Infracţiunile informatice - crime invizibile

Lector univ. drd. Flaviu CIOPEC
Asist. univ. drd. Magdalena ROIBU
Universitatea de Vest Timişoara

Information and communication technologies have a fundamental impact on today's society. The success of the „information world" has been considered essential for Europe's development, competitiveness and employment opportunities.

But making that success truly effective requires to face the persistent threat of integrity-related computer-crime.

Our study addresses the cyber-crime issue from the point of view of three procedural challenges: detection, prosecution and sanctioning of the specific offenses.

1. PROBLEMA CRIMINALITATII INFORMATICE

Societatea globală („Macworld") de azi oferă nenumărate oportunităţi individului modern: consumăm timp, bani, resurse şi, din ce în ce mai mult, informaţie – prin intermediul mijloacelor electronice.

Consumatorii de informaţie electronică se confruntă nu doar cu avantajele sistemului informatic (e.g. acces imediat la orice informaţie şi interacţiune prin intermediul internetului), ci şi cu efectele nocive ale procesului informatic – criminalitatea informatică.

Nevoia iminentă de a lupta împotriva noilor forme de criminalitate, determinate de evoluţia tehnologiei, a devenit un punct fierbinte pe agenda europeană.

Astfel, la nivelul Uniunii Europene, s-au făcut eforturi notabile pentru existenţa unei legislaţii adecvate în materie, care să includă atât noţiuni de drept material, cât şi aspecte de drept procedural care să reglementeze problema în discuţie.

România, ca stat-membru UE, este ţinută să adopte (şi, evident, să adapteze) legislaţia comunitară specifică, acest demers având loc chiar înaintea aderării ţării noastre la UE: în 2004, România a ratificat Convenţia Consiliului Europei privind criminalitatea informatică prin Legea nr. 64/2004[1]. De asemenea, există şi o serie de legi interne care tratează diferite manifestări ale criminalităţii informatice, mai precis Legea nr. 8/1996[2] privind drepturile de autor şi drepturile conexe (modificată în 2006), Legea nr. 365/2002[3] privind comerţul electronic (inclusiv falsificarea instrumentelor de plată electronică), Legea nr. 161/2003[4] privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, Legea nr. 135/2007[5] privind arhivarea documentelor în formă electronică, ş.a.

Cele câteva legi interne în vigoare nu tratează în termeni exhaustivi problema criminalităţii informatice, acest lucru fiind valabil şi în cazul legislaţiilor altor state comunitare.

[1] Legea nr. 64/2004, publicată în Monitorul Oficial al României nr. 343/2004.
[2] Legea nr. 8/1996, modificată prin Legea nr. 329/2006 publicată în M.O.R. 657/2006.
[3] Legea nr. 365/2002, modificată prin Legea nr. 121/2006 publicată în M.O.R. 403/2006.
[4] Legea nr. 161/2003, supusă abrogării parţiale, publicată în M.O.R. 279/2003.
[5] Legea nr. 135/2007, publicată în M.O.R. 345/2007.

Dimensiunea transnaţională a criminalităţii informatice justifică necesitatea absolută a unei cooperări efective la nivel european, bazată pe asistenţă reciprocă în ceea ce priveşte metodele de urmărire şi tragere la răspundere.

Prezentul articol analizează provocarea permanentă pe care o reprezintă criminalitatea informatică pentru spaţiul comunitar şi, implicit pentru România, acordând o atenţie deosebită aspectelor procedurale referitoare la descoperirea, urmărirea şi sancţionarea infracţiunilor informatice.

2. PROVOCĂRI DE NATURĂ PROCEDURALĂ

Prezentul articol nu îşi propune nici să pună în discuţie o fenomenologie a criminalităţii informatice, şi nici să ofere soluţii perfecte de prevenire a unor astfel de infracţiuni postmoderne.

Abordarea noastră este orientată mai curând către aspectele de ordin procedural, astfel încât lucrarea va dezbate trei probleme specifice, care au nevoie de eficientă soluţionare, anume:

a. descoperirea infracţiunilor informatice (aspectul „*multi loci*")
b. urmărirea penală (cercetarea şi ridicarea de obiecte/înscrisuri)
c. sancţionarea – prin sancţiuni efective, proporţionale şi disuasive

CONTEXTUL GENERAL

Infracţiunile informatice sunt descoperite în realitate doar în proporţie mică de către organele de urmărire penală, ceea ce face şi mai dificilă o imagine de ansamblu a dimensiunii fenomenului.

În timp ce o descriere corespunzătoare a diferitelor categorii de infracţiuni informatice este relativ uşor de realizat (e.g. infracţiuni constând în sabotarea sistemelor informatice sau încălcarea drepturilor de autor), o sinteză referitoare la întinderea prejudiciului cauzat prin astfel de infracţiuni se dovedeşte extrem de dificilă.

