi ironiei cu care este şi în prezent tratată problematica cyberterorismului – noul mileniu a debutat prin manifestarea unui interes constant de conturare a unui „drept al Internetului”.

Din perspectiva europeană, una din primele reglementări juridice aplicabile spaţiului virtual o constituie Directiva 2000 / 31 / CE a Parlamentului european din 8 iunie 2000 - act normativ care se referă în special la comerţul electronic de pe piaţa UE. O semnificaţie aparte o are şi semnarea, la 23 noiembrie 2001, la Budapesta, a Convenţiei asupra Criminalităţii Informatice de către statele membre ale Consiliului Europei. Convenţia s-a dorit a fi un preambul la măsurile ce se impun a fi luate la nivel naţional cu privire la infracţiunile ce aduc atingere confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice acces ilegal, interceptare ilegală, frauda informatică etc.).

Convenţia asupra cybercriminalităţii mai cuprinde reglementări cu privire la domeniul de aplicare a normelor, condiţiile de supraveghere şi conservare rapidă

a datelor informatice stocate, confiscările şi interceptările de date informatice, competenţa şi cooperarea internaţională, inclusiv în domeniul extrădării.
Acordând credit unui recent raport emis de Departamentul Apărării al SUA, în mod curent, cel puţin 10 ţări posedă mijloace informatice ofensive şi capacitate de luptă în plan electronic similare cu cele americane. Mai mult decât atât, încă din 1996, un document al Government Accounting Office nominaliza un număr impresionant de 120 de state care aveau posibilităţi informatice de un nivel mai ridicat sau mai scăzut. Realitatea acestei potenţiale ameninţări este relatată şi intr-un articol din 2000 apărut în Liberation Army Daily – ziarul oficial al Armatei populare a Chinei – intitulat "*asimilarea resurselor strategice ale Internetului în cadrul Sistemului Militar, la acelaşi nivel de semnificaţie cu pământul, marea şi aerul*". Articolul tratează pregătirile Chinei de a realiza tehnologie informatică avansată în scopul de a exploata oportunităţile strategice ale Internetului şi de a sprijini crearea a patru ramuri în cadrul armatei şi serviciilor de securitate care să audieze posibilităţile de atac informatic.

CAPITOLUL VII
CONCLUZII ŞI PROPUNERI DE LEGE FERENDA

Pe plan legislativ, este esenţial rolul *Convenţiei Consiliului Europei pentru combaterea criminalităţii informatice,* semnata la Budapesta, la data de 23 noiembrie 2001. Având ca obiect realizarea unui demers comun al mai multor state de a implementa în legislaţiile lor naţionale modalităţi de combatere a infracţionalităţii bazate pe sisteme informatice, Convenţia acordă, în Articolul 9, un spaţiu important pornografiei infantile, reglementând fapte pe care statele semnatare urmează sa le incrimineze în legea penala interna şi oferind anumite precizări de ordin conceptual.

Pornind de la prevederile Convenţiei, Parlamentul României a adoptat recent *Legea nr. 161/2003 privind unele masuri pentru asigurarea transparentei*

în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei[3] care în *Titlul III* reglementează *prevenirea şi combaterea criminalităţii informatice. în* cuprinsul reglementarii, prevederile art.35 alin.l lit.i) şi alin.2 (definirea expresiilor "materiale pornografice cu minori" şi "fără drept"), precum şi cele ale art.51 (incriminarea pornografiei informatice prin sisteme informatice) din lege au relevanta pentru studiul nostru.

Cu promisiunea de a încerca, cu un prilej ulterior, realizarea un comentariu larg pe marginea dispoziţiilor legii romane aplicabile, ne vom referi, în continuare, la unele consideraţii din cuprinsul *Raportului Explicativ* la Convenţia Consiliului Europei, pe marginea Articolului 9 din Convenţie, precum şi la efectele pe care acestea le generează în practica.

În lumina acestui document internaţional, libertatea de exprimare în Internet trebuie sa fie supusa unor rigori extreme, întrucât spaţiul cibernetic este locul care oferă pedofililor posibilităţi ample de a schimba idei, fantezii şi sfaturi, destinate să încurajeze şi să faciliteze exploatarea sexuală a copiilor. Prin urmare, conţinuturile de acest gen nu includ doar imagini, dar şi veritabile "dezbateri", mai cu seamă în camerele de conversaţie, intre promotorii unor asemenea practici îndreptate împotriva minorilor.

Cu toate acestea, Articolul 9 din Convenţie se refera la "imagini" şi "înfăţişări vizuale". Nu este limpede în ce măsură se tinde sau nu să se criminalizeze şi acele resurse Internet unde, sub diverse forme, se vorbeşte în termeni favorabili despre exploatarea sexuala a copiilor sau unde sunt reproduse nuvele cu conţinut pedofil. Este posibila o interpretare în sens afirmativ, pornind de la definirea, în Articolul 1 lit. b) din Convenţie, a noţiunii de "date informatice". Acestea constituie "orice reprezentare a unor fapte, informaţii sau concepte intr-o forma care poate fi prelucrata printr-un sistem informatic", deci, apreciem noi, şi a

[3] Publicată în M.Of., Partea I, nr.279 din 21.04.2003.

unor informaţii în forma verbala. Totuşi, Articolul 9 din Convenţie nu utilizează formula "date informatice". în opinia noastră, incriminarea ar trebui sa se extindă, în orice caz, asupra acelor conţinuturi din Internet care fac apologia faptelor penale cu caracter sexual, îndreptate împotriva copiilor. Problema se poate complica în cazul paginilor Web care prezintă nuvele implicând relaţii sexuale cu sau intre minori, în raport cu care partizanii libertăţii de exprimare în Internet ar putea invoca argumente referitoare la valoarea artistica a unor asemenea producţii.

