Internet-ul şi criminalitatea informatică

Prof. univ. dr. Dan Banciu

Conf. univ. dr. Ion Vlăduț

Internet-ul reprezintă o „rețea a rețelelor" informaționale care reuneşte câteva mii de rețele de ranguri diferite ce provin din zeci de țări ale lumii. Este o rețea virtuală forma1ă dintr-un număr în continuă creştere de rețele locale (*Local Area Network-LAN*) – publice şi private, rețele pe arii extinse (*Wide Area Network – WAN*), rețele regionale şi naționale interconectate [**1**].

Internet-ul reprezintă cel mai mare cartier al *Cyberspace*-ului şi pune la dispoziția utilizatorilor câteva categorii majore de servicii: *World Wide Web*-ul, *Electronic Mail*-ul, *Usenet*-ul, *Internet Relay Chat*-ul [**2**].

World Wide Web-ul reprezintă o "piață electronică" pentru bunuri, servicii şi o vastă gamă de aplicații. Aici, diferiți utilizatori îşi constituie *site*-uri, care se prezintă ca nişte "vitrine electronice" în *Cyberspace.*

Electronic mail-ul (prescurtat *e-mail*), adică "poşta electronică", este o "fiică" a tradiționalei poşte, care dă posibilitatea celor care au acces la Internet să comunice şi să transmită, cu o viteză remarcabilă şi un cost redus, diverse mesaje (texte scrise, grafică, imagini statice, imagini video) altor utilizatori ai rețelei, indiferent de fusul orar sau de zona geografică unde aceştia se află [**3**]. La mesajul *e-mail* transmis utilizatorul poate ataşa o fotografie sau un document (de exemplu, un studiu pe care un profesor îl trimite spre publicare la o revistă de specialitate). Este vorba despre un *Attached File* (fişier ataşat), care reprezintă o anexă electronică la mesajul trimis prin *e-mail*.

Usenet Newsgroups-ul (grupuri de ştiri Usenet) este constituit, după cum şi numele lui o sugerează, din grupuri de ştiri. Acestea sunt asemănătoare avizierelor dintr-un birou, unde fiecare poate citi anunțurile puse de alții şi poate pune el însuşi alte anunțuri.

Internet Relay Chat-ul (prescurtat, IRC – discuție în direct pe Internet) este format din mii de "camere de discuții" în care utilizatorii rețelei, tastându-şi mesajele, "stau de vorbă", în timp real, cu un grup de persoane sau cu o altă persoană.

Este indiscutabil faptul că, prin serviciile pe care le oferă, Internet-ul a adus şi aduce multiple avantaje cercetării ştiințifice, învățământului, administrației, afacerilor, comunicării inter-umane etc. Dar, Internet-ul a fost şi este pândit de mari pericole care-şi află sorgintea în faptul că această rețea, miraculoasă prin beneficiile care le aduce omului, reprezintă în acelaşi timp un mediu extrem de favorabil pentru cei care se dedau la comiterea unor fapte indezirabile social, fapte care se pot întinde de la acte teroriste până la hărțuirea sexuală sau diseminarea imaginilor pornografice. Conectându-se la această rețea cu ajutorul unui calculator (pe care a fost instalat în prealabil un program informatic

adecvat) şi al unui modem, prin intermediul unei simple linii telefonice, orice individ se poate afla la un "*click*" de crimă. Iar cei interesaţi de aceasta, acţionând şi într-un relativ anonimat, n-au întârziat nici o secundă să facă acest pas atât de mic. Mai exact spus, mulţi criminali de cele mai diverse tipuri şi ranguri şi-au mutat imediat (înainte ca sistemele de drept şi poliţieneşti să ajungă aici) "afacerile" pe terenul virgin al Internet-ului, reuşind să devină, în foarte scurt timp, mai eficienţi ca oricând în desfăşurarea acţiunilor lor socialmente periculoase. Deplasarea "afacerilor" criminale pe terenul Internet-ului nu s-a produs întâmplător, ci din raţiuni cât se poate de pragmatice, care ţin de faptul că "Această mega-reţea planetară prezintă practic cel puţin trei avantaje de marcă pentru escroci: abolirea distanţelor, costuri minime şi o faţadă şi mai anonimă" [4]. Din păcate, toate domeniile Internet-ului, atât de benefice pentru majoritatea zdrobitoare a utilizatorilor cinstiţi ai acestei reţele informaţionale, reprezintă, în acelaşi timp, câmpuri infracţionale dintre cele mai "mănoase" pentru cei interesaţi să le folosească în astfel de scopuri.

Toate serviciile oferite de Internet s-au bucurat şi se bucură de o atenţie din ce în ce mai mare din partea criminalilor. *World Wide Web*-ul este preferat pentru escrocheriile prin site-uri de *Web*. Infractorii înfiinţează un *site*, adună bani sau informaţii de identificare, după care "şterg" *site*-ul. Un escroc înfiinţează un *site* pentru a vinde produse la preţuri foarte mici, aproape prea frumoase pentru a fi adevărate. Cumpărătorul plăteşte, de obicei o sumă mult mai mică pentru un obiect care de fapt costă mult mai mult. Dar, în realitate, acesta primeşte un obiect care costă de câteva ori mai puţin decât a plătit el. Sau, infractorii înfiinţează *site*-uri pentru a colecta numere de cărţi de credit şi alte informaţii personale de la clienţi care sunt încredinţaţi că achiziţionează un bun sau un serviciu. În realitate, nu vor primi niciodată produsul sau serviciul comandat. Infractorul, însă, va vinde informaţiile altor infractori sau le va utiliza pentru propriile scopuri ilegale [**5**].