De asemenea, este puţin probabil că va fi făcută o estimare cât mai aproape de adevăr a numărului real de infracţiuni informatice comise.

În cursul anului 2003, serviciile specializate din România au cercetat doar 200 de infracţiuni de natură informatică, din care 50% au fost licitaţii electronice frauduloase, 30% bunuri comandate on-line fraudulos, 10% au privit accesul neautorizat la sisteme informatice şi 10% s-au referit la transmiterea de viruşi, pornografie infantilă şi folosirea de identităţi false[6].

Cifra neagră a infracţiunilor amintite este rezultatul mai multor cauze, printre care:

- tehnologia sofisticată utilizată de infractori;
- lipsa instruirii adecvate a ofiţerilor din cadrul organelor de urmărire penală;
- lipsa unui plan de reacţie din partea victimelor, în caz de „atacuri", fapt ce poate duce la imposibilitatea estimării pierderilor suferite;
- divergenţele dintre legislaţiile naţionale;

[6] Statistici preluate din Capitolul V al „Ghidului Introductiv pentru Aplicarea Dispoziţiilor Legale referitoare la Criminalitatea Informatică", disponibile la www.riti-internews.ro.

- lipsa unor instrumente legislative adecvate la nivel intern, precum şi a asistenţei judiciare mutuale efective;
- prioritizarea defectuoasă a operaţiunilor de cercetare a infracţiunilor informatice
- ezitarea de a denunţa infracţiunile la organele de urmărire penală

În cea din urmă situaţie, chiar dacă infracţiunea a fost sesizată, victimele nu depun plângere în vederea descoperirii şi sancţionării făptuitorului. Motivele unui astfel de comportament sunt multiple, precum preocuparea pentru imaginea publică, ce ar putea fi afectată de publicitatea negativă creată prin infracţiune; respingerea ideii de a suporta costurile unei eventuale cercetări, dată fiind complexitatea unui asemenea demers, şanse reduse de a recupera prejudiciul suferit, chiar în cazul identificării autorului infracţiunii.

Este bine ştiut că investigaţiile în domeniul infracţionalităţii informatice sunt, prin natura lor, complexe şi implică utilizarea de echipamente sofisticate, cu costuri enorme. De asemenea, instruirea personalului de specialitate este un proces de durată, care presupune costuri la fel de mari. Un alt aspect important este că asemenea investigaţii sunt consumatoare de timp. Un investigator în domeniul criminalităţii informatice poate lucra la maximum 3-4 cazuri pe lună, în timp ce un investigator „tradiţional" poate soluţiona între 40 şi 50 de cazuri în aceeaşi perioadă de timp[7].

În ceea ce priveşte reglementările de drept material din domeniul criminalităţii informatice, marile lacune au fost acoperite.

Din perspectiva dreptului procedural, însă, multe aspecte au rămas neclarificate, în principal datorită naturii volatile, intangibile a infracţiunilor informatice.

Fiecare infracţiune – încadrabilă, din punctul de vedere al conţinutului constitutiv, direct sau indirect, în categoria infracţiunilor informatice – scapă acelui *modus operandi* utilizat de metodele clasice de urmărire şi tragere la răspundere.

Acest lucru se justifică prin aceea că, în cazul infracţiunilor informatice, barierele spaţiale dispar, descoperirea făptuitorilor devine o misiune aproape imposibilă, iar tragerea la răspundere nu rămâne decât o ipoteză.

În acest sens, Michael Sussman[8] observa că: „*în activitatea infracţională are loc o revoluţie. Acest lucru creează probleme majore pentru organele judiciare din aproape toate colţurile lumii – probleme care apar cu o frecvenţă şi o forţă neexistente anterior. Revoluţia constă în felul în care computerele conectate în reţea şi alte tehnologii permit comiterea infracţiunilor la distanţă, prin internet şi comunicarea de tip wireless. Infractorul nu mai trebuie să se afle la locul crimei pentru a acţiona asupra victimei. Aproape orice infracţiune poate dobândi o dimensiune internaţională, ceea ce înseamnă că mecanismul greoi al cooperării internaţionale poate încetini sau chiar devia cercetările. Aceasta deoarece, începând cu băncile, sistemele de telefonie sau controlul traficului aerian şi terminând cu forţele armate, totul se bazează pe computere conectate în reţea, astfel încât puţine persoane fizice sau instituţii pot face faţă noii ameninţări pe care o reprezintă acest tip de infracţionalitate*".

[7] Idem.

[8] Michael A. Sussmann: *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millenium* în Peter Csonka: *The Council of Europe's Convention on Cyber-Crime and Other European Initiatives*, International Review of Penal Law, 77e année nouvelle série, 3e/4e trimestres, 2006, editura Érès, p. 476.

