Capitolul I

Amenințări şi tendințe în ce priveşte securitatea sistemelor informatice şi rețelelor de comunicații

Secțiunea I
Considerații generale

Încă de la apariția sistemelor informatice şi rețelelor de comunicații au fost căutate vulnerabilităților acestora, fie în scopul îmbunătățirii performanțelor şi siguranței în exploatare fie în scopul compromiterii lor.

Secțiunea a II-a
Principalele taxonomii dezvoltate în sfera securității sistemelor informatice şi rețelelor de comunicații

***Taxonomia*,** conform definiției[1], este mai mult decât o clasificare, în sensul că aceasta descrie principiile conform cărora clasificarea a fost făcută, dar şi procedura care trebuie urmată pentru clasificarea unui obiect nou[2].

În sfera securității sistemelor informatice şi a rețelelor de comunicații, taxonomiile au apărut din nevoia de a oferi consecvență şi coerență în limbajul utilizat pentru descrierea şi clasificarea vulnerabilităților şi atacurilor asupra acestora şi a se evita astfel (pe cât posibil) confuziile.

De asemenea, aceste taxonomii permit aplicarea cunoştințelor anterioare amenințărilor noi, cât şi un mod organizat de percepere a acestora (amenințărilor).

O ***taxonomie satisfăcătoare*** prezintă următoarele **caracteristici**[3]:

---

[1] Taxonomia este considerată „știința legilor de clasificare" (a se vedea Academia Română Institutul de lingvistică, Iorgu Iordan, *Dicționar explicativ al limbii române*, ed. a II-a, Ed. Univers Enciclopedic, București, 1998, p. 1072) sau „știința care se ocupă cu stabilirea legilor de clasificare şi sistematizare a domeniilor din realitate cu o structură complexă" (a se vedea DEX online, la http://dexonline.ro/ search.php?Cuv=taxonomie).

[2] A se vedea şi Berghe C. V., Riordan J. Piessens F., *A Vulnerability Taxonomy Methodology applied to web Services*, L.P. 4, disponibil on-line la http://chris.vandenberghe. org/publicattions/ vulnerability_taxonomy_nerdsec2005.pdf.

[3] Lough D. L., *A Taxonomy of Computer Attack with Application to Wireless Networks*, teză de doctorat susținută la Virginia Polytechnic Institute and State University, Virginia, (apr.), 2001, p. 37-39, disponibil on-line la http://scholar.lib.vt.edu/theses/available/etd-etd-04252001-234145/unrestricted/lough.dissertation.pdf. Lough compilează proprietățile unei taxonomii

- ***acceptată*** (Howard, 1997)/***adecvată*** (Amoroso, 1994), în sensul de a fi structurată de o asemenea manieră astfel încât să fie aprobată în general;
- ***comprehensibilă*** (Lindqvist şi Jonsson, 1997), în sensul de a putea fi înţeleasă atât de către specialişti, cât şi de către cei care manifestă interes în domeniu;
- ***completă*** (Amoroso, 1994)/***exhaustivă*** (Howard, 1997; Lindqvist şi Jonson, 1997), în sensul că ar trebui să ţină cont de toate posibilele ameninţări;
- ***precisă*** (Krsul, 1998; Bishop, 1999)***/clară*** (Howard, 1997; Lindqvist şi Jonsson, 1997), în sensul că trebuie să fie clar precizată astfel încât să evite ambiguitatea;
- ***repetabilă*** (Howard, 1997; Lindqvist şi Jonsson, 1997), în sensul că acele clasificări ar trebui să fie repetabile;
- ***folositoare*** (Howard, 1997; Lindqvist şi Jonsson, 1997), în sensul că trebuie să poată fi utilizată pentru o bună cunoaştere a domeniului;
- ***obiectivă*** (Krsul, 1998), în sensul că acele caracteristici trebuie să fie identificate de la obiectul cunoscut nu de la cunoştinţele subiectului;
- ***să se excludă reciproc*** (Howard, 1997; Lindqvist şi Jonsson, 1997), în sensul că o anumită ameninţare să fie grupată într-o singură categorie.

Faţă de caracteristicile prezentate, ***se poate concluziona***[1]:
- realizarea unei bune taxonomii este dificilă;
- taxonomia depinde nu numai de ameninţările respective ci şi de punctul de vedere a celui care o realizează, punct de vedere care este condiţionat de presupusa utilizare a taxonomiei;
- ameninţările, frecvent, se manifestă grupat şi prezintă proprietăţi comune.

Din motivele prezentate, nu surprinde marea diversitate a taxonomiilor dezvoltate în sfera securităţii sistemelor informatice şi reţelelor de comunicaţii.

Având în vedere că majoritatea acestor taxonomii au un pronunţat caracter tehnic, de specialitate, fiind dezvoltate de specialiştii din domeniul securităţii sistemelor informatice şi reţelelor de comunicaţii şi mai puţin pentru autorităţile de aplicare a legii, am să prezint în continuare acele taxonomii înţelese şi de aceia care nu sunt neapărat specialişti, dar manifestă interes în domeniul securităţii sistemelor informatice şi reţelelor.

---

din lucrările a cinci autori Amoroso E. G. (*Fundamentals of Computer Security Technology*, Prentice Hall, Englewood Clifs, N.J., 1994), Bishop M. (*How Attackers Break Programs, and How to Write Programs More Securely*, 8th net, USENIX Security Symposium, aug., 1999), Howard J. D. (*An Analysis of Security Incident on the Internet*, 1989-1995, teză de doctorat susţinută la Purdue University, apr., 1997), Krsul I. V. (*Software Vulnerability Analysis,* teză de doctorat susţinută la Purdue University, mai, 1998) Lindqvist U. şi Johnsson E., (*How to Systematically Classify Computer Security Intrusions*, IEEE Security and Privacy, 1997).

[1] A se vedea şi Berghe C.V., Riordan J., Piessens F., *A Vulnerability …*, *op. cit.*, p. 5.

§ 1. Palauskas N., Garsva E., Clasificarea atacurilor asupra sistemelor informatice[1]

Această taxonomie (numită de autori, din modestie, clasificare) este bazată atât pe clasificările anterioare cât şi pe experienţa autorilor.

Autorii consideră că fiecare *atac* întruneşte ***14 trăsături***[2] care sunt prezentate schematic şi în legătură[3]:

(1) *în funcţie de obiectivul atacului:*
- (1.1) dobândirea privilegiului administratorului (super-utilizatorului);
- (1.2) dobândirea privilegiului utilizatorului;
- (1.3) refuzarea serviciului;
- (1.4) încălcarea serviciului;
- (1.5) încălcarea confidenţialităţii informaţiilor sau resurselor sistemului;
- (1.6) executarea codurilor maliţioase;
- (1.7) încălcarea politicii de securitate.

(2) *în funcţie de tipul efectului:*
- (2.1) detectarea Codului executabil;
- (2.2) „Cal troian", virus;
- (2.3) detectarea Codului executabil al aplicaţiilor de (web) reţea;
- (2.4) utilizarea neautorizată a unei staţii de lucru intermediare tip „server Proxy";
- (2.5) inundarea memoriei tampon;
- (2.6) sondarea sau scanarea;
- (2.7) folosirea unor protocoale neacceptate;
- (2.8) folosirea unor porturi neacceptate;
- (2.9) deghizarea ca alt sistem „gazdă";
- (2.10) inserarea unor obiecte false.

(3) *în funcţie de nivelul modelului de referinţă ISO/OSI*
- (3.1) fizic;
- (3.2) conexiuni de date;
- (3.3) reţea;
- (3.4) transport;

---

[1] Palauskas N., Garsva E., *Computer System Attack Classification*, în Electronics and Electrical Engineering, nr. 2 (66), 2006, p. 84-87, disponibil on-line la http://www.ee.ktu.lt/journal/2006/2/1392-1215-2006-02-66-84.pdf.

[2] *Ibidem*, p. 85.

[3] *Ibidem*, p. 86.

(3.5) sesiune;
(3.6) prezentare;
(3.7) aplicație.
(4) *în funcție de sistemul de operare OS*
(4.1) Windows;
(4.2) Linux;
(4.3) Solaris;
(4.4) BSD;
(4.5) MacOS;
(4.6) altele.
(5) *în funcție de locația subiectului atacului*
(5.1) în interiorul segmentului local;
(5.2) între segmente;
(5.3) acces fizic;
(5.4) privilegiu de utilizator al sistemului;
(5.5) privilegiu de administrator de sistem.
(6) *în funcție de tipul locației obiectului*
(6.1) sistem local;
(6.2) rețea locală;
(6.3) rețea globală;
(6.4) rețea fără fir;
(6.5) rețea tip P2P.
(7) *în funcție de serviciul atacat*
(7.1) rețeaua (web), (HTTP);
(7.2) transfer de fișiere (FTP,SMB,CIFS);
(7.3) poștă (SMTP, POP 3, IMAP);
(7.4) control de rețea (SNMP);
(7.5) nume de domeniu (DNS);
(7.6) control la distanță (telnet, SSH, RDP);
(7.7) configurarea sistemului tip „Gazdă”;
(7.8) rutare dinamică (RIP, OSPF);
(7.9) incriptare (SSL);
(7.10) altele.
(8) *în funcție de concentrarea atacului*
(8.1) atomic;
(8.2) fragmentat.
(9) *în funcție de retroacțiune*
(9.1) cu retroacțiune;
(9.2) fără retroacțiune.

(10) *în funcție de condițiile inițiale de executare a atacului*
  (10.1) la solicitarea obiectului de atac;
  (10.2) la un eveniment specific obiectului de atac;
  (10.3) necondiționat.
(11) *în funcție de condițiile inițiale de executare a atacului*
  (11.1) pasiv;
  (11.2) activ.
(12) *în funcție de automatizarea atacului*
  (12.1) automatic;
  12.2 semi-automatic;
  12.3 manual.
(13) *în funcție de sursa atacului*
  (13.1) unu contra unu;
  (13.2) mai mulți contra unu;
  (13.3) unu contra mai mulți.
(14) *în funcție de calitatea legăturilor*
  (14.1) singură;
  (14.2) multiplă.