Electronic mail-ul este utilizat de infractori pentru a-şi promova activitatea prin trimiterea de mesaje către mii de adresanţi care nu le-au cerut. Practica de a trimite astfel de mesaje se numeşte *Spanning*.

La rândul lor, *Usenet Newsgroups*-urile sunt utilizate pentru a distribui pornografie cu copii sau pentru a pune copii la dispoziţia amatorilor de relaţii sexuale cu aceştia. Hoţii le folosesc pentru a face reclamă bunurilor furate, iar escrocii pentru a promova jocuri care asigură câştiguri "garantate" (cum ar fi schema de investiţii Ponzi) sau escrocherii de genul scrisorilor în lanţ [**6**].

Şi *Internet Relay Chat*-ul s-a dovedit un teren fertil pentru activităţile infracţionale. Astfel, pedofilii folosesc *chat-room*-urile pentru a-şi povesti aventurile sexuale, pentru a căuta noi victime în rândul copiilor şi al adolescenţilor, pe care, prin discuţii îndelungate, caută să-i ademenească la o întâlnire în lumea reală spre a avea relaţii sexuale cu ei. Escrocii, la rândul lor, caută în *chat-room*-uri persoane tentate de schemele lor de îmbogăţire rapidă sau de "oportunităţile" de afaceri pe care le oferă, iar toate categoriile de infractori interesaţi pot ţine "şedinţe" cu complicii lor pe canalele IRC, unde pot comunica, individual sau în grup, fără ca cineva să "vadă" ceea ce îşi transmit [**7**].

În condițiile în care, cu mijloace tehnice minime şi cheltuieli financiare aproape modice, orice utilizator poate intra în legătură cu rețeaua Internet, pentru a accesa o sumedenie de baze de date din întreaga lume, ne putem aştepta oricând ca un răuvoitor sau bolnav psihic, de oriunde de pe glob, să provoace pagube imense unor indivizi, comunități umane sau chiar state aflate la zeci de mii de kilometri distanță. În *Computers Crisis* (Computere în criză), un raport al Consiliului Național de Cercetare, se afirmă răspicat că „Teroristul zilei de mâine ar putea fi capabil să provoace daune mai mari cu un *keyboard* decât cu o bombă" [**8**].

Este din ce în ce mai evident că, în zilele noastre, grupările teroriste utilizează tot mai mult Internet-ul pentru a-şi atinge scopurile subversive. Majoritatea dintre ele sunt, de altfel, prezente pe Internet. Printre cel mai bine reprezentate sunt mişcările de gherilă latino-americane care dispun de o tehnică informatică de înaltă performanță şi, de multe ori, de masive finanțări ce provin din fondurile unor capi ai traficanților de droguri [**9**].

Ca toată lumea, de altfel, şi organizațiile teroriste utilizează Internet-ul, în primul rând, în calitatea sa de mijloc de comunicare. Prin *site*-urile pe care şi le-au creat pe *World Wide Web* aceştia îşi propagă intens ideologiile pe care le-au îmbrățişat, utilizând Internet-ul ca vector principal al legitimării lor ideologice [**10**]. Un exemplu în acest sens îl reprezintă organizația teroristă *Drumul luminos* din Peru, care, dispunând de un *site* pe *Web*, îşi promovează propria ideologie extremistă. Interesant este faptul că, aşa după cum constata fostul şef al operațiunilor F.B.I., Buck Revell, atâta timp cât mesajele acestor grupări fac numai propagandă pentru ideologia lor, fără să treacă la acțiuni criminale, teroriştii pot desfăşura liberi activități, astfel încât Internet-ul a devenit un adevărat „rai" pentru ei [**11**].

La rândul lor, simpatizanții diferitelor organizații teroriste, cu diferite ocazii, cum ar fi reuşita unor acțiuni ale acestora, construiesc *site*-uri de simpatie față de asemenea grupări. Astfel, imediat după ce gruparea teroristă *Tupac Amaru* a ocupat reşedința ambasadorului Japoniei în Peru, ținând ostateci membrii ambasadei şi pe invitații lor, în decembrie 1996, simpatizanții organizației menționate din S.U.A. şi Canada au realizat o serie de *site*-uri de simpatie pe Internet, prezentând în detaliu asaltul asupra ambasadei sau lăudând curajul şi „măiestria" teroriştilor [**12**].