Vom ilustra lacuna din sistem cu un caz recent de infracţiune informatică (categoria: infracţiune informatică tradiţională, i.e. falsificarea de carduri de debit) din România, unde victimele sunt o cunoscută bancă românească şi mii de clienţi ai acesteia.

Pe scurt, situaţia de fapt este după cum urmează: la începutul lunii mai, 2008, Bancpost şi Inspectoratul General al Poliţiei Române cercetează retrageri suspecte de numerar prin bancomate din România şi Bulgaria, ulterior din alte state europene. Poliţia nu exclude scurgerea de informaţii din interiorul băncii, întrucât seriile cardurilor respective sunt consecutive. Varianta unei eventuale erori de sistem pare puţin plauzibilă. Tranzacţiile frauduloase au fost imediat descoperite de bancă, astfel încât s-a restricţionat utilizarea cardurilor de tip Millenium la bancomate.

Cercetările în dosarul fraudei depistate la Bancpost au condus anchetatorii spre lumea interlopă a capitalei – mai precis spre două grupări, una coordonată de un clan renumit, cealaltă cunoscută pentru activităţi de clonare de carduri.

Oficial, nu au fost formulate acuzaţii.

Cele expuse anterior pot fi interpretate ca un eşec al organelor de urmărire penală de a controla o formă mai puţin tradiţională de infracţionalitate?

Deşi relativ insuficientă, legislaţia română în materie, ar putea acţiona ca factor de prevenire a unor astfel de infracţiuni, însă nu reuşeşte să producă efectul dorit asupra celor care au comis frauda.

Articolul 24, alineatele (1) şi (2) din Legea nr. 365/2002 (modificată prin Legea nr. 121/2006) conţine dispoziţii clare, însoţite de sancţiunile adecvate referitoare la falsificarea instrumentelor de plată electronică:

„(1) *Falsificarea unui instrument de plată electronică se pedepseşte cu închisoare de la 3 la 12 ani şi interzicerea unor drepturi*.

(2) *Cu aceeaşi pedeapsă se sancţionează punerea în circulaţie, în orice mod, a instrumentelor de plată electronică falsificate sau deţinerea lor în vederea punerii în circulaţie*".

În contextul infracţiunii informatice ilustrate mai sus, unde au existat alegaţii cu privire la faptul că unii dintre făptuitori ar deţine instrumente de clonare a cardurilor, legea intervine din nou; articolul 25 din aceeaşi lege prevede că: „*Fabricarea ori deţinerea de echipamente, inclusiv hardware sau software, cu scopul de a servi la falsificarea instrumentelor de plată electronică, se pedepseşte cu închisoare de la 6 luni la 5 ani*".

a) Descoperirea infracţiunilor informatice şi aspectul *multi-loci*

Dificultatea controlării infracţiunilor informatice rezidă tocmai în caracterul transnaţional al acestora.

Criminalitatea informatică este o activitate prin excelenţă afrontalieră, ce presupune un grad ridicat de anonimitate şi clandestinitate, astfel încât este favorabilă acelor infractori care caută câştigul material imediat şi speculează şansele minime de a fi descoperiţi şi traşi la răspundere.

A fost descrisă ca fiind noua „topologie socială"[9], sintagmă destinată a atrage atenţia asupra faptului că multe grupări teroriste şi de crimă organizată profită, prin activităţile lor

[9] Schneider, V. şi Hyner,D.: *The Global Governance of Cybercrime:Issue Space and the Transnational Policy Network* în Paul de Hert, Gloria Gonzales Fuster şi Bert-Jaap Koops: *Fighting Cybercrime in the Two Europes. The Added Value of the EU FrameworkDecision and the Council of Europe Convention*, International Review of Penal Law, 77e année nouvelle série, 3e/4e trimestres, 2006, editura Érès, p. 517.

ilicite, de avantajele esenţiale ale spaţiului virtual, care face orice operaţiune posibilă într-o fracţiune de secundă.

În Uniunea Europeană, infracţiunile informatice sunt considerate parte a crimei organizate[10], întrucât este ştiut faptul că aceasta din urmă îşi însuşeşte oportunităţile oferite de internet pentru a crea sisteme sigure de comunicare în vederea comiterii de infracţiuni.

Acest lucru se explică prin aceea că „*structura logică a Internetului în sine, cu numeroasele reţele prin care circulă „pachetele" de date , până când acestea sunt ordonate la destinaţie, face deosebit de dificilă descoperirea hackerilor*".[11]

De asemenea, atenţia specialiştilor IT a fost atrasă de faptul că experţii intruşi în bazele de date îşi creează propria lor reţea underground de sisteme informatice ilicite, care le permite să „sară" dintr-un sistem în altul, până când atacă sistemul ţintă.[12]

La o analiză a dispoziţiilor procedurale actualmente în vigoare în legislaţia română, se observă care sunt măsurile ce trebuie luate în cazul în care o persoană „simte" sau descoperă efectiv că s-a comis o infracţiune informatică.