Autorii consideră[1] (și de aici se conturează caracterul de taxonomie) că „realizarea obiectivului este cea mai importantă pentru atacator (1), prin urmare, evaluarea numerică a severității atacului este fondată pe aceasta. Tipul efectului (2) depinde mai mult de obiectivul intrusului la fel ca și locația subiectului și obiectului. Modelul ISO/OSI poate descrie toate procesele de sistem. Nivelul aplicației (3.7) este cel mai potrivit, din cauza potențialității și complexității sale, pentru a efectua atacuri. Există o varietate de sisteme de operare OS în rețeaua globală, familii specifice de sisteme de operare OS au vulnerabilități comune care atrag atacuri specifice OS (4). Locația subiectului atacului (5) influențează tipul efectului și probabilitatea îndeplinirii obiectului atacului. Tehnologia atacului și posibilele amenințări sunt influențate de tipul locației obiectului (6) și de serviciul atacat (7). Atacul poate fi concentrat într-un singur pachet, și atacul este denumit atomic (8.1.) sau poate fi fragmentat în câteva pachete (8.2.). Retroacțiunea (9) nu este necesară pentru toate atacurile ... Pentru a evita detectarea sau pentru o mai bună eficiență, atacatorii pot alege diferite condiții inițiale de executare (10), tipuri de impact (11) sau nivele de automatizare (12). În conformitate cu obiectivele atacului și tipul efectului, numărul surselor atacului (13) și cantitatea legăturilor (14) pot diferi".

[1] *Ibidem*, p. 85.

§ 2. Howard John D., Longstaff Thomas A., Un limbaj comun pentru incidentele privind securitatea calculatoarelor[1]

Aceasta este una dintre cele mai bune taxonomii dezvoltate, şi are ca bază teza de doctorat a lui John Howard (unul dintre autori), „*O analiză a incidentelor de securitate pe Internet 1989-1995*"[2].

Autorii au dezvoltat un set minim de termeni de „nivel înalt", împreună cu o structură care indică legăturile dintre aceştia (o taxonomie), care poate fi folosită pentru a clasifica şi înţelege informaţiile incidentelor de securitate a calculatoarelor.

Unii autori susţin[3] „Howard încearcă să concentreze atenţia pe procesul care conduce taxonomia, mai degrabă, decât pe o schemă de clasificare ... Aceasta înseamnă că întregul proces al atacului este luat în considerare, ceea ce este, cu siguranţă, valoros ... Howard nu reuşeşte să îndeplinească una dintre cerinţele taxonomiei sale: să se excludă reciproc. Unele dintre categorii se pot suprapune ... pentru organele de informare cum ar fi CERT, o astfel de taxonomie nu poate fi practică. Organele de informare sunt mai preocupate de atacul în sine decât de motivaţiile şi obiectivele din spatele lui ... problemele menţionate mai sus există încă chiar cu taxonomia perfecţionată".

Nu sunt de acord cu aceste consideraţii şi chiar dacă unele dintre subcategoriile descrise nu s-ar exclude reciproc, aşa cum susţin autorii mai sus citaţi[4] dar şi alţii[5], totuşi, *consider mai valoroasă descrierea procesului prin care atacatorul reuşeşte să îşi îndeplinească obiectivul, decât o simplă clasificare a atacurilor*.

Revenind la taxonomia dezvoltată, şi la procesul care conduce această taxonomie, trebuie precizat că, faţă de taxonomia iniţială (Howard, 1997), aceasta este structurată în 7 categorii (faţă de 5 categorii) şi fiecare categorie este mai bine structurată şi dezvoltată.

---

[1] Howard J. D., Longstaff T. A., *A Common Language for Computer Security Incidents*, Sandia Report (SAND98-8667), (oct.) 1998, disponibil on-line la http://www. cert.org/research/taxonomy_988667.pdf.

[2] Howard J. D., *An Analysis of Security Incidents on the Internet 1989-1995*, teză de doctorat susţinută la Carnegie University, Pittsburg, Pensylvania, (apr.) 1997, disponibil on-line la http://www.dtic.mil/mil/cgi-bin/GetTRDoc?AD=ADA389085& Location=U2&doc=GetTRDOC.pdf.

[3] Hansman S., Hunt R., *A taxonomy of network and computer attacks*, în Computers &Security, (iun) 2004, p.4, disponibil on-line la http://ce.sharif.edu/courses/83-84/1/ce534/resorces/root/Papers/attacks; Steichen P., Advanced Security Methodologies – Computer and Network attacks, p. 15-16, disponibil on-line la http://pst.libre.eu/m2ssic-metz/02_attacks.pdf.

[4] *Ibidem*.

[5] Lough D. L., *A taxonomy …*, *op. cit.*, p. 50.

În prezentarea și explicarea taxonomiei dezvoltate, autorii identifică trei grupuri generale:

- ***eveniment*** – „o acțiune îndreptată către o țintă, intenționându-se a avea drept rezultat o schimbare a statusului țintei respective”[1] –, care include categoriile „acțiuni” și „ținte”, și este inclus grupul general „atac(uri)”;
- ***atac(uri)*** – „o serie de măsuri luate de un atacator pentru a obține un rezultat neautorizat”[2] –, care include, alături de grupul general „eveniment” și categoriile „unelte”, „vulnerabilitate” și „rezultate neautorizate” și este inclus în grupul general „incident” –;
- ***incident*** – „un grup de atacuri care se pot distinge de alte atacuri datorită deosebirii atacatorilor, atacurilor, obiectivelor, localizării și sincronizării”[3] – care include alături de grupul general „atac(uri)” și categoriile „atacatori” și „obiective” –.

Alături de aceste grupuri generale identifică alți termeni mai generali care pot fi necesari pentru a putea descrie complet un incident[4]:

- locația (numele, numărul, cele care au raportat);
- data (raportării, începerii, încheierii);
- numărul incidentului;
- acțiunile corective.

Categoriile și subcategoriile incluse în taxonomia dezvoltată sunt următoarele:

a) ***atacatorul*** – „un individ care încearcă unul sau mai multe atacuri pentru a atinge un obiectiv” –; din această categorie fac parte:

- ***hackeri*** – „atacatori care atacă calculatorul pentru provocare, statut sau emoția obținerii accesului” –;
- ***spioni*** – „atacatori care atacă calculatoarele pentru informații care să fie folosite pentru avantaje politice” –;
- ***teroriști*** – „atacatori care atacă calculatoarele pentru a provoca teamă pentru avantaje politice” –;
- ***invadatori corporativi*** – „angajați (atacatori) care atacă calculatoarele concurenților pentru câștig financiar” –;
- ***criminali profesioniști*** – „atacatori care atacă calculatoarele pentru câștig financiar” –;
- ***vandali*** – „atacatori care atacă calculatoarele pentru a provoca daune” –.

b) ***instrumentul*** – „mijloc de exploatare a vulnerabilității unui calculator sau rețele” –; din această categorie fac parte:

---

[1] Howard J. D., Longstaff T.A., *A Common Language …*, *op. cit.*, p. 7.
[2] *Ibidem*, p. 12.
[3] *Ibidem*, p. 15.
[4] *Ibidem*, p. 17-18.

- *atac fizic* – „mijloc de a fura fizic sau a strica calculatorul, rețeaua, componentele sale sau sistemele de suport ale sale (cum ar fi aerul condiționat, energia electrică etc.)" –;

- *schimb de informații* – „un mijloc de a obține informații de la alți „atacatori" (cum ar fi buletine electronice), sau de la persoane care au fost atacate (așa numita inginerie socială)" –;

- *comandă a utilizatorului* – „un mijloc de a exploata o vulnerabilitate prin introducerea de comenzi într-un proces prin intermediul introducerii de date direct de utilizator în interfața procesului. Un exemplu este introducerea comenzilor Unix prin intermediul unei conexiuni telnet sau de la un port SMPT" –;

- *script sau program* – „un mijloc de a exploata o vulnerabilitate prin introducerea de comenzi într-un proces prin executarea unui fișier de comenzi (script) sau a unui program în interfața procesului. Exemple sunt o sesiune Shell script pentru a exploata o eroare a programului, un program de conectare tip cal troian sau un program de spargere a parolei" –;

- *agent autonom* – „un mijloc de exploatare a unei vulnerabilități prin utilizarea unui program sau a unui fragment dintr-un program care operează independent de utilizator. Exemple sunt virușii și viermii" –;

- ***kit de instrumente*** – „un pachet de programe care conține scripturi, programe sau agenții autonome care exploatează vulnerabilitățile. Un exemplu este larg răspânditul kit de instrumente numit kit de acces la rădăcină" –;

- ***instrument distribuit*** – „un instrument care poate fi distribuit la mai multe sisteme tip gazdă care pot fi apoi coordonate pentru a efectua în mod anonim un atac „după un anumit timp simultan asupra unor sisteme tip gazdă" –;

- ***interceptor de date*** – „un mijloc de monitorizare a radiațiilor electromagnetice provenite de la un calculator sau rețea folosind un dispozitiv extern" –.

c) ***vulnerabilitate*** – „un punct slab într-un sistem care să permită o acțiune neautorizată" –; din această categorie fac parte:

- *vulnerabilitate de proiectare* – „o vulnerabilitate în proiectarea sau specificațiile echipamentului sau programului care chiar și după o implementare perfectă va avea ca rezultat o vulnerabilitate" –;

- *vulnerabilitate de implementare* – „o vulnerabilitate care rezultă dintr-o eroare în implementarea programului sau echipamentului care au fost proiectate corespunzător" –;

- *vulnerabilitate de configurare* – „o vulnerabilitate care rezultă dintr-o eroare în configurarea unui sistem, cum ar fi să ai un cont cu parole implicite, să ai permisiune de scriere ... pentru fișiere noi sau să ai active servicii vulnerabile" –.

d) ***acțiune*** – „o măsură luată de către un utilizator sau proces în vederea obținerii unui rezultat"; din această categorie fac parte:

- *sondare* – „accesarea unei ținte în vederea determinării caracteristicilor sale"–;

- *scanare* – „accesarea secvențială a unui set de ținte în scopul de a identifica care țintă are o caracteristică specifică" –;