Surprinzător este faptul că, în ceea ce priveşte pregătirea şi desfăşurarea acțiunilor teroriste clasice, dar şi a celor de natură informatică, orice individ amator de astfel de „distracții" care posedă un minimum de cunoştințe şi de deprinderi pentru a utiliza un computer, un *keyboard* şi un *mouse*, poate să obțină, de pe Internet, *know-haw*-ul de care are nevoie pentru atingerea scopurilor sale. Astfel, unele *site*-uri, uşor identificabile în această rețea, furnizează informații de ultimă oră cu privire la confecționarea bombelor, instrucțiuni privind manipularea substanțelor explozive şi rețetele necesare. Pe aceste *site*-uri pot fi găsite *Manualul teroristului* şi *Cartea de bucate a anarhistului*, în care este descris cu lux de amănunte modul de construire a mai multor tipuri de bombe [**13**]. Aceasta pentru a nu mai vorbi de acele pagini *Web* care prezintă ultimele tipuri de arme, informații paramilitare, tehnici de corupere sau ucidere a viitoarelor victime etc. Tot ceea ce este prezentat în astfel de *site*-uri beneficiază de imagini, scheme şi explicații amănunțite. Dar, în rețea se găseşte chiar mai mult decât atât, se găseşte şi o bună parte

din *know-haw*-ul de producere a armelor nucleare (poate nu atât de sofisticate), care se află la îndemâna tuturor doritorilor: terorişti, maniaci, instabili psihic sau state paria [14]. Din păcate, lucrurile nu se opresc la aceste activităţi care, de regulă, premerg acţiunile teroriste propriu-zise; ele merg mai departe, ajungând să incite la astfel de atacuri şi, în final, la organizarea şi desfăşurarea unor acte criminale grave.

O altă categorie de activităţi teroriste desfăşurate pe Internet o reprezintă diseminarea mesajelor de ură şi incitare la violenţă prin intermediul paginilor *Web*. Astfel, organizaţiile islamiste utilizează Internet-ul pentru a-şi disemina propaganda antievreiască şi antioccidentală. În acest scop, unele *site*-uri create de simpatizanţii mişcării Hamas cheamă la luptă împotriva evreilor şi preamăresc gloria de a muri în această luptă. De asemenea, în S.U.A., o mulţime de *site*-uri existente pe *World Wide Web* proclamă supremaţia albilor, iar gruparea teroristă *Alpha HQ* din Philadelphia publică pe paginile sale de *Web* diverse ameninţări, mesaje de hărţuire şi intimidare etnică, fapt ce l-a determinat, în octombrie 1999, pe procurorul general al statului Pensylvania, Mike Fisher, să prezinte o plângere împotriva acestei organizaţii. De altfel, aşa după cum constata Liga Antidefăimării din S.U.A., Internet-ul a devenit „un forum pentru grupările teroriste sau terorişti individuali" [**15**]. Întrucât în S.U.A. se consideră că informaţiile difuzate pe Internet ţin de dreptul la liberă exprimare, riposta autorităţilor faţă de construirea *site*-urilor de către grupările teroriste este destul de delicată. Astfel, în această ţară, deşi paginile *Web* ale grupărilor teroriste sunt publice, F.B.I.-ul nu are voie să facă dosare cu fişierele respective decât atunci când investighează un anumit caz care a fost aprobat de procuror.

Alţi sabotori de pe Internet au furat, într-un interval de două luni, toate *e-mail*-urile Centrului de Cercetări Atomice din India. Dar nu numai poşta electronică poate fi sabotată, ci şi *site*-urile de pe Internet, care constituie prăzi dintre cele mai uşoare pentru hackeri. De altfel, printre aceştia domneşte moda întrecerilor în imaginaţie pentru a sabota *site*-urile guvernamentale *Web*. Spre exemplu, în noaptea de 15 spre 16 august1996, un hacker a atacat *site*-ul *Web* al Ministerului Justiţiei din S.U.A. şi a transformat textele şi imaginile. În urma modificărilor făcute, Departamentul Justiţiei a devenit Departamentul Injustiţiei, locul fotografiei Procurorului general a fost luat de fotografia lui Adolf Hitler, împreună cu aceea a manechinului-vedetă de televiziune – Jennifer Aniston; iar întregul *site* a fost „completat" cu imagini pornografice şi zvastici [16]. La rândul lor, hackerii din ţara noastră au spart *site*-ul Ministerului de Finanţe şi au modificat informaţia guvernamentală în diferite moduri. Una dintre principalele modificări a foste adăugarea unei „taxe pe prostie", care trebuia să fie cu atât mai mare cu cât persoana era mai importantă. Banii încasaţi din această taxă urma să fie folosiţi pentru a mitui N.A.T.O. să ne primească la sânul său cu braţele deschise [**17**]!

Există însă temerea îndreptăţită că, depăşind astfel de manifestări ludice, hackerii vor merge mult mai departe şi vor modifica listele de preţuri, textele juridice sau chiar rezultatele cercetărilor ştiinţifice, ceea ce ar avea consecinţe mult mai grave [**18**].

Totodată, asistăm la o proliferare a atacurilor masive contra elementelor reţelei Internet. Sunt atacaţi furnizorii de acces la Internet, veritabile noduri fără de care nu ar putea fi posibil să se acceadă în reţea, prin bombardarea unui computer cu mesaje până acesta îşi