Textul legal român transpune în linii generale prevederile Convenţiei de la Budapesta privind criminalitatea informatică, încă de la adoptarea acesteia, în noiembrie 2001, în special cele referitoare la conservarea rapidă a datelor informatice stocate (Titlul 2, art. 16), precum şi acelea legate de dezvăluirea parţială a datelor referitoare la traficul informaţional (art. 17).

Capitolul IV din Legea nr. 161/2003 (privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei) – „Dispoziţii procedurale" – conţine o serie de prevederi care tratează problema în linii generale, stabilind rolul procedural al părţilor implicate în lanţul infracţional informatic.

„Art. 54 – *(1) În cazuri urgente şi temeinic justificate, dacă există date sau indicii temeinice cu privire la pregătirea sau săvârşirea unei infracţiuni prin intermediul sistemelor informatice, în scopul strângerii de probe sau al identificării făptuitorilor, se poate dispune conservarea imediată a datelor informatice ori a datelor referitoare la traficul informaţional, faţă de care există pericolul distrugerii ori alterării.*

(2) În cursul urmăririi penale, conservarea se dispune de procuror, prin ordonanţă motivată, la cererea organului de cercetare penală sau din oficiu iar în cursul judecăţii, de instanţă, prin încheiere.

(4) Ordonanţa procurorului sau încheierea instanţei se transmite, de îndată, oricărui furnizor de servicii sau oricărei persoane în posesia căreia se află datele prevăzute la alin.(1), aceasta fiind obligată să le conserve imediat, în condiţii de confidenţialitate".

Următoarele articole prevăd posibilitatea de ridicare a obiectelor care conţin date informatice, date referitoare la traficul informaţional sau date referitoare la utilizatori – de la persoana sau furnizorul de servicii care le deţine, pentru efectuarea de copii, care pot servi ca mijloc de probă.

Textul juridic nu se referă şi la ce poate constitui un caz „temeinic justificat" sau un indiciu „temeinic" referitor la iminenţa unui act infracţional de natură informatică, motiv

[10] Pentru reglementarea română a se vedea art. 2 par. b pct. 18 din Legea nr. 39/2003 privind prevenirea şi combaterea criminalităţii organizate.

[11] Adamski, A.: *Crimes Related to the Computer Network. Threats and Opportunities:A Criminological Perspective*, articol disponibil la www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.

[12] Anderson, K.: *International Intrusion: Motives and Patterns* în Adamski,A, articolul citat *supra.*

pentru care este dificil de prevăzut ce anume circumstanţe pot fi calificate drept temeinice, astfel încât să atragă cercetarea penală.

Un posibil răspuns ar putea veni din jurisprudenţa relevantă internă/europeană/internaţională, pentru a decide dacă anumite acte ilicite intră sub incidenţa reglementărilor penale din domeniul criminalităţii informatice.

Într-o decizie din anul 2006 (decizia nr. 5288/2006), Înalta Curte de Casaţie şi Justiţie din România a condamnat la pedeapsa închisorii patru inculpaţi (care acţionau în oraşe diferite) care au folosit un skimmer (dispozitiv destinat a servi la citirea benzii magnetice a cardurilor) şi o mini-cameră pe care au montat-o în interiorul unui bancomat extern, datele astfel obţinute fiind descărcate pe computer. Scopul infractorilor era de a retrage numerar, prin folosirea de instrumente de plată electronică falsificate.

În cazul citat există cel puţin două „indicii temeinice".

Primo, martorul ocular a observat că era practic imposibil să folosească bancomatul, deoarece fanta în care se introduce cardul prezenta modificări; martorul a văzut inculpaţii simulând efectuarea unei operaţiuni ATM, luând skimmerul şi mini-camera, pe care le-au ascuns într-un ziar.

Secundo, alegaţiile martorului au fost confirmate de imaginile înregistrate de camera de supraveghere montată la exterior, în care se observă cum cei doi autori retrag dispozitivele din bancomat.

Trebuie menţionat că obligaţia de conservare a datelor informatice impusă furnizorilor de servicii şi persoanelor fizice nu trebuie în niciun caz să impieteze asupra principiilor democratice prevăzute în convenţiile europene şi internaţionale care promovează drepturile şi libertăţile individului.