- *inundare* – „accesarea repetată a unei ținte în scopul de a supraîncărca capacitatea țintei" –;

- *autentificare* – „prezentarea identității cuiva unui proces și, dacă este necesar, verificarea acelei identități în vederea accesării unei ținte" –;

- *ocolire* – „evitarea unui proces prin utilizarea unei metode alternative de accesare a țintei" –;

- *păcălire* – „deghizare prin „asumarea apariției unei alte entități în rețea" –;

- *citire* – „obținerea conținutului datelor din dispozitivele de stocare sau alte medii de date" –;

- *copiere* – „reproducerea unei ținte lăsând neschimbată ținta originală" –;

- *furt* – „luarea în posesie a unei ținte fără a lăsa o copie în locația originală" –

- *modificare* – „schimbarea conținutului sau caracteristicilor unei ținte" –;

- *ștergere* – „îndepărtarea unei ținte sau transformarea în irecuperabilă" –.

e) ***țintă*** – „o entitate logică sau fizică a unui calculator sau rețele" –:

- *cont* – „un domeniu pentru accesul utilizatorului pe un calculator sau rețea care este controlat ținându-se seama de o înregistrare de informații care conține numele contului utilizatorului, parola și restricții de utilizare" –;

- *proces* – „un program în executare, constând în programul executabil, datele și stiva programului, controlul programului, indicatorul de stivă SP și alți regiștrii și toate celelalte informații necesare pentru executarea unui program" –;

- *dată* – „reprezentarea de date, concepte sau instrucțiuni într-o manieră adecvată pentru comunicare, interpretare sau prelucrare de către om sau prin mijloace automate. Datele pot fi sub forma fișierelor, în memoria volatilă sau permanență a calculatorului sau într-un dispozitiv de stocare, sau într-o formă de date în tranzit printr-un mediu de transmitere" –;

- *componentă* – „una dintre părțile din care este făcut calculatorul sau rețeaua"–;

- *calculator* – „un dispozitiv care este alcătuit din unul sau mai multe componente asociate, inclusiv unitatea de procesare și unitățile periferice, care este controlată de programe stocate intern și care poate efectua calcule substanțiale, incluzând numeroase operațiuni matematice sau operațiuni logice, fără intervenție umană în timpul execuției" –;

- *rețea* – „un grup de calculatoare gazdă interconectate și interdependente, elemente de comutare și ramificații interconectate" –;

- *inter-rețele* – „o rețea de rețele" –.

f) ***rezultat neautorizat*** – „o consecință neautorizată a unui eveniment" –; din această categorie fac parte:

- ***acces crescut*** **–** „o creştere neautorizată în domeniul de acces de pe un calculator sau reţea" –;

- ***divulgare de informaţii*** **–** „diseminarea de informaţii către orice persoană care nu este autorizată să acceseze acele informaţii" –;

- ***falsificare de informaţii*** **–** „modificarea neautorizată a datelor de pe un calculator sau reţea" –;

- ***refuzare a serviciului*** **–** „deteriorarea sau blocarea intenţionată a resurselor calculatorului sau reţelei" **–**;

- ***furt de resurse*** **–** „utilizarea neautorizată a resurselor calculatorului sau reţelei" –;

g) ***obiective*** – „scopul sau obiectivul final al unui incident" –; din această categorie fac parte:

- ***provocare, status, emoţie;***
- ***câştiguri politice;***
- ***câştiguri financiare;***
- ***pagubă*****.**

Taxonomia completă este prezentată de autori sub formă grafică[1] fiind evidenţiată relaţia dintre evenimente, de la atacuri la incidente, şi sugerează că prevenirea îndeplinirii obiectivelor atacatorilor ar putea fi realizată prin asigurarea faptului că un atacator nu ar reuşi parcurgerea celor şapte paşi descrişi mai sus.

§ 3. Weber Daniel James, O taxonomie a intruziunilor în calculatoare[2]

Taxonomia dezvoltată de acest autor, a fost creată special pentru testarea şi evaluarea sistemelor de detectare a intruziunilor (IDS).

Autorul consideră[3] „taxonomia necesită un mod de descriere a nivelurilor privilegiului, un mod de descriere a tranziţiilor şi un mod de clasificare a acţiunilor". Astfel:

(1) ***niveluri ale privilegiului utilizatorului***:

a) ***fără acces (O)***, când nu are practic acces la un sistem;

b) ***reţea la distanţă (R)***, când are un minim acces de reţea la un sistem prin intermediul altor reţele;

---

[1] *Ibidem*, p. 16.

[2] Weber D. J., *A Taxonomy of Computer Intrusions*, lucrare de dizertaţie susţinută la Massachuetts Institute of Technology, (iun.) 1998, disponibil on-line la http://dspace.mit.edu/bitstream/handle/1721.1/9861/41473759.pdf.

[3] *Ibidem*, p. 40.

c) ***rețea locală (L)***, când are abilitatea să citească și să scrie în rețeaua locală ceea ce dispozitivul țintă folosește;

d) ***acces modem (M)***, când are abilitatea să se conecteze direct la un calculator țintă;

e) ***acces utilizator (U)***, când are abilitatea să ruleze comenzi normale de utilizator;

f) ***acces la rădăcină/status de administrator (S)***, când are acces total la sistem.

(2) ***acțiuni***:

a) ***sondare***, în situația în care sunt colectate datele despre sistem:

- sondare (Utilizator), când privesc utilizatorul dispozitivului;

- sondare (Serviciu), când privesc serviciile dispozitivului;

- sondare (Dispozitiv), când privesc dispozitivele în rețea.

b) ***refuz al serviciului***, în situația în care este împiedicat accesul legitim la sistem (include deteriorarea serviciului):

- Refuz (Temporar), când refuzul este temporar, cu recuperare automată;

- Refuz (Administrativ), când refuzul necesită acțiunea administratorului pentru recuperare;

- Refuz (Permanent), când refuzul este permanent.

c) ***interceptare/citire a datelor***, în situația în care sunt interceptate/citite datele:

- interceptare (Fișiere), când sunt vizate fișierele unui sistem;

- interceptare (Rețea), când este vizat traficul de rețea.

d) ***alterare/creare a datelor***, în situația în care sunt alterate/create datele:

- Alterare (Date), când vizează alterarea datelor stocate;

- Alterare (Urmărire, intruziune), când vizează înlăturarea urmelor intruziunii.

e) ***utilizare a sistemului de către atacatori***, în situația în care sistemul țintă este utilizat de atacator:

- Utilizare (Recreațională), când vizează utilizarea sistemului pentru distracție;

- Utilizare (Productivă), când vizează utilizarea sistemului în scopuri productive;

- Utilizare (În legătură cu intruziunea), când vizează utilizarea resurselor sistemului pentru a-l ajuta să pătrundă în alte locații;

- Utilizare (Regizare atacuri), când vizează utilizarea calculatorului ca o trambulină pentru lansarea altor atacuri pe alte sisteme.

(3) ***metode de tranziție***:

a) ***deghizare (m)***, în situația în care se prezintă într-o lumină falsă;

b) ***abuzare de facilități (a)***, în situația în care acțiunile legitime sunt duse către extreme;

c) ***implementare de erori (b)***, în situația în care o eroare într-un program de încredere permite atacul.

Autorul folosește un șir de caractere alfa numerice pentru a prezenta și descrie unele dintre atacurile comune[1].

Atac	Șir (de caractere alfa numerice)	Descriere
Inundare cu pachete SYN	R–a–Refuz (Temporar)	Utilizatorul are nevoie de acces la rețea pentru a realiza un refuz temporar al serviciului
Analiza parolelor	L–a–Intercep-tare (Rețea)	Utilizatorul cu acces la rețeaua unui calculator citește parolele
Spargerea parolelor	U–Folosire (Intruziune)	De la un cont de utilizator, cineva folosește sistemul pentru a sparge parolele
Aruncare	U–b–s	Utilizatorul exploatează o eroare în programul de scoatere și devine administrator
Ghicirea parolei	R–a–U	Utilizatorul cu acces la rețea ghicește în mod repetat parolele
Scriere FTP	U–b–s: Alterare (Date)	O eroare de câteva FTP care permite unui utilizator să creeze pe sistem orice fișier care nu exista anterior, cum ar fi punerea unui fișier nou într-o bază de date. Acesta nu se transformă în mod necesar într-un compromis al rădăcinii.
Cal troian	U'–U''–Interceptare (Date)	Un utilizator solicită unui al doilea utilizator să ruleze un anumit program. Când al doilea utilizator a procedat în acest sens, directorul de poștă electronică este făcut public, permițându-i celui de-al doilea utilizator să citească fișierele.

Sursă: Weber D. J., *A Taxonomy of Computer Intrusion*, lucrare de dizertație susținută la Massachusetts Institute of Technology, (iun.) 1998, p. 51

§ 4. Lough Daniel Lawry, O taxonomie a atacurilor asupra calculatoarelor cu aplicație pentru rețelele fără fir[2]

Cu toate că taxonomia dezvoltată de acest autor este prea generală, ea are la bază o analiză complexă atât a atacurilor, cât și a altor puncte de vedere prezentate de alți autori.

[1] *Ibidem*, p. 51.

[2] Lough D. L., *A Taxonomy of Computer Attack with Application to Wireless Networks*, teză de doctorat susținută la Virginia Polytechnic Institute and State University, Virginia, (apr.), 2001, disponibil on-line la http://scholar.lib.vt.edu/theses/available/etd-etd-04252001-234145/unrestricted/lough.dissertation.pdf.

Autorul a denumit-o VERDICT, un acronim al celor patru cauze considerate responsabile pentru erorile securității calculatoarelor – Validare (V), Expunere (E), Randomizare (R), Dealocare (D) – și al condițiilor inadecvate (ICT), susținând[1] că „acoperă toate aspectele procesului de securitate, de la securitatea fizică la dispozitivele și programele sistemelor".