dă duhul. Dar cel mai mare pericol îl reprezintă faptul că teroriştii individuali sau grupările teroriste ar putea ataca şi penetra reţele de calculatoare importante ale statului. În condiţiile Internet-ului, teroriştii au acum posibilitatea de a lansa atacuri greu detectabile din orice punct al globului. Pot infecta sistemele informatice cu viruşi complecşi ceea ce ar putea provoca disfuncţionalităţi grave în sisteme. Conform unor estimări, pagubele aduse de celebrul virus „*I Love You*", lansat anul trecut la începutul lunii mai, sunt de ordinul miliardelor de dolari [**19**]. Bande teroriste, seniori ai narcoticelor sau unele state dedate la acte teroriste pot intra în reţeaua Internet şi sabota nodurile critice din foarte vulnerabilul sistem de comunicaţii şi legături prin satelit al unei ţări [**20**]. Ei pot lansa atacuri masive cu viruşi informatici asupra reţelelor de telecomunicaţii, de apărare, de alimentare cu energie electrică, gaze şi apă sau asupra sistemelor de dirijare a transporturilor aeriene, navale şi terestre, asupra sistemelor informatice din bănci, burse, societăţi de asigurări etc. Viaţa a demonstrat că chiar sistemele militare americane, care se presupune că sunt printre cele mai sigure din lume, prezintă cu regularitate semne de slăbiciune în faţa atacurilor informatice, adesea întreprinse de amatori cu motivaţii ludice, care aproape întotdeauna rămân surprinşi de amploarea şi consecinţele faptelor lor. De exemplu, în 1997, trei adolescenţi din portul Zadar din Croaţia, după ce au spart codurile de protecţie, au intrat în computerul Pentagonului şi au copiat fişiere confidenţiale privind bazele militare [**21**]. Ei au fost repede prinşi graţie urmelor lăsate pe Internet, dar fapta lor dovedeşte încă o dată vulnerabilitatea sistemelor informatice vitale ale unui stat de talia S.U.A. Un semnal de alarmă a tras şi liderul unui grup de crackeri chinezi, care, în 1999, a pretins că a accesat sistemele de securitate ale calculatoarelor care monitorizează sateliţii chinezi, ceea ce a dus la pierderea temporară a controlului acestora [**22**].

Din păcate, astfel de cazuri nu sunt puţine (numai în februarie 1999 au fost înregistrate 11 penetrări în reţeaua Pentagonului!) şi ele dovedesc tot mai mult că atacurile electronice, „viruşii" şi „bombele informatice" înfăptuite de mafioţi angajaţi alături de un guvern islamist, de piraţi informatici reconvertiţi la războiul economic sau la manipularea cursurilor bursiere şi la sabotaje distructive nu sunt nici pe departe pericole imaginare, ci cât se poate de verosimile [**23**].

În principiu, în cazul criminalităţi în domeniul reţelelor de date, în special în ce priveşte Internet-ul, se pot distinge infracţiunile care vizează paralizarea lor în întregime, a unor părţi ale acestora sau a unor structuri care lucrează cu ele, prin programe virusate sau cu atacuri DDoS prin Hacking [**24**].

Atacurile *Denial – of Service (DoS*) constau în inundarea unei adrese de IP (IP – *Internet Protocol* – număr de identificare a unui calculator sau alt tip de dispozitiv conectat direct la Internet) cu date, şi în consecinţă, blocarea lui şi a legăturii Internet. Cele mai multe atacuri DoS sunt lansate împotriva *site*-urilor *Web*, cu scopul de a împiedica vizitarea acestora de către utilizatorii obişnuiţi. Un astfel de atac a blocat *site*-urile Internet *Ebay* şi *Yahoo!* în februarie 2000, când bombardamentele din partea hackerilor au cauzat prăbuşirea respectivelor servere.

În acelaşi timp, pot fi lansate şi atacuri mai puternice de tipul DoS distribuit (DDoS), care constau în utilizarea mai multor calculatoare pentru un atac DoS. Hackerul comandă mai

multe calculatoare pe care le foloseşte ca platforme de lansare a atacului. Prin această manevră el ridică mult amploarea şi intensitatea atacului şi, în acelaşi timp, îşi asigură o mai bună protecţie a propriei identităţi.

La concluzii asemănătoare ajunge şi raportul Subcomisiei Senatului S.U.A. pentru investigaţii asupra securităţii, care consemnează faptul că „Istoria recentă arată că infractorii se adaptează rapid la instrumentele de comunicare anonime şi nedetectabile" [**25**]. Organizaţiile criminale s-au convertit cu o viteză uimitoare la tehnologiile actuale cele mai sofisticate. Spre exemplu, ele folosesc programele informatice de criptografiere pentru a comunica pe Internet cu o marjă foarte mare de siguranţă sau, aşa după cum recunoşteau autorităţile columbiene, una dintre noile grupări apărute la Cali, după loviturile date cartelurilor din această zonă, a utilizat Internet-ul pentru a-şi extinde şi coordonarea traficului de droguri [**26**]. La rândul lor, „şefii Mafiei italiene, în general inteligenţi şi abili, au observat deja, sau vor înţelege mai devreme sau mai târziu, enormele posibilităţi oferite de informatică, de reţele şi, mai ales, de Internet" [**27**]. Dar, Internet-ul constituie un mijloc formidabil şi pentru bandele organizate care se ocupă cu traficul ilegal de arme, de medicamente, cu spălarea enormelor sume de bani murdari ş.a [28]. Există suficiente motive care ne îndreptăţesc să credem că această formă atât de gravă a infracţionalităţii, care este crima organizată, s-a orientat hotărât spre Internet şi alte înalte tehnologii conexe acestei reţele. Un astfel de motiv constă în faptul că pentru grupările crimei organizate Internet-ul reprezintă un mijloc ideal de comunicare rapid, ieftin şi destul de sigur în condiţiile utilizării programelor informatice de criptografiere. Astfel, în ianuarie 1996, mai multe grupări criminale din Detroit au creat un *site Web*, pe care, după 3 luni, când acesta a fost închis de prestatorul de servicii, l-au mutat la un furnizor din Noua Zeelandă. „Denumit <<Glock 3>> acest *site* avea rolul de releu între bandele din lumea întreagă, de la *West Side Crips* din Phoenix, până la *Lil Shorty's* din Londra sau chiar *Gangster's Disciples* din Chicago. Căci în Statele Unite proliferează *Street gang*-urile (bandele de stradă)" [**29**].