În acest sens, articolul 15 – „Condiţii şi măsuri de protecţie" (Titlul 1) al Convenţiei privind criminalitatea informatică, prevede următoarele:

„1. *Fiecare parte va veghea ca stabilirea, realizarea şi aplicarea prerogativelor şi a procedurilor prevăzute în prezenta secţiune să fie supuse condiţiilor şi măsurilor de protecţie prevăzute în dreptul său intern, care trebuie să asigure o protecţie adecvată a drepturilor şi libertăţilor omului, în special a drepturilor stabilite în conformitate cu obligaţiile pe care aceasta le-a subscris în aplicarea Convenţiei Consiliului Europei pentru apărarea drepturilor omului şi libertăţilor fundamentale (1950), a Pactului internaţional privind drepturile civile şi politice al Naţiunilor Unite (1966), precum şi a altor instrumente internaţionale aplicabile privind drepturile omului, şi care trebuie să integreze principiul proporţionalităţii.*

2. *Ţinând cont de natura procedurii sau a prerogativelor acordate, aceste condiţii şi măsuri de protecţie vor include, între altele, atunci când situaţia o impune, o supervizare judiciară sau alte forme de supervizare independentă a motivelor care justifică aplicarea, precum şi limitarea ariei de aplicare şi a duratei prerogativelor sau procedurii în cauză.*

3. *În măsura în care acest lucru este în conformitate cu interesul public, în special cu buna administrare a justiţiei, fiecare parte va examina efectul prerogativelor şi al procedurilor privind drepturile, responsabilităţile şi interesele legitime ale părţilor*".

De asemenea, articolul 9 din Directiva 2006/24/EC privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicaţii electronice accesibile publicului sau de reţele de comunicaţii electronice accesibile publicului şi de modificare a Directivei 2002/58/CE conţine dispoziţii clare ce accentuează faptul că în circumstanţe speciale, grave, cum ar fi infracţiunile de crimă organizată şi terorism, autorităţile

competente trebuie să aibă acces la datele cheie, dar acestea trebuie să ţină seama de limitările impuse de instrumentele internaţionale de protecţie a drepturilor omului:

Articolul (9) „*Autorităţile publice pot interveni în exercitarea acestui drept* (n.a. dreptul la respectarea vieţii private şi a corespondenţei) *numai în conformitate cu legea şi în cazul în care este necesar, într-o societate democratică, inter alia, în interesul siguranţei naţionale sau al siguranţei publice, în vederea prevenirii dezordinii sau criminalităţii sau în vederea protecţiei drepturilor şi libertăţilor celorlalţi. Deoarece păstrarea datelor s-a dovedit a fi un instrument de investigare atât de necesar şi eficace pentru aplicarea legii în mai multe state membre şi, în special, în ceea ce priveşte problemele grave, cum sunt criminalitatea organizată şi terorismul, este necesară asigurarea că datele păstrate sunt puse la dispoziţia autorităţilor de aplicare a legii pentru o anumită perioadă, sub rezerva condiţiilor prevăzute de prezenta directivă. Adoptarea unui instrument de păstrare a datelor care să respecte cerinţele articolului 8 din CEDO este, prin urmare, o măsură necesară*".

Raportat la importanţa implicaţiilor ce derivă din Directiva privind păstrarea datelor, Comisia Europeană a emis recent o decizie – Decizia din 25 martie 2008 (2008/324/CE)[13] care urmăreşte crearea unui grup de experţi în domeniul păstrării datelor, care să lucreze la o „platformă pentru păstrarea datelor electronice în vederea investigării, a depistării şi urmăririi infracţiunilor grave".

Mai precis, date fiind exigenţele legitime ale autorităţilor naţionale, preocupate de conservarea mai eficientă a datelor informatice, pentru contracararea infracţionalităţii informatice, articolul 2 din amintita Directivă prevede astfel „ *Comisia intenţionează să creeze un grup format din autorităţi de aplicare a legii din Statele Membre, asociaţii din industria comunicaţiilor electronice, reprezentanţi ai Parlamentului European şi ai autorităţilor de protecţie a datelor, inclusiv Autoritatea Europeană pentru Protecţia Datelor*".

b) Urmărirea penală şi tragerea la răspundere

Actele de criminalitate informatică ar trebui prevenite prin mijloace tehnice, şi, de fapt s-a dezvoltat o întreagă industrie legată de securitatea informaţiei, tocmai în scopul amintit.

În acelaşi timp, însă, metodele tradiţionale de investigare, cum sunt percheziţia şi ridicarea de obiecte şi înscrisuri, nu sunt total abandonate.

În multe cazuri, datorită naturii şi complexităţii infracţiunilor informatice, percheziţia în accepţiunea clasică se dovedeşte nu doar învechită, ci şi nefuncţională.

Aceasta se întâmplă deoarece, intervalul de timp dintre descoperirea infracţiunii şi formalităţile procedurale guvernate de reguli stricte (nu avem în vedere aici infracţiunile flagrante), care conduc la identificarea autorului sau autorilor – are o influenţă negativă asupra fazei de urmărire penală.