Convenţia situează în sfera ilicitului penal "oferirea" sau "punerea la dispoziţie" a pornografiei infantile prin intermediul sistemelor informatice. Este avuta în vedere crearea de pagini Web şi de conexiuni către asemenea site-uri.
Raportul explicativ nu insista asupra modalităţilor practice de "a oferi" şi "a pune la dispoziţie", dar menţionează ca aceste acţiuni trebuie sa implice posibilitatea persoanei respective de a furniza, în mod efectiv, conţinuturile prohibite. în acest context, apreciem ca sunt situaţi în afara sferei ilicitului penal acei creatori de site-uri sau link-uri ce folosesc denumiri apte sa sugereze pornografia infantila, fără să o ofere insa în mod efectiv, scopul lor fiind acela de a deturna traficul de internauţi către aceste locuri unde se pot găsi diverse reclame publicitare, câştigul material pentru site-ul gazda constând în numărul mare de accesări din partea utilizatorilor. Fără îndoială, folosirea, pentru aceste scopuri, a unor adrese URL şi denumiri de pagini Web mai mult decât provocatoare poluează teritoriul virtual şi sunt de neacceptat intr-o comunitate care adera, totuşi, la norme morale minimale. Cât timp insa o asemenea conduita nu va cădea, în mod expres sub incidenţa legii penale, ea va continua sa fie practicata.
În ultima vreme, se discută chiar dacă denumiri precum *"Lolita "* sau *"Teens",* utilizabile pentru resursele Internet, nu ar fi suspecte în sensul sugerării

pornografiei infantile[4]. Fără a nega o asemenea posibilitate, nu putem să nu observăm cursul cel puţin curios pe care dezbaterile subsumate acestei teme au început să îi înregistreze, în contextul problematicii limitelor libertăţii de exprimare în Internet. Prin urmare, ar trebui să ne ferim (să ne temem) de utilizarea unor cuvinte cu înţelesuri sugestive!

Cât priveşte expresia "comportament sexual explicit", Raportul Explicativ evoca definiţia utilizata de legea penala a S.U.A., pe care am redat-o mai sus.
În legătură cu formula "material pornografic", se face o trimitere - firească, în opinia noastră - la standardele naţionale ale fiecărui stat semnatar al Convenţiei, vizând clasificarea unor materiale determinate, ca fiind obscene, contrare bunelor moravuri sau indecente. Într-adevăr, Convenţia nu îşi putea propune stabilirea unui standard internaţional, având în vedere diferenţele culturale semnificative ce continuă să se manifeste în acest perimetru[5]. Pentru aceste motive, Raportul Explicativ afirma situarea în afara sferei noţiunii de material pornografic a acelor producţii "care au o valoare artistica, medicala, ştiinţifica sau similara." în consecinţa, problema calificării corecte a acestor noţiuni, în scopul stabilirii răspunderii penale, va genera, în continuare, dispute şi viziuni neunitare, în condiţiile în care Internetul este o reţea globala, în care sunt conţinuturile şi libertatea de a le exprima nu se opreşte la frontierele naţionale.

Convenţia şi-a propus sa nu se limiteze la interzicerea imaginilor ce prezintă un minor angajat intr-un comportament sexual explicit, ci sa extindă aria de protecţie a minorilor, chiar şi în acele situaţii în care aceştia nu sunt, în mod efectiv, utilizaţi în crearea de producţii pornografice în Internet. Scopul

[4] A se vedea Danny, Webmasterjoint, *Why You Should Avoid Words Like Lolita,* comentariu disponibil la adresa http://vvww.webmasterioint.com/articles/0902/whv avoid lolita.php

[5] Deşi procesul de globalizare este în curs, implicând reducerea distantelor fizice intre oameni, ca efect al utilizării tehnologiilor informaţiei, totuşi, o uniformizare a modelelor culturale şi de civilizaţie continua sa rămână un obiectiv greu de atins. în acest sens, în literatura de specialitate se afirma ca "globalizarea poate fi măsurata în funcţie de gradul în care depăşirea distantei fizice e însoţita de depăşirea distantei culturale" (a se vedea J. Tomlinson, *Globalizare şi cultura,* Editura Amarcord, Timişoara, 2002, p.15).

acestui demers este acela de a obstacula formarea unei subculturi în rândul utilizatorilor de servicii Internet, care, altminteri, ar contribui la proliferarea abuzurilor împotriva copiilor.

În aceasta abordare, prevederile Articolului 9 alin.2 lit.b) şi c) din Convenţie includ în sfera noţiunii de "pornografie infantila" înfăţişarea vizuală:
- a unei persoane care pare să fie un minor având un comportament sexual explicit;
- a unei imagini reale care reprezintă un minor având un comportament sexual explicit.

În prima situaţie, este vorba despre o persoana care, în mod obiectiv, este adultă dar care prezintă aparentele înfăţişării unui minor. Concret, ar putea fi vorba despre persoane peste 18 ani, dar a căror evoluţie fizica nu reflectă, în *mod evident,* vârsta adultă, fiind confundabili cu minori. Credem ca este inutil sa subliniem problemele de interpretare ce se vor degaja în situaţii de acest tip, chiar daca, principial, argumentele pentru incriminarea şi a acestei forme de pornografie ni se par a fi valide. Care vor fi insa modalităţile practice capabile să ateste, fără dubiu, "aparentă" (contradicţia în termeni este evidentă) că persoana înfăţişată este un minor şi ce mijloace vor putea sta la îndemâna făptuitorului pentru a înlătura răspunderea penală? Dincolo de problematica penala şi procesual penala incidenţa, apreciem ca aceasta maniera de reglementare îngustează în mod considerabil sfera libertăţii de exprimare, până la un punct în care discuţia asupra constituţionalităţii unei astfel de norme penale devine greu de ocolit.

În cea de a doua situaţie, avem de-a face cu producţii pornografice (aşa-numita *"pornografie sintetica")* create prin combinarea imaginilor unui adult având un comportament sexual explicit, dar peste a cărui fizionomie a fost suprapus, prin mijloace cibernetice, chipul unui minor *(Computer Generated Porn).* Şi în acest caz, deşi la realizarea producţiilor pornografice nu au fost

folosiţi copii, totuşi, rezultatul obţinut este de natura să încurajeze pedofilia şi exploatarea sexuala a minorilor.