Piratarea programelor pentru calculator reprezintă altă formă a criminalităţii legate de Internet. Ea se realizează prin încărcarea programelor difuzate pe Internet în memoria internă a unui calculator atunci când această operaţiune nu este expres autorizată de către titularul dreptului de autor [**30**]. În cadrul unei operaţiuni desfăşurate împotriva pieţei negre, în 1997, poliţia italiană a capturat, la Livorno, peste patruzeci de mii de C.D.-ROM-uri piratate şi o mare cantitate de dischete de la un grup de douăzeci şi nouă de persoane care, după ce preluau programele din reţeaua Internet, fabricau produsele finite în mai multe ateliere clandestine. Tot cu ocazia amintită, poliţia avea să confişte importante cantităţi de echipamente de înregistrare şi programe informatice destinate să „spargă" dispozitivele de protecţie cu care erau prevăzute produsele originale" [**31**].

Astăzi, când există un număr foarte mare de baze de date, care graţie Internet-ului pot fi consultate din orice colţ al lumii, spionajul informatic cunoaşte o şi mai mare amploare şi diversificare. Furtul de informaţii îngrijorează tot mai mult companiile, societăţile şi firmele din cele mai variate domenii de activitate. Informaţiile comerciale, de genul listelor de produse, de preţuri, de clienţi, de furnizori, al metodelor de promovare a produselor sau al studiilor de marketing sunt cele mai „vânate" [**32**]. Acestora li se

adaugă tehnologiile de fabricație, metodele de instruire a personalului, *know-how*-ul invențiile în curs de patentare ș.a.

Comenzile de produse frauduloase de pe Internet cu cărți de credit false sunt, deja, de domeniul trecutului, sau au rămas doar în „grija" infractorilor începători. Întrucât majoritatea magazinelor virtuale cu nume mari au încetat să mai trimită în România produse comandate din țara noastră, datorită faptului că multe cumpărături se făceau cu cărți de credit folosite fraudulos, „specialiştii" români în frauda pe Internet au găsit metode mult mai sigure şi mai profitabile de a fura din conturile altora [**33**]. Acest lucru s-a întâmplat odată cu deschiderea de către Internet a unei noi ere pentru publicitate. Spre exemplu, există companii de publicitate care plătesc deținătorilor de *site*-uri pentru faptul că aceştia ataşează pe *site*-urile lor un *banner* al unei firme sau pentru faptul că îşi afiliază *site*-ul personal la una dintre companiile specializate în promovarea pe Internet („*affiliate*"). În ceea ce priveşte ultima metodă, trebuie precizat faptul că aceste companii plătesc deținătorului *site*-ului care s-a afiliat şi a ataşat un spot publicitar o sumă de bani proporțională cu numărul de *click*-uri de pe *banner* –ul promoțional instalat pe *site*-ul acestuia. O astfel de activitate este profitabilă pentru toate părțile şi, în acelaşi timp, perfect legală. Dar, infractorii români de pe Internet au găsit în această metodă o nouă posibilitate de a-şi însuşi anumite sume de bani tot cu ajutorul cărților de credit fraudate. Infractorul se afiliază la mai multe *site*-uri, de regulă *site*-uri comerciale, care acordă un procentaj din vânzări celor care au adus cumpărători pentru produsele expuse. Concret, utilizatorul pune un *link* pe *site*-ul său. Cum procedează infractorul ? Ne explică Marian Q. un „specialist" din Oradea: „După ce ai pus *link*-urile pe *site*-ul tău, te apuci frumos să dai *click* pe ele. Acestea te duc la *site*-uri de vânzări de diverse chestii şi te apuci să cumperi cu cărți de credit false. De unde procuri aceste cărți de credit? E grija fiecăruia să-şi facă rost... şi nu e foarte dificil. Astfel, faci cumpărături cât de mult poți, cu adrese de livrare aiurea, căci nu te interesează să primeşti produsele, ci de data asta doar procentajul din vânzări că doar eşti <<*affiliate*>> ... nu ?" Astfel, la sfârşitul lunii, „*affiliate*"-ul primeşte prin cec suma ce i se cuvine, sub formă de procente din vânzările realizate prin intermediul său. Spre a nu risca să intre sub incidența Interpol-ului, infractorii români preferă să dea „tunuri" de până la 2.000 de dolari într-o lună (peste această sumă intervine Interpol-ul), apoi să construiască un alt *site* şi să facă o altă afiliere, ştiind bine că autoritățile din țara noastră, potrivit actualei legislații, nu se pot atinge de ei. „Cel mai mult – se confesează Marius – am scos aproape 2.000 de dolari într-o lună. Dar trebuie să ai cap, pentru că dacă cei cu care eşti „*affiliate*" au cea mai mică bănuială că este un fals, întrerup imediat tranzacția". Desigur există multe alte forme ale fraudei pe Internet, însă în studiul de față am ținut să ne referim, în primul rând, la cea mai răspândită dintre ele în România. În al doilea rând, ne vom opri asupra unei afaceri nu tocmai ortodoxe care vizează cumpărarea în scop de revânzare a domeniilor Internet care aparțin unor personalități sau firme renumite [**34**]. Sperând să se îmbogățească peste noapte, unii „întreprinzători" au cumpărat domenii cu numele anumitor celebrități, în ideea că mai târziu vor primi bani grei în schimbul acestora. Este de notorietate cazul lui Dan Parisi, un fost muncitor în construcții, care a cheltuit peste 100.000 de dolari pentru a înregistra mai mult de 500 de companii cunoscute, printre care şi Microsoft, ATT, Intel s.a. Tot el deținea şi domeniul „*Madonna com*", pe cale l-a folosit pentru un *site* sexy până în 1999 când avocații cunoscutei stele a muzicii uşoare, susținând că Parisi a înregistrat domeniul cu scopuri „malefice", l-au revendicat pentru