De aceea, în astfel de cazuri, este absolut necesară o bună coordonare a procedurii de conservare a datelor informatice.

Atunci când se încalcă ordinul legal de punere la dispoziţie a datelor informatice de către persoanele fizice sau persoanele juridice – furnizori de servicii – procurorul sau instanţa pot dispune, motivat, percheziţia şi, eventual, sechestrarea datelor informatice stocate.

[13] Pentru a consulta textul complet al directivelor amintite, a se vedea www.eur-lex.europa.eu.

Percheziţia presupune acces imediat la sistemul informatic prin intermediul sau asupra căruia s-a comis infracţiunea informatică[14].

Articolul 19, alineatele 1-4 (Titlul 4) – „Percheziţia şi sechestrarea datelor informatice stocate" din Convenţia privind criminalitatea informatică, ale cărui dispoziţii sunt fidel reproduse de Legea de ratificare nr. 64/2004, se referă la mijloace de probă adecvate, precum percheziţia şi accesarea sistemelor informatice în cazul unor infracţiuni specifice, precum abuzurile asupra dispozitivelor (art.6), frauda informatică (art. 8), infracţiuni informatice referitoare la pornografia infantilă (art. 9), infracţiuni informatice referitoare la atingerile aduse proprietăţii intelectuale (art. 10).

Art. 19

„1. *Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a conferi autorităţilor sale competente dreptul de a percheziţiona sau de a accesa într-un mod similar:*

a) un sistem informatic sau o parte a acestuia, precum şi datele informatice care sunt stocate în acesta; şi

b) *un suport de stocare informatic, care permite stocarea datelor informatice pe teritoriul său*

2. *În cazul în care autorităţile părţii vor percheziţiona sau accesa într-un mod similar un sistem informatic specific ori o parte din acesta, în conformitate cu paragraful 1 subparagraful a) şi vor avea motive de a considera că datele urmărite sunt stocate într-un alt sistem informatic sau într-o parte a acestuia situat pe teritoriul său şi că aceste date sunt în mod legal accesibile de la sistemul iniţial ori sunt disponibile pentru acest sistem iniţial, fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru ca numitele autorităţi să fie în măsură de a extinde rapid percheziţia sau accesarea într-un mod similar a celuilalt sistem.*"

Similar, articolul 56 alineatul (1) din Legea nr. 161/2003 cuprinde următoarele reguli aplicabile în materia mijloacelor de probă: „*Ori de câte ori, pentru descoperirea şi strângerea probelor, este necesară cercetarea unui sistem informatic sau a unui suport de stocare a datelor informatice, organul competent prevăzut de lege poate dispune efectuarea unei percheziţii*".

În condiţiile procedurii tradiţionale de percheziţie, organele de urmărire penală îşi ghidează activitatea conform dispoziţiilor din Codul de procedură penală român, referitoare la efectuarea percheziţiei (articolele 104-105).

Cei care efectuează propriu-zis percheziţia au obligaţia, ca şi în cazul consevării datelor informatice, să respecte caracterul confidenţial al operaţiunii, în mod contrar putând risca sancţiuni datorită unui comportament ce încalcă prevederile articolului 8 din Convenţia Europeană a Drepturilor Omului, anume respectarea vieţii private şi de familie.

Trebuie subliniat faptul că atunci când infracţiunea informatică a depăşit graniţele unei anume jurisdicţii, în sensul că, fie actele infracţionale comise de aceeaşi persoană s-au desfăşurat într-un stat, dar au produs urmarea periculoasă în altul, fie o pluralitate de infractori au comis aceeaşi faptă, dar au acţionat din state diferite, o acţiune singulară de descoperire şi pedepsire a acestor acte ilicite este inutilă, deci contraindicată[15].

---

[14] Pentru o analiză critică a reglementărilor în materia supravegherii sistemelor informatice a se vedea D. Julean, F.Ciopec: *Autoritatea procurorului în situaţii speciale*, Editura Universitaria, Craiova, 2006.

[15] Grabovsky, P: *The Mushroom of Cyber Crime* în Paul de Hert, Gloria Gonzales Fuster şi Bert-Jaap Koops: *Fighting Cybercrime in the Two Europes. The Added Value of the EU Framework Decision and the*

De asemenea dificultatea în a descoperi şi combate crimele informatice derivă din diferenţele la nivelul legislaţiilor naţionale, care conduc la obstrucţionarea urmăririi penale, a judecăţii şi a unei eventuale condamnări ulterioare: „ *Atunci când legile unui stat incriminează anumite infracţiuni informatice, în timp ce legile altui stat nu o fac, cooperarea în dezlegarea infracţiunii şi tragerea la răspundere a autorului, s-ar putea dovedi imposibilă. Altfel a spune, când un infractor parcurge în spaţiul virtual trei, patru sau cinci ţări, înainte de a ajunge la victima ţintă, legile inadecvate din una dintre aceste ţări, îl protejează de fapt pe infractor de răspunderea penală din alte ţări*”[16].