Potrivit autorului[2], „o vulnerabilitate poate fi rezultatul uneia sau mai multor din cele patru caracteristici", astfel:

- validarea, este o problemă generală; o validare inadecvată (incorectă/ ineficientă) ar putea permite unei erori să apară; în plus, față de validarea sistemului de operare (OS), include de asemenea securitatea fizică;

- expunerea, poate fi o cauză a unei alte erori sau un efect al unei alte erori; totul, inclusiv variabile, obiecte și acțiuni, ar trebui să fie considerate expuse necorespunzător până se probează contrariul;

- randomizarea, este una dintre stâlpii fundamentali ai criptografiei, dar este folosită și în alte situații ca: parolele, vectorii de inițiere etc.; o randomizare inadecvată poate genera o expunere la un atac;

- dealocarea, sau rămășițele care rezultă în urma dealocării, cuprinde mai mult decât ștergerea datelor din calculator; având în vedere tipurile de rămășițe (acces, compunere și date), o dealocare necorespunzătoare poate genera probleme.

Având în vedere caracterul prea general, și faptul că nu folosește termenii recunoscuți pentru descrierea atacurilor (gen: virus, vierme, cal troian, etc.), s-ar putea să nu fie folositoare organismelor de informare pentru îndeplinirea sarcinilor zilnice de a identifica atacurile noi și a furniza sfaturi pentru acestea.

§ 5. RAND Europe, O taxonomie a incidentelor de securitate

În Manualul de proceduri legale ale abuzului de calculator și rețea (versiunea actualizată din 2005)[3] este propusă o taxonomie a incidentelor de securitate în funcție de care s-a solicitat țărilor corespondente să furnizeze informații.

Această taxonomie are la bază clasificarea din versiunea inițială (2003) a manualului[4] la care adaugă mesajele comerciale nesolicitate tip „spam".

---

[1] *Ibidem*, p. 158.

[2] *Ibidem*, p. 152.

[3] RAND Europe & Lawfort, *Update to the Handbook of Legal Procedures of Computer Misuse in EU Countries for assisting CSIRTS*, (dec.) 2005, p. 13-15, disponibil on-line la http://www.rand.org/pubs/technical_reports/2006/RAND_TR337.pdf.

[4] RAND Europe, *Handbook of Legislative Procedures of Computer and Network Misuse In EU Countries*, 2002, p. 12-14, disponibil on-line la http://europa.eu.int/information_ society/ europe/2005/doc/all_about/csirt_handbook_v1.pdf.

Cu toate că se intitulează taxonomie, este de fapt o clasificare și o descriere a unor categorii de incidente.

Consider că prima clasificare, din versiunea inițială (2003) a manualului, descrie și explică mai bine categoriile de incidente identificate, și am să o prezint, în continuare.

Inițial, au fost identificate ***8 categorii de abuzuri ale calculatoarelor și incidente de securitate*** pe care echipele de răspuns la incidente de securitate (CSIRT) le poate trasa dincolo de contextele juridice diferite, și anume:

(1) ***amprentare a calculatorului*** (țintei)

- ***definiție***: acțiuni efectuate în scopul de a strânge informații despre o țintă;
- ***tehnici***: sondare, scanare, interogare a DNS-ului, trimitere pachete cu ecou;
- ***vector de atac***: porturi active VDP/TCP, O/S, adrese ale calculatoarelor tip gazdă, caracteristici ale calculatoarelor tip server SNMP.

(2) ***cod malițios***

- ***definiție***: compromiterea țintei gazdă prin intermediul executării unui program independent;
- ***tehnici***: executarea voluntară sau involuntară a unui program independent;
- ***vector de atac***: viruși, viermi, căi ascunse, troieni.

(3) ***refuz al serviciului***

- ***definiție***: accesare repetată a țintei care supraîncarcă capacitatea sau întrerupe serviciul;
- ***tehnici***: executare a programelor care efectuează cereri nesfârșite a resurselor calculatorului cum ar fi: memoria, tipul procesorului, conexiunile TCP – UDP, spațiul discului;
- ***vector de atac***: inundare SYN, „ping-uirea morții".

(4) ***compromitere a contului***

- ***definiție***: acces neautorizat la un sistem sau la resursele sistemului la nivel de administrator de sistem (rădăcină) sau utilizator;
- ***tehnici***: exploatare, fie la nivel local fie la distanță, a vulnerabilităților programului în vederea obținerii accesului neautorizat la conturile utilizatorului. Același rezultat poate fi obținut prin folosirea acreditivelor care au fost obținute ilegal (furt, interceptare, coerciție);
- ***vector de atac***: inundarea memoriei tampon, atacuri tip CGI sau folosirea acreditivelor furate (nume utilizator și parolă).

(5) ***tentativă de intruziune***

- ***definiție***: tentativă de acces neautorizat la un sistem;
- ***tehnici***: fie încercarea de a obține acces la un sistem prin ghicitul acreditivelor utilizatorului, fie încercarea fără succes de a executa oricare dintre vectorii de atac descriși aici;

- ***vector de atac***: tentative multiple de conectare, tentative de inundare a memoriei tampon, folosirea identității utilizatorului/parolei implicite; tentativa de exploatare a vulnerabilităților mai vechi, tentativa de folosire a conturilor implicite, tentativa de conectare a porturilor SMNP.

6) ***acces neautorizat la informații***

- ***definiție***: tentativa de a obține acces neautorizat la date;

- ***tehnici***: încercarea de a obține accesul la date, fie la nivel local, fie la distanță, eludând mecanismele de control al accesului;

- ***vector de atac***: injectare SQL, manipulare parametrii CGI.

(7) ***acces neautorizat la transmisii***

- ***definiție***: interferența fără drept și prin mijloace tehnice, cu transmisiile non-publice de date informatice la, de la sau în interiorul unui sistem informatic;

- ***tehnici***: interceptare de pachete de rețea sau scoatere de pachete din fluxul de trafic;

- ***vector de atac***: deturnarea sesiunii, atac tip „omul din mijloc", interceptare, înregistrare.

(8) ***modificare neautorizată a informației***

- ***definiție***: modificare neautorizată a informațiilor care sunt ținute într-un sistem informatic în formă electronică;

- ***tehnici***: modificarea sau crearea local sau la distanță, oricărui tip de date, care rezidă în calculator fără autorizația necesară;

- ***vector de atac***: viruși, modificarea fișierelor, jurnal, instalarea programelor neautorizate, injectare SQL, scoaterea din arhive, formatarea discului dur.

(9) ***accesare neautorizată a sistemelor de comunicații***

- ***definiție***: utilizare neautorizată a unui sistem de comunicații;

- ***tehnici***: modificarea setărilor de configurarea sistemelor de comunicații în vederea obținerii de avantaje personale din utilizarea acestora;

- ***vector de atac***: falsificarea DNS, utilizarea neautorizată a agenților de transfer de poștă electronică, Proxy, modificarea tabelelor de rutare.

Capitolul II

Conceptul, principalele caracteristici şi evoluţia criminalităţii informatice

Secţiunea I
Consideraţii generale

Aşa cum precizam, „informatizarea" vieţii sociale şi „tehnologizarea" făptuitorilor au constituit premisele apariţiei (sau grefarea elementelor „clasice" de criminalitate) unei noi forme de manifestare a criminalităţii (în general), criminalitatea informatică.

Secţiunea a II-a
Conceptul „criminalitate informatică"

§ 1. Noţiunea de criminalitate

Definită liber, *criminalitatea* desemnează *ansamblul infracţiunilor comise într-un interval temporal şi spaţial determinat*.

Valenţele noţiunii de criminalitate pot fi multiple; în funcţie de anumite criterii de clasificare, dintre cele mai des întâlnite[1], amintim:

a) în funcţie de criteriul *subiectiv*, se subclasifică, având în vedere ***elementele de referinţă cu care se operează***:

- *spaţial*: criminalitate naţională/regională/zonală, care presupune *totalitatea infracţiunilor comise pe teritoriul* unui/unei anumit/anumite stat/regiune/zone;
- *temporal*: criminalitate anuală/semestrială/lunară/zilnică, care presupune că *în acel interval temporal se comite un anumit număr de infracţiuni*;
- *modalitatea comiterii*: criminalitate *cu violenţă* (lovirile, vătămările corporale, tâlhăria etc.)/*fără violenţă* (furtul, înşelăciunea etc.) etc.;
- *subiecţi activi*: criminalitate *feminină/masculină*, criminalitate *juvenilă/adultă*, criminalitate *obişnuită/a „gulerelor albe"* etc.

---

[1] A se vedea şi Sandu I. E., Sandu F., Ioniţă G. I., *Criminologie*, Ed. Sylvi, Bucureşti, 2001; Nistoreanu G., Păun C., *Criminologie*, Ed. Europa-Nova, Bucureşti, 1996; Stănoiu R.M., *Criminologie*, Ed. Oscar Print, Bucureşti, 1998; Cioclei V., *Manual de criminologie*, Ed. All Beck, Bucureşti, 1998.

b) în funcție de criteriul *obiectiv*, se subclasifică, având în vedere ***gradul diferit de cunoaştere a amplorii fenomenului*** de către organele de aplicare a legii:

- *criminalitatea reală*, care presupune *totalitatea infracțiunilor comise efectiv*, indiferent dacă sunt/nu sunt cunoscute de către organele de aplicare a legii;

- *criminalitatea aparentă*, care presupune *totalitatea faptelor aparent penale* (nu infracțiuni, pentru că în urma administrării probelor se poate confirma sau înlătura această aparență) *semnalate* organelor de aplicare a legii și înregistrate ca atare;

- *cifra neagră a criminalității*, care presupune diferența dintre criminalitatea reală și criminalitatea aparentă și este reprezentată de *infracțiunile comise efectiv dar care rămân necunoscute* organelor de aplicare a legii din diferite motive (abilitatea făptuitorilor, omisiunea încunoștințării organelor de aplicare a legii, ineficiența sistemului judiciar, pasivitatea victimelor etc.);

- *criminalitatea legală*, care *presupune totalitatea faptelor penale pentru care s-au pronunțat* hotărâri definitive de condamnare.

§ 2. Noțiunea de criminalitate informatică[1]

La nivel internațional/regional nu se manifestă un consens în ceea ce privește terminologia fenomenului.