Extinderea prohibiţiei şi asupra acestor genuri de pornografie a avut deja rezonanta în practica de drept constituţional. În Statele Unite ale Americii, în mai multe rânduri, instanţele judecătoreşti, inclusiv Curtea Supremă, au avut a se pronunţa asupra plângerilor de neconstituţionalitate îndreptate contra unor reglementari federale şi statale, care adoptaseră aceasta opţiune de politica legislativa încă înainte de semnarea Convenţiei Consiliului Europei.

Din suita argumentelor formulate de instanţe, în sensul susţinerii neconstituţionalităţii reglementarilor care incriminau pornografia infantila bazata pe aparenta imaginilor şi sintetizarea de imagini, am reţinut următoarele:

- este inadmisibila incriminarea unei fapte intr-o maniera vaga, de natura sa lase destinatarul normei "sa ghicească" ce conduita este permisa şi ce acţiuni se situează în sfera ilicitului penal;
- efectele nocive ale pornografiei depind de intermedierea mentala, de modul în care o persoana răspunde la stimuli sexuali; or, daca admitem ca procesul de condiţionare a reacţiilor este guvernat de exprimarea unor idei şi gânduri, atunci libertatea de exprimare ar trebui practic suprimata;
- formulări de genul "pare sa fie" *("appears to be") şi* "lasă impresia ca" *("conveys the impression of")* sunt prea vagi, iar dispoziţiile penale în care sunt incluse ar putea determina oricând interzicerea unor producţii de la Hollywood (gen *"American Beauty ");*
- există o serie de lucruri nevinovate, cum ar fi desenele animate, jocurile video şi bomboanele, care, în condiţii determinate, ar putea fi folosite în scopuri imorale; cu toate acestea, nu putem accepta ca ele sa fie interzise, deoarece ar putea fi utilizate abuziv;
- Primul Amendament este periclitat cel mai mult atunci când legea încearcă să controleze gândul; dreptul de a gândi este începutul libertăţii, iar exprimarea

gândurilor se impune a fi ocrotita în fata restricţiilor, întrucât ea reprezintă începutul gândirii.

Instanţele judecătoreşti la care ne-am referit au recunoscut ca imaginile aparente şi cele sintetizate de pornografie infantila sunt repudiabile din punct de vedere moral, dar nu au reuşit sa concilieze acest aspect cu o valoare constituţionala sacra a democraţiei americane - libertatea de exprimare. Este important de menţionat ca soluţia adoptata în final a fost precedată de hotărâri divergente ale instanţelor inferioare, de opinii separate, inclusiv în rândul judecătorilor Curţii Supreme. Aceasta realitate indică, o data în plus, dificultatea realizării echilibrului între valori constituţionale concurente şi ar trebui să determine o reacţie prudentă şi echilibrată în orice demers legislativ şi procesual-penal de combatere a conţinuturilor negative.

Un factor pe care îl consideram demn de discutat este şi acela al *viabilităţii categoriilor juridice* de care dispunem, în vederea atingerii acestui echilibru dezirabil. Ne putem întreba în ce măsură conceptele fundamentale ale dreptului (ale dreptului constituţional şi ale celui penal, în particular) sunt, actualmente, suficient de profunde şi, totodată, ample, pentru a le putea utiliza în procesul de argumentare, pe marginea problematicii generate de dezvoltarea impetuoasa a tehnologiilor informaţiei. îndrăznim sa afirmam ca aceste categorii au astăzi tendinţa de a rămâne în urma realităţilor obiective.

De aceea, pentru a determina o viziune corecta, rezonabila şi cat mai puţin controversata asupra subiectului pe care îl analizam, inclusiv în scopul remodelării unei legislaţii care, din raţiuni cunoscute, a fost impusa cu prea mare repeziciune, este necesara, după părerea noastră, reevaluarea aparatului conceptual existent şi articularea unor elemente teoretice menite să contribuie la formularea unor categorii moderne ale dreptului constituţional şi ale dreptului penal.

. Pentru a putea atrage răspunderea penală, Convenţia prevede că faptele incriminate trebuie să fie săvârşite cu "intenţie" şi "fără drept". Raportul Explicativ subliniază (pct.103) că termenul "fără drept" îngăduie statelor-părţi la Convenţie să ia în considerare drepturi şi libertăţi fundamentale, cum sunt libertatea de gândire, libertatea de exprimare şi protecţia sferei private, care, în circumstanţe determinate, să se poată constitui în cauze care înlătură caracterul penal al faptei.

În ceea ce priveşte necesitatea comiterii faptelor cu intenţie, Raportul Explicativ nu aduce precizări suplimentare, mai ales în legătură cu faptul dacă este avută în vedere şi *intenţia indirectă.* Poate că acest aspect ar merita aprofundat, în sensul de a stabili în ce măsura Internetul - prin specificul sau, acela de a nu putea oferi informaţii precise asupra naturii unui conţinut, decât în mod treptat, prin parcurgerea traseelor informaţionale, de la un link la altul - este compatibil cu o teorie a răspunderii penale întemeiata pe ideea de vinovăţie inclusiv în forma intenţiei indirecte. Aminteam mai sus despre posibilitatea accesării accidentale a unor conţinuturi ilegale, chiar şi în cadrul serviciilor oferite de furnizori de prestigiu, de riscul imposibilităţii recunoaşterii unui conţinut determinat, în funcţie de titulatura mai mult sau mai puţin criptică a unei adrese URL ori a unei pagini Web, mai cu seamă dacă aceasta din urmă este într-o limbă necunoscută utilizatorului.

Referitor la problematica săvârşirii faptelor "fără drept", înţelegem să evocam un aspect care suscită, la rândul sau, o serie de discuţii şi care, de curând, a fost oglindit intr-o decizie de speţa. Este vorba despre aşa-numitul fenomen de *"Internet Entrapment",* constând în masuri adoptate de autorităţile publice în vederea descurajării pornografiei infantile în teritoriul virtual.