clienta lor. Mulți alți profitori ca Parisi au pierdut în instanță drepturile asupra unor domenii purtând nume sonore, precum: Julia Roberts, Jimi Hendrix, Yahoo! ş.a.

În multe țări ale lumii, afişarea şi distribuirea materialelor obscene în public constituie o infracțiune. Ori nu există nici un dubiu că Internet-ul, prin natura sa deschisă, a devenit un astfel de loc. Ca atare, desfăşurarea unor asemenea activități prin intermediul acestei mega-rețele cade, de cele mai multe ori, sub incidența legii penale. Cu toate acestea, locațiile ce conțin materiale „pentru adulți" sunt foarte numerose. Se pare că prima condamnare pentru o astfel de faptă comisă pe Internet s-a petrecut în S.U.A., unde Robert şi Carleen Thomas din California au fost condamnați potrivit unui statut criminal federal, care interzice distribuirea de imagini obscene [**35**]. Tot pentru diseminarea pornografiei pe Internet, în Germania, *CompuService* – o mare companie de servicii *on-line* – a fost obligată să închidă accesul la o serie de astfel de locații. De asemenea, în Franța tot în anul 1996 au fost arestați doi manageri ISP care lucrau pentru *WorldNet*, respectiv pentru *FranceNet* şi au fost acuzați de pedofilie, fiind făcuți responsabili pentru materialele distribuite în grupurile de discuții *all binaries* [**36**].

Mai recent, în Germania, Statisticile Poliției Judiciare pe 1999 au înregistrat peste 2.000 de cazuri de popularizare şi deținere de pornografie infantilă, din care jumătate din acestea (puțin peste 1.000) au fost depistate prin „*surf*" pe Internet, de Biroul Federal de Criminalistică prin Investigații Independente [**37**]. Înmulțirea unor astfel de cazuri, şi impactul negativ al diseminării materialelor obscene pe Internet au dus la creşterea îngrijorării opiniei publice în legătură cu multiplicarea unor astfel de activități în rețea.

Dar, pe lângă unele forme mai vechi ale criminalității legate de Internet, şi-au făcut apariția şi altele mai noi ca: „ofertele pentru adopție" care ascund vânzări mascate de copii (cazul celor două gemene Kimberley scoase de o familie americană la vânzare pe Internet, petrecut la începutul anului 2001), furtul de identitate, violarea zonei informațiilor private a utilizatorilor Internetului; vânzarea la licitație a unor obiecte naziste (cazul companiei *Yahoo!* care, prin sentința din 20 noiembrie 2000 a Tribunalului de Mare Instanță din Paris a fost obligată să țină seama, în termen de 3 luni, de notificarea făcută la 22 mai 2000 aceleiaşi companii prin care i se cerea să ia măsuri de natură să facă imposibilă consultarea pe *Yahoo! com* a serviciului de licitație a unor obiecte naziste sau al oricărui *site* sau serviciu care se constituia într-o apologie a nazismului sau o contestare a crimelor naziste) ş.a.

Sunt voci care susțin că reglementările tehnice şi morale ar fi suficiente pentru buna funcționare a rețelei. Noi, însă, avem îndoieli serioase în această privință. Pe ce se bazează ele? Pe faptul că Internet-ul a fost şi este pândit de mari pericole care-şi află sorgintea în aceea că această rețea, miraculoasă prin beneficiile care le aduce omului, reprezintă în acelaşi timp un mediu extrem de favorabil pentru cei care se dedau la comiterea unor fapte indezirabile social, fapte care se pot întinde, după cum am văzut, de la acte teroriste până la hărțuirea sexuală sau diseminarea imaginilor pornografice.

Fără doar şi poate, atât criminalii individuali, cât şi cei care s-au constituit în bande organizate, nu pot fi lăsați să folosească Internet-ul pentru a-şi realiza scopurile infracționale. De aceea, în condițiile unei dezvoltări spectaculoase a Internet-ului şi ale

proliferării criminalității în această rețea, se impun ca necesare şi oportune unele măsuri de prevenire şi combatere a acestui fenomen atât de nociv şi periculos, între care, printre cele mai semnificative şi eficiente, ar putea fi cele de natură juridică.