Pentru a descrie infracțiunile comise prin intermediul/asupra sistemelor informatice și rețelelor de comunicații sunt folosiți termeni precum: ***„criminalitate în legătură cu (utilizarea) calculatorul (ui)"*** *(„computer-related crime")*, ***„criminalitate informatică"*** (*„cybercrime"/„computer crime"),* ***„criminalitate cibernetică"*** *(„cyber crime"),* ***„criminalitate de înaltă tehnologie"*** (*„high-tech crime"*), ***„criminalitate electronică"*** (*„electronic crime"/„e-crime"*).

Însăși încercările de definire a fenomenului sunt destul de stângace și controversate, astfel că, de cele mai multe ori, se evită, reținându-se doar o clasificare funcțională a infracțiunilor la care acesta face referire.

Primele încercări de definire a fenomenului au fost prezentate în ***Raportul Organizației pentru Cooperare și Dezvoltare Economică*** (OECD) „Criminalitatea

[1] Ioniță G.I., *Criminalitatea informatică și investigarea criminalistică digitală – controverse terminologice și de conținut*, în Revista Română de Criminalistică, iunie 2010, vol. XI, nr. 3, Editura Asociației Criminaliștilor din România, București, 2010, p. 395-398; *Idem*, *Conceptul, principalele caracteristici și evoluția criminalității informatice*, în Instituții juridice contemporane în contextul integrării României în Uniunea Europeană, ed. a III-a, Ed. Pro Universitaria, București, 2009, p. 765-770.

în legătură cu calculatorul: Analiza politicilor legale"[1], grupul de experţi adoptând ca definiţie de lucru „abuzul informatic este considerat orice comportament ilegal, neetic sau neautorizat în legătură cu procesarea automată şi transmiterea datelor" neconsiderând utilă o definire mai precisă, dar optând pentru o clasificare funcţională.

Nici mai recent această problemă nu a fost clarificată, astfel că în ***Comunicarea Comisiei Comunităţilor Europene*** „Către o politică generală de luptă împotriva criminalităţii cibernetice"[2], „criminalitatea cibernetică" este înţeleasă ca „infracţiuni comise prin utilizarea reţelelor de comunicare electronice şi a sistemelor de informare sau împotriva unor astfel de reţele sau de sisteme".

Din fericire, ***furnizorii de soluţii*** pentru securitatea sistemelor informatice şi reţelelor de comunicaţii, abordează noţiunea mai pragmatic, considerând[3] criminalitatea informatică „orice infracţiune care este comisă prin utilizarea calculatorului sau a reţelei, sau a dispozitivului (hardware)".

Resursele Internet de informare consideră această formă de manifestare a criminalităţii o „activitate criminală în care calculatorul sau reţeaua este sursă, instrument, ţintă sau locul infracţiunii"

Au existat ***încercări de definire*** în felurite moduri, pentru a servi studiilor efectuate în domeniu[4].

Astfel, s-a definit[5] criminalitatea informatică ca „orice acţiune ilegală în care un calculator este instrumentul sau obiectul unei infracţiuni; cu alte cuvinte, orice infracţiune al cărei mijloc sau scop este să influenţeze funcţionarea calculatorului", sau s-a definit abuzul informatic ca „orice incident asociat cu tehnologia informatică în care o victimă a suferit sau ar fi putut să sufere o pagubă şi din care autorul, intenţionat, a obţinut sau ar fi putut obţine un câştig".

În ***Strategia de securitate cibernetică a României***[6], *criminalitatea informatică* a fost considerată „totalitatea faptelor prevăzute de legea penală sau de

---

[1] OECD report, ICCP no. 10, Computer-related Crime: Analysis of Legal Policy,1986.

[2] Commission of The European Communities, Communication from The Commission to The European Parliament, The Council and The Committee of The Regions, COM (2007) 267 final, Brussels, 22.05.2007, disponibil on-line la http://eur-lex. europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:026:FIN:EN:PDF.

[3] Symantec, *What is cybercrime?*, disponibil on-line la http://www.symantec.com/norton/cybercrime/definition.jsp.

[4] Council of Europe, *Computer-related Crime, Recommendation No. R (89) 9 on computer-related crime and final report of the European Committie on Crime Problems*, Council of Europe Publishing and Documentation Service, Strasbourg, 1990, p. 13.

[5] *Ibidem*.

[6] Stategia de securitate cibernetică a României din 15.05.2013, publicată în M. Of. nr. 296/23.05.2013.

alte legi speciale care prezintă pericol social şi sunt săvârşite cu vinovăţie, prin intermediul ori asupra infrastructurilor cibernetice".

Fără a comenta, în detaliu, această „definiţie", trebuie observat că se pleacă de la definiția infracțiunii [aşa cum era prevăzută de art. 17 C. pen. (1968)], dar se face o ***confuzie nepermisă*** prin precizarea faptelor „prevăzute de legea penală sau de alte legi speciale", întrucât [potrivit art. 141 C. pen. (1968)] prin „lege penală" se înțelegea (şi se înțelege) „orice dispoziţie cu caracter penal" indiferent în ce act normativ este cuprinsă.

Plecând de la definiția criminalității (în general), mai sus prezentată, *dar adaptând-o particularităților proprii* acestei forme de manifestare a criminalităţii, am considerat ***criminalitatea informatică*** ca fiind ***ansamblul infracțiunilor comise, prin intermediul sau în legătură cu utilizarea sistemelor informatice sau rețelelor de comunicații, într-un interval temporal şi spațial determinat.*** *Sistemele informatice şi rețelele de comunicații pot fi instrumentul, ținta sau locația acestor infracțiuni.*

§ 3. Infracțiuni din sfera criminalității informatice[1]

Având în vedere *tipologia prevăzută în Convenția* privind criminalitatea informatică, dar completând-o, în funcţie de modalităţile de manifestare a fenomenului, am considerat că *infracțiunile din sfera criminalității informatice* pot fi **grupate** în:

A. ***Infracțiuni împotriva confidențialității, integrității şi disponibilității datelor şi sistemelor informatice***:

- Accesarea ilegală;
- Interceptarea ilegală;
- Afectarea integrităţii datelor;
- Afectarea integrităţii sistemului.

B. ***Infracțiuni informatice***:

- Falsificarea informatică;
- Frauda informatică;

[1] Ioniță G.I., *Criminalitatea informatică şi investigarea criminalistică digitală – controverse terminologice şi de conținut*, în Revista Română de Criminalistică, iunie 2010, vol. XI, nr. 3, Editura Asociației Criminaliştilor din România, Bucureşti, 2010, p. 395-398; *Idem*, *Conceptul, principalele caracteristici şi evoluția criminalității informatice*, în Instituții juridice contemporane în contextul integrării României în Uniunea Europeană, ed. a III-a, Ed. Pro Universitaria, Bucureşti, 2009, p. 765-770.

- Furtul de identitate;
- Abuzurile asupra dispozitivelor.

C. ***Infracțiuni referitoare la conținut***:

- Interacțiunea cu materialul pornografic și erotic (în țările unde este incriminat ca infracțiune);
- Pornografia infantilă;
- Actele de natură violentă, rasistă sau xenofobă;
- Actele care privesc convingerile religioase (în țările unde este incriminată ca infracțiune);
- Jocurile de noroc ilegale și jocurile online;
- Atacurile cu mesaje nesolicitate tip „spam";
- Furnizarea de informații privind săvârșirea de infracțiuni.

D. ***Infracțiuni referitoare la atingerile aduse drepturilor de proprietate intelectuală***:

- Încălcarea drepturilor de autor și a drepturilor conexe;
- Încălcarea drepturilor de proprietate industrială.

E. ***Infracțiuni complexe***:

- Terorismul informatic;
- Războiul informatic;
- „Spălarea" banilor prin intermediul sistemelor informatice;
- Atacurile tip „phishing".

Este evident că această clasificare ***comportă îmbunătățiri***, dar *prezintă unele avantaje*:

- include grupele de infracțiuni stabilite de Convenția privind criminalitatea informatică, grupe care sunt acceptate și consacrate la nivel internațional (chiar dacă sunt unele probleme de armonizare a legislațiilor interne);
- introduce o nouă grupă „Infracțiuni complexe", necesară de altfel, dat fiind formele cele mai grave de manifestare a criminalității informatice (terorismul informatic, războiul informatic, „spălarea" banilor prin intermediul sistemelor informatice, atacurile tip „phishing" etc.), fie nu sunt incriminate fie sunt adăugate forțat în alte grupări;
- poate cuprinde marea majoritate a formelor particulare de manifestare a criminalității informatice existente, dar și altele noi care pot să apară.

La o analiză atentă a acestei clasificări (întrucât nu pot să o numesc taxonomie) se poate constata că aceasta ***respectă***, în mare măsură, ***caracteristicile unei taxonomii*** (în concordanță cu cele compilate de Lough și prezentate mai sus). Rămâne doar ca ***în timp să*** *se demonstreze utilitatea și*, în acest mod, *acceptabilitatea acesteia*.

Secțiunea a III-a
Principalele caracteristici ale criminalității informatice[1]

Analiza cazuisticii criminalității informatice, conturează următoarele ***caracteristici***[2] ale fenomenului:

A. ***Transfrontalitate***: această caracteristică este dată de faptul că utilizarea (legitimă/nelegitimă) sistemelor informatice şi reţelelor de comunicaţii, depăşeşte frontierele convenţionale ale statelor.

B. ***Anonimitate***: această caracteristică se concretizează printr-un avantaj al făptuitorului, respectiv acela de a rămâne necunoscut de victime/autorităţile de aplicare a legii (cel puţin în momentul comiterii infracţiunii), datorită faptului că nu este prezent la locul faptei şi nu poate fi identificat fizic (aşa cum se întâmplă în majoritatea infracţiunilor).

C. ***Credibilitate***: această caracteristică s-a desprins datorită faptului că orice instituţie/unitate, din orice domeniu, are un site Internet iar utilizatorul, bazându-se pe încrederea în autorităţi, dar şi pe faptul că site-ul este un loc public, poate fi uşor înşelat.