În concret, agenţi de politie sub acoperire săvârşesc, "cu drept", fapte de natura celor incriminate de Convenţie, oferind materiale pornografice cu minori, organizând capcane şi incitând diverşi utilizatori sa se angajeze în practici pedofile. Fără a subestima eforturile politiei, de depistare şi anihilare a vastelor

reţele având ca obiect traficul cu astfel de materiale, zelul apărătorilor legii ajunge, în anumite împrejurări, să fie, el însuşi, generator de criminalitate în rândul unor utilizatori situaţi în afara profilului specific de infractor.

Aceasta acţiune de impunere a legii - care, uneori, este greu de distins de instigarea la săvârşirea de infracţiuni - mizează pe ceea ce Internetul exploatează în cea mai mare măsura în materie de libertate a exprimării: *curiozitatea utilizatorilor*. Spre deosebire de interesul manifestat de o persoana în răsfoirea unor ziare şi reviste aşezate pe taraba sau în căutarea unor titluri de pe rafturile librăriilor şi din fişierele bibliotecilor, interesul specific al navigatorilor adânciţi în zona conţinuturilor virtuale este puternic exacerbat. Posibilitatea de a sari de la un conţinut la altul, intr-o diversitate tematica fără precedent, prin parcurgerea rapida a mii şi mii de conexiuni, de a te lasă surprins de "ceea ce urmează", de a nu întâmpina restricţii de ordin material - toate acestea inflamează curiozitatea, dezvolta fantezii, amplifica trebuinţe, duc la pierderea noţiunii timpului si, în multe cazuri, la "dependentă de reţea" sau, în alţi termeni, la ceea ce psihologii au ajuns sa numească *Internet Addiction Disorder (IAD)*[6]. Afirmându-şi gusturile, trebuinţele şi fanteziile în nesfârşitele căutări de conţinuturi, utilizatorul se expune manipulărilor şi îşi reduce capacitatea de a se autocenzura.

Pe acest fond, şansa de a determina un utilizator sa se abată de la normele sale obişnuite de conduita si, mai mult, de la prevederi legale pe care adesea nu le cunoaşte, nu le înţelege ori, dacă le cunoaşte şi le înţelege, nu are certitudinea interpretării lor corecte, este extrem de ridicata.

[6] A se vedea, cu privire la analiza acestui sindrom psihic, J.M. Grohol, *Internet Addiction Guide,* 2003, studiu disponibil la adresa http://psychcentral.com/netaddiction/ şi R.A. Davis, *Internet Addiction*, materiale disponibile la adresa http://www.internetaddiction.ca/

BIBLIOGRAFIE

LEGISLAŢIE

- CONSTITUŢIA ROMÂNIEI, republicată, emitent: ADUNAREA CONSTITUANTĂ; publicată în: MONITORUL OFICIAL nr. 767 din 31 octombrie 2003
- CODUL PENAL AL ROMÂNIEI, republicat, emitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 65 din 16 aprilie 1997
- LEGE nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei; emitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 279 din 21 aprilie 2003
- LEGE nr. 64 din 24 martie 2004 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică adoptată la Budapesta la 23 noiembrie 2001; emitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 343 din 20 aprilie 2004
- LEGE nr. 365 din 7 iunie 2002 privind comerţul electronic, emitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 483 din 5 iulie 2002
- HOTĂRÂRE nr. 1.308 din 20 noiembrie 2002 privind aprobarea Normelor metodologice pentru aplicarea Legii nr. 365/2002 privind comerţul electronic; emitent: GUVERNUL; publicat în: MONITORUL OFICIAL nr. 877 din 5 decembrie 2002
- LEGE Nr. 8 din 14 martie 1996 privind dreptul de autor şi drepturile conexe; emitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL NR. 60 din 26 martie 1996, modificată de LEGEA nr. 285 din 23 iunie 2004 pentru modificarea şi completarea Legii nr. 8/1996 privind dreptul de autor şi drepturile conexe; emitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 587 din 30 iunie 2004; ORDONANŢA DE URGENŢĂ nr. 123 din 1 septembrie 2005 pentru modificarea şi completarea Legii nr. 8/1996 privind dreptul de autor şi drepturile conexe; emitent: GUVERNUL; publicat în: MONITORUL OFICIAL nr. 843 din 19 septembrie 2005
- LEGE nr. 196 din 13 mai 2003 privind prevenirea şi combaterea pornografiei; etnitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 342 din 20mai 2003; modificată de LEGEA nr. 496 din 12

noiembrie 2004 pentru modificarea şi completarea Legii nr. 196/2003 privind prevenirea şi combaterea pornografiei; emitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 1.070 din 18 noiembrie 2004

- ORDONANŢA nr. 130 din 31 august 2000 privind regimul juridic al contractelor la distanţă; emitent: GUVERNUL; publicat în: MONITORUL OFICIAL nr. 431 din 2 septembrie 2000, modificată de LEGEA nr. 51 din 21 ianuarie 2003 pentru aprobarea Ordonanţei Guvernului nr. 130/2000 privind regimul juridic al contractelor la distanţă; emitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 57 din 31 ianuarie 2003
- LEGE nr. 455 din 18 iulie 2001 privind semnătura electronică; emitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 429 din 31 iulie 2001
- ORDIN nr. 389 din 27 iunie 2007 privind procedura de avizare a instrumentelor de plata cu acces la distanta, de tipul aplicaţiilor Internet-banking, home-banking sau mobile-banking; emitent: MINISTERUL COMUNICAŢIILOR ŞI TEHNOLOGIEI INFORMAŢIEI; publicat în: MONITORUL OFICIAL nr. 485 din 19 iulie 2007
- REGULAMENT nr. 4 din 13 iunie 2002 privind tranzacţiile efectuate prin intermediul instrumentelor de plată electronică şi relaţiile dintre participanţii la aceste tranzacţii; emitent: BANCA NAŢIONALĂ A ROMÂNIEI; publicat în: MONITORUL OFICIAL nr. 503 din 12 iulie 2002
- LEGE nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date; emitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 790 din 12 decembrie 2001
- LEGE nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice; emitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 1.101 din 25 noiembrie 2004
- LEGE nr. 102 din 3 mai 2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal; emitent:' PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 391 din 9 mai 2005
- LEGE nr. 451 din 1 noiembrie 2004 privind marca temporală; emitent: PARLAMENTUL; publicat în: MONITORUL OFICIAL nr. 1.021 din 5 decembrie 2004