Iată câteva argumente, sperăm noi, suficient de solide pentru a pune în lumină necesitatea creării unui Drept al Internet-ului.

Desigur, susținând această idee, nu uităm faptul că, având rădăcini aproape în toate țările lumii şi fiind lipsit de o autoritate centrală, Internet-ul este considerat de liberaliştii civili şi activiştii *on-line* ca o adevărată piață liberă a ideilor de tot felul. Nu putem să nu luăm în considerație lupta lor sisifică de a feri Internet-ul de constrângerile juridice care, prin impunerea unor sancțiuni civile sau penale pentru activitățile neglijente sau ilegale, ar amenința expansiunea şi, nu în ultimul rând, spiritul acestei rețele [**38**]. Dar, în acelaşi timp, aşa cum am arătat în urmă cu câteva pagini, oamenii simt nevoia irepresibilă, adânc înrădăcinată în ființa lor, de un "grăunte" de ordine în viața socială, în activitățile pe care le desfăşoară. Pentru a nu fi distrus, în final, de acțiunile bandelor criminale, Internet-ul, care s-a constituit ca o "lume" nouă, are nevoie de o anumită ordine, de o minimă reglementare juridică.

Necesitatea reglementării juridice a Internet-ului rezultă şi din aceea că unele fapte comise în această rețea cad deja sub incidența unor legi existente. Faptul că astfel de comportamente şi-au mutat locul de desfăşurare nu schimbă cu nimic natura lor criminală. În multe țări există o serie de acte normative care, chiar dacă n-au vizat, spre exemplu, diseminarea materialelor obscene în rețeaua Internet, sunt aplicabile şi se aplică şi în cazul comiterii acestor fapte prin intermediul rețelei amintite. Astfel, în Marea Britanie există mai multe acte normative care incriminează diferite aspecte ale obscenității: *Obscene Publications Act* (Actul publicațiilor obscene) din 1959, *Protection of Children Act* (Actul protecției copilului) din 1978, *Indecent Displays Act* (Actul afişajelor indecente) din 1981, *Telecommunications Act (Actul telecomunicațiilor) din 1984, Criminal Justice Act* (Actul justiției criminale) din 1988 sau *Criminal Justice and Public Order Act* (Actul Justiției Criminale şi a Ordinii Publice) din 1994 [**39**].

Dar nu numai obscenitățile, ci multe alte fapte comise prin intermediul Internet-ului şi care aduc atingere intereselor individului, comunității sau societății, intră sub incidența legilor actuale din diferite țări. Din păcate, însă, unele fapte indezirabile social care s-au petrecut şi se petrec în rețeaua Internet reprezintă o chestiune atât de nouă şi cu o dezvoltare şi o diversificare atât de rapide încât ele n-au putut fi incriminate de reglementările juridice mai vechi şi au scăpat chiar şi celor mai noi legi din țările puternic informatizate, fără a mai vorbi de celelalte țări rămase mult în urmă din acest punct de vedere, cum este şi cazul României. Mai mult, chiar şi faptele comise în Internet şi care pot fi incriminate pe baza unor legi nespecifice, de cele mai multe ori nu-şi găsesc o soluționare deplină pe baza acestor acte normative învechite, întrucât ele îmbracă aspecte noi în manifestările lor. Astfel, chiar în ceea ce priveşte difuzarea materialelor obscene, faptă complex incriminată de legile anterioare, s-a resimțit acut lipsa unor reglementări specifice privind comiterea acestei fapte prin Internet. Aşa se face că anul 1996 a reprezentat începutul intervențiilor guvernamentale în această materie. Este cazul S.U.A., unde la 1 februarie 1996 Congresul a adoptat *Telecommunications Reform Act* (Actul

reformei telecomunicațiilor) care stipula mai multe sancțiuni cu trimitere directă la diseminarea materialelor pornografice în Internet. La aceeaşi dată, guvernul Franței a mers mai departe şi a lansat un apel pentru stabilirea unor standarde internaționale în legătură cu Internet-ul şi adoptarea unor standarde etice în acest domeniu [**40**].

Iată că problemele instituirii unor reglementări juridice relative la desfăşurarea anumitor tipuri de activități în Internet câştigă din ce în ce mai mult teren în rândul țărilor *high-tech*, cum ar fi S.U.A., Marea Britanie, Franța, Germania, Japonia ş.a., dar şi al unor organisme reprezentative ale unor comunități regionale sau ale comunității internaționale. Prin urmare, "oamenii sunt preocupați nu doar de folosirea eficientă şi dezvoltarea continuă a domeniului tehnologiei informației şi al Internet-ului, ci şi de stabilirea cadrului legal în care să se desfăşoare interacțiunile în acest domeniu, numit şi *Cyberspace* sau *Global Village*" [**41**]. În acelaşi timp, pornindu-se de la faptul că Internet-ul este o rețea publică deschisă, care transgresează granițele tuturor statelor conectate, se conturează tot mai clar ideea că chiar instituirea unor legi naționale bune în această materie (ceea ce este încă departe de a se înfăptui) n-ar fi suficientă, astfel de legi ar fi inefective şi ineficiente, întrucât un fenomen global cum este această rețea nu poate fi reglementat local. În condițiile în care este posibil, de exemplu, să se folosească un calculator din România pentru a se accesa un calculator din Germania, în scopul de a dobândi acces la un calculator aflat în S.U.A., este greu de crezut că legile naționale în materie de Internet vor fi eficiente. „Numai un spațiu juridic mondial va putea stăvili fuga înainte a mafiilor telemarketing-ului" [**42**], spun doi autori avizați precum Serge Le Doran şi Philippe Rosé, referindu-se numai la un domeniu restrâns al activităților desfăşurate în această rețea. Dar acest lucru este valabil pentru toate domeniile marii rețele.