Legislaţia română prevede mai multe tipuri de activităţi deosebit de utile în cazul în care se impune o acţiune de cooperare internaţională în scopul urmăririi, judecării şi sancţionării actelor de criminalitate informatică.

Articolul 60 (Capitolul V) , alineatele 1 şi 2 din Legea nr. 161/2003 menţionează că autorităţile judiciare dintr-un stat cooperează în mod direct cu omologii lor (instituţii similare sau organizaţii internaţionale specializate) în vederea combaterii infracţionalităţii informatice.

Această cooperare poate lua forma unor activităţi[17] precum: asistenţa judiciară internaţională în materie penală, extrădarea şi mandatul european de arestare, anchete comune, identificarea, blocarea, sechestrarea şi confiscarea produselor şi instrumentelor infracţiunii, schimbul de informaţii, asistenţa tehnică sau de altă natură pentru colectarea şi analiza informaţiilor, formarea personalului de specialitate ş.a.

Odată demarate aceste activităţi, autorităţile străine competente pot solicita intervenţia Serviciului de Combatere a Criminalităţii Informatice din România, care funcţionează în cadrul Direcţiei de investigare a infracţiunilor de criminalitate organizată şi terorism (DIICOT) din Parchetul de pe lângă Înalta Curte de Casaţie şi Justiţie.

De asemenea, referitor la cooperarea internaţională în domeniul criminalităţii informatice, Convenţia privind criminalitatea informatică, la articolul 35 (Titlul 3) a prevăzut aşa-numita „Reţea 24/7”, destinată ca „*punct de contact disponibil 24 de ore din 24, 7 zile din 7, în scopul asigurării unei asistenţe imediate pentru investigaţiile referitoare la infracţiunile privind sisteme sau date informatice sau pentru a strânge dovezile unei infracţiuni în format electronic*”.

c) Sancţiuni

La fel ca în cazul altor infracţiuni, actele de criminalitate informatică sunt sancţionate de lege, indiferent dacă sunt comise de persoane fizice sau juridice.

Multe legislaţii europene prevăd şi răspunderea penală a persoanelor juridice, iar natura şi întinderea sancţiunilor pot varia considerabil, de la un sistem juridic la altul.

Articolul 12 (titlul V) din Convenţia privind criminalitatea informatică se ocupă de problema răspunderii penale a persoanelor juridice.

Council of Europe Convention, International Review of Penal Law, 77e année nouvelle série, 3e/4e trimestres, 2006, editura Érès, p. 517.

[16] Csonka, P.: *The Council of Europe's Convention on Cyber-Crime and Other European Initiatives*, International Review of Penal Law, 77e année nouvelle série, 3e/4e trimestres, 2006, editura Érès, p. 477.

[17] Pentru reglementarea română a se vedea Legea nr. 302/2004 privind cooperarea judiciară internaţională în materie penală.

Multe dintre infracţiunile informatice sunt comise de indivizi care acţionează sub acoperirea departamentelor de conducere ale marilor companii, astfel încât determinarea răspunderii acestora poate fi un demers dificil. Prin urmare, este esenţial a stabili dacă infractorul a acţionat pe cont propriu, ca persoană fizică, fără a avea legătură cu compania sau „*în calitate de membru al unui organ al persoanei juridice, care exercită o funcţie de conducere în cadrul acesteia, având la bază: a) o calitate de reprezentare a persoanei juridice; b) puterea de luare a deciziilor în numele persoanei juridice; c) puterea de a exercita controlul în cadrul persoanei ju*ridice" (Art. 12 alin. (1)).

Convenţia prevede răspunderea solidară (Art. 12 alin. (2)) între persoana juridică şi persoana fizică, în special când infracţiunea este rezultatul „absenţei supravegherii sau controlului din partea persoanei fizice".

Răspunderea persoanei juridice, fie civilă, administrativă sau penală, nu exclude răspunderea penală a persoanei fizice, dacă se dovedeşte o relaţie ierarhică profesională între persoana fizică şi companie.

Tentativa şi complicitatea (Art. 11) la infracţiunile informatice se pedepsesc. Convenţia conferă puteri discreţionare fiecărui stat semnatar, în sensul că, pentru anumite infracţiuni (e.g. interceptarea ilegală, afectarea integrităţii datelor, frauda informatică, infracţiuni informatice referitoare la pornografia infantilă), statelor semnatare li se acordă dreptul de a nu aplica, în tot sau în parte, sancţiunea adecvată pentru tentativă la anumite infracţiuni.