- LEGE nr. 589 din 15 decembrie 2004 privind regimul juridic al activităţii electronice notariale; emitent: PARLAMENTUL; publicat în: MONITORUL OFICI AL nr. 1.227 din 20 decembrie 2004

TRATATE, CURSURI, MONOGRAFII, ARTICOLE ROMÂNEŞTI

- G.Rătescu, L. Ionescu-Dolj, I.Gr. Perieteanu, V. Dongoroz, HL.Asnavorian, M. Papadopolu, N. Pavalescu, Codul penal adnotat, vol.I (partea generală), voi.II şi III (partea specială), Editura Librăriei, Socec, Bucureşti, 1937
- L.Vasiliu, D. Pavel, G. Antoniu, D. Lucinescu, V. Papadopol, V. Rămureanu,
- codul penal comentat şi adnotat, partea generală, Editura Ştiinţifică şi enciclopedică, Bucureşti, 1972
- L. Vasiliu şi colaboratorii, Codul penal comentat şi adnotat, partea specială, Vol. I, Editura Ştiinţifică şi Enciclopedică, Bucureşti, 1975
- L. Vasiliu şi colaboratorii, Codul penal comentat şi adnotat, partea specială, Vol II, Editura Ştiinţifică şi Enciclopedică, Bucureşti, 1977
- V. Dongoroz, S.Kahane, L. Oancea, L. Fodor, N. Iliescu, C. Bulai, R..Stănoiu,
- Aplicaţii teoretice ale codului penal român, partea generală, vol.I, Editura Academiei, Bucureşti, 1969
- V. Dongoroz, S. Kahane, I. Oancea, I. Fodor, N. Iliescu, C. Bulai, R. Stănoiu,
- Aplicatii teoretice ale codului penal român, partea generală, vol.II, Editura Academiei, Bucureşti, 1970
- V. Dongoroz, S. Kahane, I. Oancea, I. Fodor, N. Iliescu, C. Bulai, R. Stănoiu, , Explicaţii teoretice ale Codului penal român, voi.III., Partea specială, Editura Academiei, Bucureşti, 1971
- V. Dongoroz, S. Kahane, I. Oancea, I. Fodor, N. Iliescu, C. Bulai, R. Stănoiu, Explicaţii teoretice ale codului penal român, voi. IV, Editura Academiei Române, Bucureşti, 1972
- V. Dongoroz, Drept penal (reeditarea ediţiei din 1939), Asociaţia Română de Ştiinţe Penale, Bucureşti, 2000
- Ion Neagu, Drept procesual penal. Tratat, Editura Global Lex, Bucureşti, 2002
- Al. Boroi, Ghe. Nistoreanu, Drept penal, partea generală, Editura AllBeck Bucureşti, 2004
- Dobrinoiu, G.Nistoreanu, I.Pascu, Al.Boroi, I.Molnar, V.Lazăr, Drept penal, partea generală, Editura Europa Nova, Bucureşti, 1997
- M. Zolyneak, Drept penal, partea generală, Editura Fundaţiei Chemarea, Iaşi, vol.I 1992, vol.II 1992, vol.III 1993

- C. Bulai, Manual de drept penal, partea generală, Editura All, Bucureşti, 1997
- T. Dima, Drept penal, partea generală, vol.I 2004, vol.II 2005, Editura Lumina Lex, Bucureşti
- V. Dobrinoiu, W. Brânză, Drept penal, partea generală, Editura Lumina Lex, Bucureşti, 2003
- F.Streteanu, Drept penal, partea generală, Editura Rosetti, Bucureşti, 200
- AI. Boroi, Ghe. Nistoreanu, Drept penal, partea specială, Editura AllBeck, Bucureşti, 2004
- V. Dobrinoiu, Drept penal, partea specială, vol.I, Editura Lumina Lex, Bucureşti, 2004
- V. Dobrinoiu, N. Conea, C.R. Romiţan, M. Dobrinoiu, N. Neagu, C.
- Tănăsescu, Drept Penal Partea Specială voi. II, Ed. Lumina Lex, 2004
- V. Dobrinoiu, Drept Penal - Partea Specială. Teorie şi Practică Judiciară, Ed. Lumina Lex, 2002
- Toader, Drept penal, partea specială, Editura AllBeck, Bucureşti, 2002
- V. Lazăr, Drept penal, partea specială, Editura AllBeck, Bucureşti,
- Antoniu, C. Bulai, Practica judiciară penală, vol.I, partea generală, Editura Academiei, Bucureşti, 1988
- Antoniu. C. Bulai, Practica judiciară penală, vol.II, partea generală, Editura Academiei, Bucureşti, 1990
- Antoniu, C. Bulai, Practica judiciară penală, vol.III, partea specială, Editura Academiei, Bucureşti, 1992
- Dobrinoiu şi colaboratorii, Cauze penale comentate, partea specială, Bucureşti, 2003
- Toader, Drept penal, partea specială, culegere de probleme din practica judiciară, Editura All Beck, Bucureşti, 2003
- Antoniu, E. Dobrescu, T. Dianu, G. Stroe, T. Avrigeanu, Reforma legislaţiei
- , Editura Academiei, Bucureşti, 2003
- I.Vasiu, Criminalitatea Informatică, Ed. Nemira, 1998
- I.Vasiu, L. Vasiu, Informatica Juridică şi Drept Informatic, Ed. Albastră, 2002
- I.Vasiu, Drept şi Informatică. Protecţia juridică a programelor, Studii de drept Românesc, Ed. Academiei Române, 1993
- Amza, CP. Amza, Criminalitatea Informatică, Ed. Lumina Lex, 2003
- I.Vasiu, Totul despre Hackeri, Ed. Nemira, 2001
- L. Vasiu, I. Vasiu, INTERNET- Ghid de navigare, Ed. Albastră, 1996
- D. Oprea, Protecţia şi Securitatea Informaţiilor, Ed. Polirom, 2003
- C. Troncotă, Neliniştile Insecurităţii, Ed. Tritonic, 2005