D. ***Simplitate***: această caracteristică este conturată de faptul că, spre deosebire de alte infracţiuni, comiterea infracţiunilor din sfera criminalităţii informatice nu presupune acte pregătitoare costisitoare sau mijloace complicate de finalizare a activităţii infracţionale; practic, pentru comiterea multor astfel de infracţiuni, este nevoie doar de un sistem informatic conectat la Internet şi de minime cunoştinţe în domeniu.

E. ***Rapiditate***: această caracteristică este conferită de transmiterea aproape instantanee a datelor prin sistemele informatice; singura condiţie impusă fiind ca sistemele să fie conectate într-o reţea; acest aspect poate fi esenţial pentru comiterea unor infracţiuni.

F. ***Costuri foarte reduse***: această caracteristică a apărut ca urmare a faptului că tehnologia informaţiilor a devenit, din ce în ce mai accesibilă, şi din punct de vedere al costurilor; în prezent, pentru orice persoană de condiţie medie, costurile achiziţionării unor sisteme informatice sunt rezonabile iar obţinerea accesului la Internet presupune cheltuieli din ce în ce mai reduse.

---

[1] Ioniță G. I., *Principalele caracteristici ale criminalității informatice la sfârșitul secolului XX și începutului de mileniu,* în volumul (4) A noua sesiune de comunicări ştiinţifice a cadrelor didactice din Universitatea Româno-Americană cu participare internaţională, 28-29 mai 2004, Ed. Universul Juridic, Bucureşti, 2006, p. 206-211.

[2] A se vedea şi Alecu G., Barbăneagră A., *Reglementarea penală şi investigarea criminalistică din domeniul informatic*, Ed. Pinguin Book, Bucureşti, 2006, p. 13-25.

Secțiunea a IV-a
Aspecte privind evoluția criminalității informatice[1]

Comparativ cu oricare altă invenție importantă, calculatoarele au trecut mult mai rapid prin stadiile de dezvoltare, amplasare și integrare socială și au generat schimbări sociale și politice care, rareori, au fost anticipate și remarcate[2].

Este adevărat că această utilizare a calculatoarelor, în toate sectoarele vieții sociale (transporturi, telecomunicații, servicii medicale, siguranță națională etc.), a condus la dezvoltarea societății (în ansamblu) dar, în același timp, a favorizat și dezvoltarea și specializarea activităților criminale.

Poate că, și din acest motiv, se consideră[3] că apariția și dezvoltarea fenomenului criminalității informatice nu este decât consecința negativă a așa-numitei „computerizări a societății".

§ 1. Etapele evoluției

În ce privește *„evoluția"* (dacă o putem numi astfel) acestui fenomen putem distinge patru ***etape***, și anume:

- *prima* (specifică anilor '80), care a fost caracterizată de *banalizarea informaticii, piratarea programelor, falsificarea cărților de credit* etc.;

- *a doua* (specifică sfârșitului anilor '80), a fost favorizată de apariția rețelelor locale și extinse, precum și a punților de legătură, și caracterizată de importante *deturnări de fonduri și „isprăvile" hacker-ilor* care accesau calculatoarele NASA, CIA și oricare altă țintă care reprezenta un simbol politico-tehnologic sau un element al puternicului complex militaro-industrial american;

- *a treia* (specifică anilor '90), care a coincis cu proliferarea sistemelor informatice și rețelelor de comunicații (Internet-ului, în special) și a fost caracterizată de *specializarea făptuitorilor*, apariția unor „veritabili" profesioniști ai pirateriei, deturnărilor de fonduri, sabotajelor informatice;

- *a patra* (în prezent), favorizată de faptul că sistemele informatice au pătruns în toate sectoarele vieții sociale și le controlează pe cele mai importante dintre ele (transporturi, apărare, etc.), și care este caracterizată de conturarea de *noi și grave amenințări* ca *terorismul informatic*, *războiul informatic* etc.

---

[1] Ioniță G. I., *Criminalitatea informatică. Implicații sociale și juridice,* în volumul (4) A noua sesiune de comunicări științifice a cadrelor didactice din Universitatea Româno-Americană cu participare internațională, 28-29 mai 2004, Editura Universul Juridic, București, 2006, p. 197-205.

[2] A se vedea și Negroponte N., *Era digitală*, (trad.) Ed. All, București, 1999.

[3] Alecu G., Barbăneagră A., *Reglementarea ..., op. cit.*, p. 13.

§ 2. Amenințări actuale

Această dezvoltare şi specializare a activităţilor criminale, conturează (practic) patru tipuri de ameninţări[1]:

- *sistemul informatic ţintă* a infractorilor – situaţia în care atacatorii doar accesează sistemele informatice sau îşi însuşesc ilegal (conţinutul) informaţiile stocate pe acestea; exemplu: informaţiile personale, clienţii, planurile de marketing, (aproape) tot ce prezintă valoare comercială şi este stocat pe discul dur (HDD);

- *sistemul informatic instrument* al infractorilor – situaţia în care atacatorii accesează sistemele informatice fiind interesaţi de procesul prin care pot comite o altă infracţiune şi nu de informaţiile stocate pe acestea; exemplu: folosirea unei parole pentru accesarea unui cont şi transferarea respectivelor fonduri;

- *sistemul informatic facilitează* comiterea discretă a altor infracţiuni – situaţia în care atacatorii utilizează sistemele informatice pentru comiterea mai uşoară/sigură a infracţiunilor care puteau fi comise şi fără ajutorul acestora; exemplu: spălarea banilor, pedofilia, etc.;

- *sistemul informatic favorizează în mod direct* comiterea infracţiunilor – situaţia în care atacatorii se folosesc direct de sistemele informatice pentru comiterea altor infracţiuni; exemplu: piratarea programelor, contrafacerea componentelor etc.

§ 3. Principalii factori care influențează dezvoltarea criminalității informatice, provocări ale combaterii fenomenului[2]

3.1. Dependența de tehnologia informației şi comunicațiilor

Aşa cum precizam, chiar dacă nu ne place să recunoaştem, *depindem din ce în ce mai mult* de tehnologia informaţiei şi comunicaţiilor (ICT).

Astfel, comunicaţiile, transportul (aerian, feroviar, naval, etc.), furnizarea utilităţilor (energie, gaz, apă) etc., depind de această tehnologie iar integrarea continuă în viaţa de zi cu zi este posibil să dobândească valenţe noi[3].

Această dezvoltare bazată pe tehnologia informaţiei şi comunicaţiilor face sistemele şi serviciile mai vulnerabile la atacurile împotriva infrastructurilor critice.

---

[1] A se vedea şi Serge L.D. & Rosé P., *Cyber-mafia*, (trad.) Ed. Antet, Bucureşti, 1998, p. 28.

[2] Ioniță G.I., *Principalii factori care influențează dezvoltarea criminalității informatice, provocări ale combaterii fenomenului*, în Instituții juridice contemporane în contextul integrării României în Uniunea Europeană, ed. a III-a, Ed. Pro Universitaria, București, 2009, pp. 771-777.

[3] A se vedea şi alte aspecte în Bohn J., Coroamă V., Langheinrich M., Mattern F., Rohs M., *Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications*, Journal of Human and Ecological Risk Assesment, vol. 10, nr. 5, p. 736-786, (oct.) 2004, disponibil on-line la http://www.vs.inf.ethz.ch/publ/papers/hera.pdf (ultima dată accesat la 27.01.2018).

În aceste condiţii, chiar şi scurte întreruperi a serviciilor, cauzate de atacuri informatice, provoacă pagube financiare imense afacerilor/activităţilor bazate pe o astfel de tehnologie.

Peste această dependenţă se suprapune o altă vulnerabilitate a infrastructurii tehnice existente, respectiv *omogenitatea sistemelor de operare*.

Or, în contextul în care majoritatea utilizatorilor folosesc sisteme de operare dezvoltate de Microsoft, „munca" atacatorilor este mult uşurată, aceştia putând concepe atacuri eficiente prin concentrarea pe această unică ţintă.

De precizat că dependenţa societăţii de tehnologia informaţiei şi comunicaţiilor, cu problemele evidenţiate, este generalizată, nefiind specifică doar ţărilor dezvoltate, ci şi ţărilor în curs de dezvoltare.

3.2. Numărul utilizatorilor

Internet-ul şi serviciile pe care le oferă se bucură de o popularitate aflată în continuă creştere, apropiindu-se (la 30 iunie 2017) de *4 miliarde de utilizatori*[1].

Această ascensiune a popularităţii Internet-ului şi *creşterea numărului utilizatorilor*, generează o altă problemă, respectiv creşterea numărului potenţialelor ţinte şi a atacatorilor.

Cu toate că numărul utilizatorilor care folosesc Internet-ul pentru activităţi ilegale este dificil de estimat, chiar dacă ar fi de numai 0,1% din totalul utilizatorilor, s-ar apropia de 4 milioane.

Creşterea numărului utilizatorilor Internet-ului generează dificultăţi şi pentru organele de aplicare a legii, întrucât este *dificilă automatizarea proceselor de investigaţie*.

Ca exemplu: căutarea pe baza unui cuvânt cheie pentru conţinut ilegal (spre exemplu, imagini pornografice cu minori), cu toate că poate fi efectuată destul de uşor, identificarea propriu-zisă a imaginilor cu un astfel de conţinut constituie o adevărată provocare; chiar şi abordările bazate pe valoarea „Hash" au succes numai în cazul în care imaginile au fost evaluate în prealabil, valoarea „Hash" a fost stocată într-o bază de date şi imaginile care au fost analizate nu au fost modificate.

3.3. Disponibilitatea dispozitivelor şi accesului

Comiterea infracţiunilor din sfera criminalităţii informatice a devenit destul de facilă, întrucât echipamentele (hardware) şi programele (software) necesare, precum şi accesul la Internet, nu mai constituie un impediment.

---

[1] Conform Internet World Stats, *Internet Usage Statistics*, disponibil on-line la http://www.internetworldstats.com/stats.htm (ultima dată accesat la 27.01.2018).

Astfel, în ceea ce privește *echipamentele* (hardware), de remarcat faptul că puterea de procesare a acestora a crescut continuu, putându-se comite infracțiuni grave, chiar și cu echipamente ieftine sau folosite.