De aceea, "cunoaşterea diferitelor legi ce guvernează Internet-ul şi hotărârea comunității internaționale de a acoperi toate golurile acestei noi lumi şi de a le armoniza este una foarte actuală" [**43**]. Ori, în mod indiscutabil, aceste preocupări vor trebui să conducă, mai devreme sau mai târziu, la un *Drept al Internet-ului*, la un drept cu un caracter la fel de transfrontalier şi de global cum este însăşi această fabuloasă rețea informațională, iar în final la o lege a *Cyberspace*-ului.

Referințe bibliografice

[1] Ioana Vasiu, Criminalitatea informatică, Nemira, Bucureşti, 1998, p.121-122.

[2] John Spiropoulos în colaborare cu National Cybercrime Training Partnership (NCTP), Lupta împotriva infracțiunilor săvârşite cu ajutorul calculatorului, supliment al cursului Infracțiuni săvârşite cu ajutorul calculatorului, sponsorizat de NCTP, f.l., 1999, p.1-7. Pentru detalii, vezi: Victor-Valeriu Patriciu, Ioana Vasiu, Şerban-George Patriciu, Internet-ul şi dreptul, Editura ALL BECK, Bucureşti, 1999, p.18-108.

[3] Ioana Vasiu, op.cit., p.124.

[4] Serge Le Doran, Philippe Rosé, Cyber-Mafia, Editura Antet, Bucureşti, 1998, p.153.

[5] John Spiropoulos, op.cit., p.2.

[6] Ibidem, p.3.

[7] Ibidem, p.5.

[8] Alvin şi Heidi Toffler, Război şi antirăzboi, ANTET, f.l., f.a., p. 179.

[9] Emilian Stancu, Terorism şi Internet, în „Pentru Patrie”, nr. 12/2000, p. 26
[10] Serge Le Doran, Philippe Rosé, op. cit., p. 205.
[11] Emilian Stancu, op. cit., p. 26.
[12] Ibidem.
[13] Ibidem.
[14] Alvin şi Heidi Toffler, op. cit., p. 237.
[15] Emilian Stancu, op. cit., p. 26.
[16] Ibidem, p. 225.
[17] „Chip Computer Magazin”, nr. 12/1999, p. 18.
[18] Serge Le Doran, Philippe Rosé, op. cit., p. 207.
[19] Cornelia Popeea, Virusul iubirii, în „PC World România”, iunie 2000, p.17.
[20] Alvin şi Heidi Toffler, op. cit., p. 128.
[21] Serge Le Doran, Philippe Rosé, op. cit., p. 222-223.
[22] Emilian Stancu, op. cit. p. 27.
[23] Serge Le Doran, Philippe Rosé, op. cit., p. 204-205.
[24] Johann Kubika, Posibilităţi de combatere a criminalităţii informatice şi pe Internet, în „Buletin Informativ” al Academiei de Poliţie „Alexandru Ioan Cuza”, Editura „Academica”, Bucureşti, 2000, p. 144.
[25] Ibidem, p. 241.
[26] Ibidem, p. 30-31.
[27] Ibidem, p. 33.
[28] Johann Kubika, op. cit., p. 144; Serge Le Doran, Philippe Rosé, op. cit., p. 177.
[29] Serge Le Doran, Philippe Rosé, op. cit., p. 46.
[30] Annemarie Levins, Le piratage de logiciels:un fléau mondial, în „Revue Internationale de Police Criminelle”, numéro 476-477, 1999, p. 5.
[31] Serge Le Doran, Philippe Rosé, op. cit., p. 172.
[32] Ioana Vasiu, op. cit., p. 173.
[33] Vasile Damian, Frauda pe Internet are sediul în România. Românii conduc detaşat în topul celor mai ingenioşi hoţi din reţeaua mondială, în „Capital”, nr. 38, 21 septembrie 2000, p. 27.
[34] Cătălina Eftene, Goana după aur s-a mutat pe Internet, în „Capital”, nr. 38, 21 septembrie 2000, p. 28.
[35] Ioana Vasiu, op. cit., p. 128.
[36] Ibidem, p. 132.
[37] Johann Kubika, op. cit., p. 145.
[38] Ioana Vasiu, op.cit., pp.125-126.
[39] Ibidem, pp.131-133.
[40] Ibidem, p.129.
[41] Victor-Valeriu Patriciu, Ioana Vasiu, Şerban-George Patriciu, Internet-ul şi dreptul, Editura ALL BECK, Bucureşti, 1999, p.XIII.
[42] Serge Le Doran, Philippe Rosé, op.cit., p. 164.
[43] Victor-Valeriu Patriciu, Ioana Vasiu, Şerban-George Patriciu, op.cit., p.XIII.