- V. Hanga, Dreptul şi calculatoarele, Ed. Academiei Române, 1991
- L. Bird, Internet. Ghid complet de utilizare, Ed. Corint, 2004
- W. Odom, Reţele de calculatoare, Ed. Corint, 2004
- V.V. Patriciu, Criptografia şi securitatea reţelelor de calculatoare, Ed. Tehnică, 1994
- L. Klander, Anti-Hacker, 1999
- G. Antoniu, Noul cod penal. Codul penal anterior. Studiu comparativ, Editura AllBeck, Bucureşti, 2004
- C. Barbu, Aplicarea legii penale în spaţiu şi timp, Editura Ştiinţifică, Bucureşti, 1972
- G. Antoniu, Vinovăţia penală, Editura Academiei Române, Bucureşti, 1995
- Streteanu, R. Chiriţă, Răspunderea penală a persoanei juridice, Editura Rosetti, Bucureşti, 2002
- F. Streteanu, Concursul de infracţiuni, Editura Lumina Lex, Bucureşti, 1997
- Mircea, Vinovăţia în drept penal român, editura Lumina Lex, Bucureşti, 1998
- V. Papadopol, D. Pavel, Formele unităţii infracţionale în dreptul penal român, Editura Şansa, Bucureşti, 1992
- V. Dobrinoiu, Traficarea funcţiei şi a influenţei în dreptul penal, Editura Ştiinţifică şi Enciclopedică, Bucureşti, 1983
- V. Dobrinoiu, Corupţia în dreptul penal român, Editura Lumina Lex, Bucureşti, '95
- Costică Voicu şi colaboratorii, Globalizarea şi criminalitatea economico-lanciară, Editura Universul Juridic, Bucureşti, 2005
- Balaban, Infracţiuni prevăzute în legi speciale care reglementează domeniul Comerţului, Editura Rosetti, Bucureşti, 2005
- Tratate, cursuri, monografii, articole străine
- Vonin, Precis de droit penal special, Ed. Dalloz, Paris, 1953
- Veron, Droit penal special, Armând Colin, Paris, 1998
- Bainbridge, Computers and the Law, Ed. Pitman, Londra, 1990
- Bertrand, Les contracts informatiques, Ed. Les Paques, Paris, 1983
- Bertrand, Protection juridique du logiciel, Ed. Les Paques, paris, 1984
- ,L. Le Moigne, La Modelisation des Systemes Complexes, Ed. Dunod, 1990
- ,L. Le Moigne, Systemique et Complexite, Revue Internationale de Systemique, 1990
- L. Le Moigne, Traduction de Sciences des Systenmes, Sciences de l artificiel, Ed. Dunod, 1991
- C. Lugan, La systemique sociale, Ed. PUF, 1993

- L von Bertalanffy, General System Theory: Foundations, Development, Applications, New York, 1968
- L. von Bertalanffy, The Organismic Psychology and Systems Theory, Worcester, 1968
- L. von Bertalanffy, Theorie des Systemes, Ed. Dunod, 1973
- L. von Bertalanffy, Perspectives on General Systems Theory, Scientific-Philosophical Studies, New York, 1975
- J. de Rosnay, Le macroscope vers un vision globale, Paris, Seuil, 1975
- E. Morin, La metode, Ed. Dunod, 1991
- B. Walliser, Systemes et Modeles. Introduc tion critique a l 'analyse de systemes, Seuil, 1977
- Y. Barel, Prospective et analyse de systeme, Documentation francaise, 1971
- E. Friedberg, Politiques urbaines et strategies corporatives, Ed. Sociologie du Travail, 1969
- Friedberg, Les organisations et la mutaţi on informatique, Ed. Education permanente, 1983
- E. Friedberg, L 'acteur et le systeme, Paris, Seuil, 1981
- W.R. Ashby, Introduction to Cybernetics, Chopman&Hall, 1956
- W.R. Ashby, Principles of Self-Organizing Systems, US Office of Naval Research, 1962
- E.F. Codd, A Relaţional Model of Data for Large SharedData Banks, 1970
- E.F Codd, Further normalization of the Data Base Relaţional Model, IBM research Report, 1971
- E.F Codd, Relaţional DataBase: A Practicai Foundation, ACM, 1982
- A.. Aulin, The Cybernetics Laws of Social Progress, Oxford, 1982
- M. Eigen, P. Schuster, The Hypercycle: A Principie of natural self-organization, Springer, Berlin, 1979
- M. Mirapaul, Kosovo Conflict Inspires Digital Art Projects, New York Times Cybertimes), April 15, 1999.
- McShane, Yugoslavs Condemn Bombs Over E-mail to U.S. media, Nando Times, April 17, 1999, www.nandotimes.com.
- J. Pollock, A. Petersen, Unsolicited E-Mail Hits Targets in America in First Cyberwar, Wall Street Journal, April 8, 1999
- Montgomery, Enemy in Site - // 's Time to Join the Cyberwar, Daily Telegraph, Australia, April 19, 1999.
- Verton, Net Service Shields Web Users in Kosovo, Federal Computer Week, April 19, 1999.
- V. Rodger, Online Hiiman-Rights Crusaders, USA Today, August 25, 1999.