Articolul 13 – „Sancţiuni şi măsuri" prevede că:

„ *1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru ca infracţiunilor stabilite în aplicarea art. 2-11 să li se poată aplica sancţiuni efective, proporţionale şi disuasive, care cuprind pedepse privative de libertate.*

2. Fiecare parte va veghea ca toate persoanele juridice trase la răspundere în aplicarea art. 12 să facă obiectul sancţiunilor sau măsurilor penale ori nepenale efective, proporţionale şi disuasive, care cuprind sancţiuni pecuniare".

Este de notat că, în timp ce în cazul persoanelor fizice, sancţiunile cele mai uzuale sunt amenda sau privarea de libertate, în funcţie de gravitatea faptei, în cazul persoanelor juridice, sancţiunile pecuniare sunt predominante.

Potrivit dreptului comunitar, sancţiunile trebuie să respecte trei cerinţe caracteristice: să fie efective, proporţionale şi disuasive.

Bogata jurisprudenţă a Curţii de Justiţie a Comunităţilor Europene[18] a făcut posibilă înţelegerea fiecăreia dintre cele trei cerinţe pe care trebuie să le îndeplinească sancţiunile.

Sancţiunea este efectivă atunci când implementarea ei nu este nici imposibilă, nici stopată prin piedici extrem de nerezonabile.

Ea este proporţională când este concepută pentru a-şi atinge scopul legitim (efectivitate şi disuasivitate) şi când, în vederea atingerii scopului menţionat, se alege soluţia cea mai puţin oneroasă.

În fine, sancţiunea va fi disuasivă atunci când are efect de descurajare a oricăror încălcări ale scopurilor şi regulilor dreptului comunitar.

[18] A se vedea opiniile Avocatului General în cauza *Berlusconi* C-387/02, disponibile la www.eur-lex.europa.eu.

3. REMARCI DE FINAL

Infracţionalitatea a dobândit amploare rapid în „lumea nedefinită a spaţiului virtual", astfel încât se impune intervenţia neîntârziată a autorităţilor judiciare în vederea controlului fenomenului[19].

Recomandarea este cu atât mai potrivită, cu cât se constată o evoluţie a anumitor aspecte ce ţin de infracţionalitatea informatică, după cum urmează:

- actele de infracţionalitate informatică sunt din ce în ce mai frecvente

Aceasta tendinţă se explică prin aceea că toate aspectele vieţii sociale contemporane, dominată de hi-tech, depind, în mare măsură, de sistemele informatice. Prin urmare, atacurile asupra şi prin intermediul computerului au crescut.

- infracţiunile informatice pot fi comise de aproape orice persoană şi pot vătăma aproape orice persoană

Dacă, la origini, sistemele informatice erau o caracteristică a domeniilor militar şi guvernamental, astăzi, datorită corelării între înalta performanţă tehnologică şi costurile scăzute, acestea pot fi accesate de aproape orice persoană.

- infracţiunile informatice sunt „flexibile" şi sunt în plin proces de internaţionalizare

Procesarea electronică a datelor informatice este compatibilă cu domeniul telecomunicaţiilor. Or, infracţiunile informatice sunt comise tot mai frecvent prin intermediul reţelelor de telecomunicaţii.

- infracţiunile informatice, cu precădere cele comise prin intermediul Internetului, devin domeniul privilegiat al grupărilor de crimă organizată

Gradul de anonimitate al sistemelor computerizate internaţionale, precum şi metodele de transmitere codificată a mesajelor, la care se adaugă eşecul instituţiilor specializate de a controla fluxul informaţional, reprezintă avantaje clare pentru activităţile de crimă organizată, mai ales pentru cele de natură transfrontalieră.

- există, şi în cazul infracţiunilor informatice, dificultăţi de armonizare a dreptului penal naţional al Statelor-Membre ale Uniunii Europene

Jurisprudenţa Curţii de Justiţie a Comunităţii Europene (Cauza C-176/03) abordând distribuirea competenţelor în materie penală, în continuare disputate între Pilonul 1 comunitar şi Pilonul 3, atrage atenţia asupra dificultăţilor de reglementare legislativă şi în materia criminalităţii informatice, ce pot apărea la nivel instituţional comunitar.

[19] Kraisorn Porsutee (Secretar de Stat, Ministerul Informaţiei şi Tehnologiei Comunicaţiilor, Tailanda) – opinii exprimate în cadrul workshopului *Criminalization of Computer Wrongdoing, Prerequisite for Combating Cybercrime*, ocazionat de al unsprezecelea Congres ONU „Crime Prevention and Criminal Justice", aprilie 2005, comunicat de presă disponibil la www.unis.vienna.org.