De asemenea, comiterea infracțiunilor din sfera criminalității informatice este mai facilă și pentru că *instrumentele specializate* (software) sunt disponibile liber, pe Internet, sunt proiectate special pentru a localiza porturi deschise, a sparge parole de protecție, etc. și, datorită tehnicilor „mirroring" și de schimb „P2P", este dificilă limitarea disponibilității și a răspândirii pe scară largă a acestora.

În ce privește *accesul la Internet*, deși costul acestuia este mai ridicat în țările în curs de dezvoltare (comparativ cu țările dezvoltate), acesta nu constituie un impediment, numărul utilizatorilor din aceste zone crescând rapid.

Oricum, de regulă, pentru a scădea probabilitatea de identificare, atacatorii nu se vor înregistra pentru a folosi un serviciu Internet, ci vor prefera serviciile ce pot fi utilizate fără înregistrare (ca terminale publice, rețele fără fir, rețele compromise și servicii pre-plătite etc.).

3.4. Disponibilitatea informațiilor

Numărul *site-urilor disponibile* pe Internet se apropie (septembrie 2017) de 2 miliarde[1].

Acum, un atacator poate găsi pe Internet, destul de ușor și rapid, *informații detaliate*, de la cum să construiască o bombă folosind substanțe și produse comercializate liber, până la planurile unei clădiri sau ale unei rețele de utilități, informații care, înainte de dezvoltarea Internet-ului, erau incomparabil mult mai dificil de obținut.

Disponibilitatea informațiilor este facilitată și de *motoarele* puternice *de căutare* dezvoltate care permit identificarea a milioane de pagini în câteva secunde și filtrarea informațiilor căutate.

3.5. Lipsa mecanismelor de control

Toate rețelele de comunicare (de la rețelele de telefonie, la Internet) au nevoie de *administrare centrală și standarde tehnice* pentru a asigura operabilitatea.

Și Internet-ul ar trebui să fie *guvernat* de anumite reguli iar organele de aplicare a legii încearcă să dezvolte standarde legale care necesită un anumit grad de control central.

---

[1] Conform Netcraft, *September 2017 Web Server Survey*, disponibil on-line la https://news.netcraft.com/archives/2017/09/11/september-2017-web-server-survey.html (ultima dată accesat la 27.01.2018).

Inițial, Internet-ul a fost conceput[1] ca o rețea militară, bazată pe o arhitectură de rețea descentralizată, care a încercat să păstreze funcționalitățile principale intacte și în operabile, chiar și atunci când componente de rețea au fost atacate, fiind rezistentă la încercările de control extern.

Cert este faptul că Internet-ul nu a fost proiectat pentru a facilita anchete penale sau pentru a preveni atacurile din interiorul rețelei.

Ca exemplu de probleme generate de lipsa unor instrumente de control este abilitatea utilizatorilor de a eluda tehnologia de filtrare, folosind servicii de comunicații anonime criptate.

3.6. Dimensiunile internaționale

Protocoalele utilizate pentru transferurile de date pe Internet se bazează pe o *dirijare optimă*, fiind posibil ca, în cazul în care resursele sunt limitate în cadrul procesului de transfer în interiorul unei țări, pachetele de date să poată părăsi țara, să se transmită prin rutere din afara teritoriului acesteia, pentru ca, ulterior, să fie redirecționate înapoi în țară, la destinația lor finală.

De asemenea, multe *servicii Internet* se bazează pe serviciile din străinătate; de exemplu, furnizorii gazdă pot oferi spațiu web de închiriat într-o țară dar pe baza echipamentelor (hardware) dintr-o altă țară.

Astfel, multe dintre *procesele de transfer* de date pot dobândi caracter transnațional.

Or, în situația în care atacatorii și țintele sunt situate în țări diferite, investigațiile necesită o *cooperare* a organelor de aplicare a legii în toate țările unde această activitate infracțională se desfășoară ori produce efecte, fiind, adesea, îngreunate[2].

Această cooperare între organele de aplicare a legii din țări diferite, necesită *timp* și, de toate aceste „întârzieri" beneficiază tocmai infractorii, care aleg deliberat ținte din afara propriei țări și acționează din țări cu legislație permisivă în ce privește criminalitatea informatică.

3.7. Independența locației și prezenței la locul infracțiunii

Accesul la Internet conferă atacatorilor un alt avantaj, de care profită din plin, respectiv acela de *a nu fi prezenți în aceeași locație cu victima* pentru a comite infracțiuni din sfera criminalității informatice.

---

[1] Pentru o scurtă istorie a Internet-ului, a se vedea Leiner B. M., Cerf V. G., Clark D. D., Kahn K. E., Kleinrock L., Lynch D. C., Postel J., Roberts L. G., Wolff S., *A Brief History of the Internet*, disponibil on-line la https://www.internetsociety.org/internet/history-internet/brief-history-internet/ (ultima dată accesat la 27.01.2018).

[2] A se vedea și Goodman S. E., Sofaer A. D., *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Press, Standford, CA, 2001, disponibil on-line la http://media.hoover.org/sites/default/files/documents/0817999825_1.pdf (ultima dată accesat la 27.01.2018).

De regulă, când comit astfel de infracțiuni, atacatorii au în vedere aspecte ca: statutul legislației criminalității informatice, eficacitatea organelor de aplicare a legii, disponibilitatea de acces anonim la Internet etc.

În acest context, una din *provocările cheie* în lupta împotriva criminalității informatice o constituie prevenirea *„paradisurilor" informatice*.

Atâta timp cât aceste paradisuri există, atacatorii le vor utiliza pentru a împiedica/îngreuna desfășurarea investigațiilor autorităților de aplicare a legii; ca exemplu, Nigeria, ce a trebuit să ia măsuri împotriva înșelătoriilor financiare distribuite prin poșta electronică („celebra" scrisoare nigeriană).

3.8. Automatizarea

Unul dintre cele mai mari *avantaje* ale tehnologiei informației și comunicațiilor, respectiv posibilitatea de *automatizare a unor procese*, generează multe consecințe majore, ca: mărirea vitezei proceselor, creșterea amplorii și impactului proceselor, limitarea implicării oamenilor etc.

Acest avantaj este folosit, din plin, și de către atacatori.

Astfel, spammer-ii folosesc instrumente (software) specializate, pe care cheltuiesc mii de dolari, care va gestiona milioane de mesaje nesolicitate (tip spam), va scana automat Internet-ul pentru a găsi servere, de tip proxy, prin intermediul cărora să transmită (și să mascheze) aceste mesaje[1].

De asemenea, și hacker-ii folosesc astfel de instrumente (software) specializate, pentru a lansa automat atacuri, zilnic fiind raportate aproape o jumătate de milion de astfel de incidente[2].

Astfel, prin automatizarea proceselor, atacatorii pot plănui escrocherii care presupun un *număr mare de atacuri* și *pierderi relativ scăzute* pentru fiecare victimă.

Acționând de o asemenea manieră, atacatorii pot obține un *profit crescut* cu *riscuri mult mai reduse*, întrucât, cu cât este mai mică fiecare pierdere, cu atât este mai mare șansa ca victima să nu raporteze atacul.

3.9. Resursele

Alături de creșterea puterii de procesare a sistemelor informatice folosite de un singur utilizator și creșterea capacităților rețelei poate ridica probleme majore;

---

[1] A se vedea și Berg T., *The Changing Face of Cybercrime: New Internet Threats Create Challenge to Law Enforcement*, în Computer Law, Michigan Bar Journal, (iun) 2007, p. 21, disponibil on-line la https://www.michbar.org/file/barjournal/article/documents/pdf4article1163.pdf (ultima dată accesat la 27.01.2018).

[2] A se vedea Hacker Watch - Anti-Hacker Community, *Event Tracking*, disponibil on-line la http://www.hackerwatch.org (ultima dată accesat la 27.01.2018).

un exemplu în acest sens îl reprezintă *rețelele (ro)bot*, respectiv acele rețele formate din sisteme informatice compromise („zombi") care rulează programe sub controlul extern al altui sistem informatic („master").

Rețelele (ro)bot au devenit, în ultimii ani, un *risc serios pentru securitatea informatică*, permițând atacatorilor, ca, prin utilizarea a mii de sisteme informatice compromise („zombi") într-o astfel de rețea, să poată lansa atacuri de tip „refuzul serviciului" (DoS), „hacking", trimiterea de mesaje nesolicitate „spam" etc., asupra unor sisteme informatice pe care, altfel, nu le-ar fi putut atinge.

În același timp, aceste rețele fac *mult mai dificilă urmărirea originii atacului*, urmele inițiale conducând doar la sistemul informatic compromis („zombi") prin care a fost lansat atacul, nu la sistemul informatic („master") care l-a controlat.

Pe de altă parte, și *discrepanța dintre resursele folosite* de atacatori și cele folosite de organele de aplicare a legii devine tot mai accentuată, primii (atacatorii) controlând sisteme informatice și rețele tot mai puternice, comparativ cu ultimii (organele de aplicare a legii), care, sunt limitați de fondurile alocate.

3.10. Viteza proceselor de schimb de date

O altă *facilitate* a tehnologiei, care *poate genera probleme*, este reprezentată de viteza cu care se realizează schimbul de date; ca exemplu, transmiterea unui simplu mesaj de poștă electronică (oriunde în lume) durează doar câteva secunde.

Aceste *transferuri rapide* de date, creează dificultăți organelor de aplicare a legii în desfășurarea activităților specifice.

Este cunoscut faptul că, pentru instrumentarea în condiții optime a oricărei cauze, dar mai cu seamă a celor din sfera criminalității informatice, un factor vital este reprezentat de timpul de răspuns, care trebuie să fie cât mai scurt.

În aceste condiții, o *luptă eficientă* împotriva criminalității informatice este condiționată de adoptarea unei legislații corespunzătoare și de folosirea unor instrumente care să permită organelor de aplicare a legii să reacționeze prompt pentru a preveni ștergerea urmelor și a putea identifica atacatorul și documenta activitatea infracțională desfășurată.

3.11. Viteza de dezvoltare

Dezvoltarea explozivă a Internetului a fost facilitată și de dezvoltarea unei *interfețe de utilizator grafice* „prietenoasă" și ușor accesibilă.