- Lohr, Go Ahead, Be Paranoid: Hackers Are Out to Get Yon, New York Times, March 17, 1997.
- Arquilla, D. Ronfeldt, M. Zanini, Networks, Netwar, and Information-Age Terorism, Countering the New Terrorism, RÂND, 1999
- L. Staten, Testimony before the Subcommittee on Technology, Terrorism and Government Information, U.S. Senate Judiciary Committee, February 24, 1998.
- Whitelaw, Terrorists on the Web: Electronic Safe Haven, U.S. News & World Report, June 22, 1998
- Oaks, Every Web Site a Chat Room, Wired News, June 14, 1999.
- Stone, Profto BuildArchive of Insurgency Groups, Newsbytes, March 3, 1999.
- Harris, Web Becomes a Cybertool for Politica/ Activists, Wall Street Journal, August 5, 1999
- Ungoed-Thomas, M. Sheehan, Riot Organisers Prepare to Launch Cyber War City, Sunday Times, August 15, 1999.
- Boyle, Crypto Can Save Lives, ZDNet, January 26, 1999
- Fairley Raney, Flood of E-Mail Credited with Hal ting U.S. Bank Plan, The New York Times (Cybertimes), March 24, 1999.
- Harris, Web Becomes a Cybertool for Political Activists, Wall Street Journal, Agust 5, 1999
- J. Gurak, Persuasion and Privacy in Cyberspace, Yale University Press, 1997.
- Edward Harris, Web Becomes a Cybertool for Political Activists, Wall Street Journal, August 5, 1999
- D,Renfeldt, J. Arquilla, Graham E. Fuller, M. Fuller, The Zapatista A Social Netvor, RÂND Report MR-994-A, 1998.
- N.McKay, Pentagon Deflects Web Assault, Wired News, September 10, 1998.
- R.Alison, Belgrade Hackers Bombard MoD Website in First Internet War, PA New,March31, 1999.
- E-Mail Attack on Sri Lanka Computers, Computer Security Alert, No. 183, Computer Security Institute, June 1998
- J.Wolf, First Terrorist Cyber-AttackReportedby U.S., Reuters, May 5, 1998.
- P.Rey, E-Strikes and Cyber-Sabotage: Civilian Hackers Go Online to Fight, Fox News, April 15, 1999.
- R.Wesly, Controversial Basque Web Site Resurfaces, Wired News, August 28,
- Y.Brides, The Zorros of the Net, Le Monde, November 16, 1997
- Anti Terrorist Squad Orders Political Censorship of the Internet, press release from Internet Freedom, September 1997.

- L.Murdoch, Computer Chaos Threat toJakarta, Sydney Morning Herald, August 18.1999
- .Williams, Federal Web Sites Under Attack After Embassy Bombing Newsbytes, May 10, 1999
- Barr, Anti-NATO Hackers Sabotage 3 Web Sites, Washington Post May 12 1999.
- Elton, Hacking in the Name of Democracy in China, The Toronto Star, July 4 1999.
- Taylor, CDC Says Hackers Are the Threat, IT Daily, August 26, 1999.
- Glave, Confusion Over Cyberwar, Wired News, January 12, 1999.
- Huang, Hackers War Erupts Between Taiwan, China, Associated Press, Taipei, Taiwan, August 9, 1999.
- Beijing Tries to Hack U.S. Web Sites, Associated Press, July 30, 1999
- Bridis, Hackers Become An Increasing Threat, Associated Press, July 7, 1999.
- Gross, Israeli Claims to Have Hacked Saddam Off the Net, London Sunday Telegraph, February 7, 1999.
- Colin, The Future of Cyberterrorism, Crime and Justice International, March 1997
- M. Pollitt, Cyberterrorism Fact or Fancy? Proceedings of the 20th National Information Systems Security Conference, October 1997
- Computers at Risk, National Academy Press, 1991.
- Church, Information Warfare Threat Analysis for the United States of America, Part Two: How Many Terrorists Fit on a Computer Keyboard'? Journal Infrastructural Warfare, Summer 1997.
- Soo Hoo, S. Goodman, L. Greenberg, Information Technology and the Terrorist Threat, Survival, Voi 39, No. 3, Autumn 1997
- Critical Foundations: Protecting America 's Infrastructures, The Report of the President's Commission on Criticai Infrastructure Protection, October 1997,Report Summary, http://www.pccip.gov.
- Protecting America 's Criticai Infrastructures: PDD 63, The White House, May 22.1998
- CIWARS Intelligence Report, Centre for Infrastructural Warfare Studies, June 21,1998
- PentagonComputer Systems Hacked, Info Security News, June 1998;
- D.Paternak, B. B. Auster, Terrorism at the Touch of a Keyboard, U.S. News & World Report, July 13,1998

RESURSE INTERNET:

1. http ://www. crime-reasearch. org
2. http ://cvberpolice. over-blog. corn

3. http://foldoc.doc.ic.ac.uk
4. http ://w ww .mir. es/policia
5. http ://www. efrauda.ro
6. http://www. ic3. gov Internet Crime Complaint Centre
7. http://www.internetcrimeforum.org.uk
8. http://ifccfbi.gov Internet Fraud Complaint Centre
9. http: //www. internetidentitv. corn Anti-phishing Consultancy
10. http: //www. interpol. int/Public/Technolo gyCrime
11. http://www.nhtcu.org National High Tech Crime Unit (UK)
12. http://www.webopedia.com Webopedia
13. http: //www .netintercept. corn Computer Forensics
14. http://www. forensicon. corn E-discovery Specialists
15. http://www.world-check.com Terrorist Profite
16. http ://www. centrex.police.uk Central Police Training and Development Authority
17. http: //www. hightechcrimeinstitute. corn
18. http://www.computerworld.com/securitv
19. http: //www. wikien. info
20. http://www.legalmountain.com Computer Crime Legislation
21. http://www .ncalt.com National Centre for Applied Learning Technologies
22. http://www, govtsecuritv.com
23. http://www.federalcrimes.com
24. http://www.scams.net
25. http://www.anti-spy.info
26. http://www.acunefix.com
27. http://rhizome.org/carnivore
28. http://wvvw.pewintemet.org
29. http://www.kindercam.com
30. http://www.epic,org Centru de Informare pentru Confidenţialitate Electronică
31. http ://www. eff.org/Pri vacy Electronic Frontier Foundation
32. http://www privacyalliance.org Online Privacy Alliance
33. http://www.fbi.or g/hq/lab/Carn i vore Carnivore Diagnostic Tool
34. http://www.cdt.org Centrul pentru Democraţie şi Tehnologie
35. http://www. stopcami vore. org
36. http ://www .pri vacyfoundation.org/workplace
37. http://vvvvw.indentix.com
38. http: //www. di gital persona. corn
39. http ://ww w. vi i sage. corn
40. http://www.gcn.com
41. http: //w w w. anonvmi zer, corn
42. http ://www. lin uxsecurirv. corn

43. http://www.w3.org/P3P Proiect Platforma pentru Preferinţe de Confidenţialitate
44. http://d1is.gseis.ucla.edu/people/pagre/bar code.html
45. http: //www. basel inemag. corn Projects Securi ty Cybercrime
46. http://www.field.associates.co.uk Computer Forensics
47. http://www.compendianet.com Computer Forensics
48. http ://w w w.idefense.com
49. http:// www.gmu.edu/security/practices George Mason University
50. http://www.cert.org Computer Emergency Response Team
51. http ://ww w. gocsi.com Institutul pentru Securitatea Calculatoarelor
52. http://www.safedwelling.com Id Theft Solutions
53. http ://w w w. infosy sec. org Securi ty Portal for Information System Security
54. http: //w w w. zybex. org
55. http: //w w w. iss.net Internet Security Solutions
56. http://www.securityfocus.com
57. http: //www. spidynamics. com
58. http://www.isec.pl iSec Securi ty Research
59. http ://ww w. global directs vcs. com.
60. http://www.accessdata.com
61. http://www.cs.georgetown.edu/-denniiig
62. http://www.cvberspacelaw.org
63. http://mobile.f-secure.com
64. http ://www .bitpipe.com/rlist/terni/cybert errorism.html
65. http ://enterprisesecurity. symantec.com/solutionfinder
66. http://www.psywarrior.com
67. http://www.nps.naw.mil/ctiw Centre on Terrorism and Iregular
68. Varfare
69. http://www.homelandsecurityx.com
70. http://cisr.nps.navy.mil Centre forinformation Systems Security Studies and Research
71. http: //www. infowarrior. org
72. http ://ww w .terrorism. corn
73. http ://www .thehackti vist, corn
74. http: //www. csis. org
75. http://www.nsa.gov
76. http: //www. thing .net/~rdom/ecd/EDTECD .html
77. http://www.gn.apc.org/pmhp/ehippies
78. http://www.telediritto.it
79. http://www.cirsfid.unibo.it/cirsfid
80. http://www.ciberspazioediritto.org
81. http://62.110.105.159/alsiud
82. http: //www. giustizia.it

83. http: //www. alfa-redi.org
84. http: //www. frammella.it
85. http: //www. interi ex.it
86. http: //www. ordineavocatimilano.it
87. http ://ww w. slentopoli.corn
88. http: //www. delitosinformaticos. corn
89. http ://www. cvberlawsa.co.za
90. http://www.lexinformatica.org/cybercrime
91. http://www.41aw.co.il
92. http ://www.wittys.com/files/mab Firewall Penetration Testing
93. http://is-it-true.org Hackers Tricks
94. http: //www. cs .princeton. edu/sip/pub/spoofing. html
95. http ://ori. careerexpo.com/pub/docsoft 197/spoof. soft, htm
96. http://www.engarde.com/software/ipwatcherrisks/overview.htm
97. http://gradeswww.acns.nwu.edu/ist/snap/doc/snirfing.htm
98. http ://www. cytechsys.com/detect.htm
99. http://www.kimsoft.com/Korea/usa-net.htm
100. http://www.observatoriodigital.net
101. http://www.itu.int/itut/studygroups/coml7/cssecurity.htm
102. http://www.learnsecurityonline.com
103. http://www. edu-central. corn
104. http://www.techlawed.org/page.php?v=24&c=28page=crime
105. http://www.acunetix.com
106. http://www.ssppyy.corn
107. http://www.tiac.net/users/smiths/aiion/anonprob.htni
108. http://www.îwf.org.uk Internet Watch Foundation
109. http://www.sparnhaus.or g/cyberattacks
110. http://www.govexec.com/storyjpage.
111. http://www.fcw.com/article88417-03-28-05
112. http://coiiventions.coe.int/Treatv/en
113. http://www.privacyinternational.org/issiies/cvbercrime
114. http://www.infinisource.com/features/cybercrime.html Premier Resource Center
114. http: //www. cvbercrime.admin.eh Switzerland Cyber crime Coordonaţi on Unit
115. http://www.nctp.org National Cybercrime Training Partnership
116. http://www.iislegal.acuk/cybercnme/cvbercrime.html
117. http://wvvw.bespacifk.coin/mt/archives/cat cybercrime.html
118. http ://www. forensics.nl
119. http://www. southeastcybercrimesiimmit.com
120. http://www.lib.msu.edti/liarris23/crimiiist/cvbercrim.html
121. http://www.icc-ccs.org/main International Chamber of Commerce Crime Services

122.http://cvber-riglits.org/cybercrinie
123.http://www.efa.org.au/Issues/Securirv Electronic FrontiersAustralia
124.http://www.îwar.org.uk/ecoespionage Information Warfare Site
125.http://www.digital-law.net/IJCLP/Cy_j004
126.http://vvvvw.intenietpolicv.net/cvbercrime Global Internet Policy Iniţiative
127.http://www.wgig.org/docs/WP cybersec.pdf
128.http://www.aph.gov.au
129.http://facultv.ncwc.edu/toconnor/315
130.http://www.iia.net.au/cvbercriinecode.htm
131.http://europa.eu.int/ISPO/eif/TnternetPoliciesSite/Crime/CrimeCommence.html
132.http://europa.eu.int/infonnation society/topics/telecomms/inteniet/crinie
133.http://www ,cvbertelecom.org/sectiritv/crime.html
134.http: //w w w. vaonl ine/doc _i nternet. htm
135.http ://www.cvbercrimelaw.net Legislaţie internaţională în domeniul criminalităţii informatice

..oo..