În același context, au fost *dezvoltate aplicații* (software) dar și *dispozitive* (hardware) cu tehnologie de rețea; ca exemplu, televizoarele cu acces la Internet.

De asemenea, *dispozitivele mobile* de comunicații au reușit să proceseze și să stocheze date și să se poată conecta la Internet, *dispozitivele de stocare* cu

capacitate mare, camerele, microfoanele etc. au putut fi integrate în alte dispozitive comune, de dimensiuni reduse (ceasuri, pixuri etc.).

Astfel, organele de aplicare a legii trebuie, permanent, să țină „pasul" cu aceste evoluții; *pregătirea continuă* a celor implicați în cercetarea infracțiunilor din sfera criminalității informatice este esențială, pentru a putea fi la curent cu cele mai noi tehnologii și să poată identifica echipamentele și alte dispozitive care pot conține date și informații relevante pentru cauză.

3.12. Comunicațiile anonime

Și anonimatul, respectiv abilitatea de a putea ascunde identitatea cuiva în timp ce comunică, a contribuit la creșterea popularității Internetului.

Din nefericire și această capacitate a Internetului poate fi folosită, atât în mod *legitim*, de către cei care, din diferite motive, nu doresc să-și dezvăluie identitatea reală[1], cât și *ilegitim*, de către cei care își ascund identitatea reală pentru a putea comite atacuri.

Prin folosirea unor servicii de comunicații anonime – ca terminale publice de Internet (în aeroporturi, gări, cafenele), rețele fără fir, servicii de telefonie mobilă pre-plătite, capacități de stocare oferite de pagini web fără înregistrare, sisteme informatice tip server de comunicații anonime etc. –, atacatorii își pot spori șansele de *a nu putea fi descoperiți*.

Pentru *disimularea identității*, atacatorii pot să recurgă și la înregistrarea unor adrese de poștă electronică fără a-și dezvălui identitatea reală, mulți furnizori oferind, în mod gratuit, astfel de servicii, fără a avea posibilitatea să verifice informațiile personale declarate.

Cu toate că unele țări au încercat *abordarea provocărilor* comunicațiilor anonime, prin punerea în aplicare a unor *restricții*, măsurile pot fi ușor *evitate* prin utilizarea rețelelor private fără fir neprotejate sau a card-urilor achiziționate din țări în care înregistrarea nu este obligatorie.

3.13. Tehnologia de criptare

Tehnologia de criptare reprezintă un alt factor care poate complica investigarea infracțiunilor din sfera criminalității informatice.

Criptarea datelor este destul de *facilă*, fiind disponibile utilitare (software) care permit protejarea fișierelor/comunicațiilor împotriva accesului/interceptării neautorizat/neautorizate.

---

[1] A se vedea și Sobel D. L., *The Process that „John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity*, în Virginia Journal of Law and Technology, 3, 2000, disponibil on-line la http://vjolt.org/wp-content/uploads/2017/Articles/vol5/symposium/v5i1a3-Sobel.html (ultima dată accesat la 28.01.2018).

De asemenea, *criptarea mesajelor* poate fi realizată și prin folosirea unor utilitare (software) de steganografie, fiind dificil să se distingă între schimbul inofensiv de fotografii și schimbul de imagini cu mesaje criptate ascunse.

Decifrarea criptării este posibilă, dar (de multe ori) este un proces dificil și anevoios, ce poate fi realizat dacă organele de aplicare a legii au acces la utilitarul (software-ul) folosit pentru a cripta fișierele.

În acest context, probabilitatea ca organele de aplicare a legii să decifreze criptarea și să acceseze datele, este mult îngreunată.

Capitolul III

Explicații criminologice ale subculturilor criminalității informatice

Secțiunea I
Considerații generale

Ca punct de plecare în studiul criminologic al subculturilor criminalității informatice, poate fi considerată ***Teoria lui Merton*** deoarece, *aplicând această teorie la subculturile criminalității informatice de astăzi*, poate fi utilă în înțelegerea fenomenului (criminalității informatice)[1].

Înainte de prezentarea Teoriei lui Merton, este *necesară prezentarea succintă a* ***Teoriei lui Durkheim*** – „unul dintre cei mai cunoscuți și mai puțin înțeleși mari sociologi"[2] – deoarece *Merton a actualizat Teoria lui Durkheim pentru a explica dezrădăcinările și dislocarea socială cauzate de Marea Recesiune Economică, care i-a lăsat pe mulți indivizi fără mijloacele de a îndeplini țelurile americane*.

Secțiunea a II-a
O scurtă prezentare a Teoriei lui Emile Durkheim

Emile Durkheim *consideră criminalitatea ca fiind atât normală, cât și funcțională și că aceasta nu poate lipsi complet din nicio societate*[3]; afirmă că „nu există nici un fenomen care să prezinte într-un mod indiscutabil toate simptomele normalității, din moment ce apare conectat îndeaproape cu condițiile vieții cotidiene"[4].

Durkheim apreciază că întrucât nu poate exista o societate în care indivizii să nu se abată, mai mult sau mai puțin, de la tipul colectiv, este inevitabil ca unele dintre aceste abateri să prezinte caracter infracțional[5].

---

[1] Ioniță G. I., *Explicații criminologice ale criminalității informatice,* în volumul (4) A XII-a sesiune de comunicări științifice a cadrelor didactice, 25-26 mai 2007, Editura Pro Universitaria, București, 2007, p. 138-147.

[2] La Capra D., *E. Durkheim, Sociologist and Philosopher*, Cornell University Press, New York, 1972, p. 5.

[3] Sandu F., Ioniță G. I., *Criminologie…, op. cit.*, p. 71

[4] Durkheim E., *The Rules of Sociological Method*, Free Press, New York, 1964, p. 66.

[5] Durkheim E., *Regulile metodei sociologice*, (traducere) Ed. Științifică, București, 1974, p. 116.

În viziunea lui, infracțiunea este „legată de condițiile fundamentale ale vieții sociale și datorită acestui fapt este folositoare, deoarece aceste condiții din care face parte, sunt indispensabile (ele însele) pentru normala evoluție a moralității și legii”[1].

Abordarea lui Durkheim vizează structura societății și instituțiile sale, precum și procesul prin care ia naștere infracțiunea și cum este aceasta legată de funcționarea unei societăți[2].

El susține că *unul dintre cele mai importante elemente ale societății este coeziunea (solidaritatea) ei socială* (care reprezintă o conștiință colectivă) și, explicând acest fenomen, *definește două tipuri de societăți*: ***mecanică*** (caracteristică societăților primitive), *dominată de conștiința colectivă și* ***organică*** (caracteristică societăților mai mari, mai complexe) în care *accentul legii se schimbă, de la conștiința colectivă la greșeala individului, legea devenind restitutivă.*

Durkheim a introdus versiunea sa conceptului de **anomie,** considerând-o ca fiind ***o stare obiectivă a mediului social caracterizată printr-o dereglare a normelor sociale datorită fie unor schimbări benefice, dar bruște, dar mai ales dezastrelor (naturale, economice, războaie etc.), societatea fiind incapabilă, momentan, să regleze, să modereze tendințele crescânde ale individului pentru satisfacerea unor idealuri de confort material și prestigiu social***.

El susține că *izolarea socială și pierderea identității este însoțită de o inevitabilă stare de anomie*, care înlocuiește fosta stare de solidaritate și conduce la o atmosferă în care infracțiunea și celelalte fapte antisociale se pot dezvolta și prospera[3].

Secțiunea a III-a
O scurtă prezentare a Teoriei lui Robert Merton

Robert Merton, cu toate că preia conceptul de anomie de la Durkheim, dezvoltă o paradigmă, examinând mai concret consecințele negative ale anomiei.

Merton pune următoarea *întrebare: „de ce frecvența comportamentelor deviante variază între diferitele structuri sociale și cum se întâmplă că devianțele au diferite forme și tipare în structuri sociale diferite*?”[4].

Față de Durkheim, Merton susține că ***adevărata problemă nu este creată de schimbarea socială bruscă ci de o structură socială care oferă aceleași idealuri tuturor membrilor săi fără însă a le oferi și mijloace egale pentru a***

[1] Durkheim E., *The Rules…, op. cit.*, p. 70.

[2] Adler F., Mueller G. O. W., Laufer W. S., *Criminology, 2nd ed.*, McGraw-Hill, New York, 1995, p. 69.

[3] Durkheim E., *The Division of Labour in Society*, Free Press, New York, 1964, p. 374-388.

[4] Merton R. K., *Social Theory and Social Structure*, Free Press, New York 1968, p. 185.

le atinge, şi că tocmai aceasta lipsă de integrare între ceea ce cultura defineşte şi ceea ce structura permite (mai întâi încurajând succesul, apoi prevenindu-l) poate provoca prăbuşirea normelor care (normele) nu mai sunt ghizi eficienţi ai comportamentului[1].

Merton a împrumutat termenul de „anomie" pentru a descrie această cădere a sistemului normativ, apreciind că „numai atunci când un sistem de valori culturale laudă, mai presus de toate, anumite simboluri comune ale succesului pentru populaţie, în timp ce structura sa, în mod riguros, limitează sau elimină accesul la modalităţile acceptate de dobândire a acestor simboluri pentru o parte semnificativă din aceeaşi populaţie, astfel comportamentul, antisocial se asigură pe o scală considerabilă"[2].

Teoria sa *accentuează importanţa* (în orice societate) a două elemente, respectiv:

- *scopurile, aspiraţiile culturale sau idealurile* pentru care oamenii cred că merită să te lupţi;

- *mijloacele instituţionalizate sau căile acceptate* pentru atingerea respectivelor idealuri.

El susţine că într-o societate stabilă aceste elemente trebuie să fie bine integrate şi că discrepanţa dintre idealuri şi mijloace determină frustrare, care duce la stres.

Merton a identificat şi explicat 5 modalităţi în care oamenii se adaptează idealurilor societăţii şi mijloacelor de obţinere, apreciind că răspunsurile indivizilor (modurile de adaptare) depind de atitudinea lor faţă de acestea (idealurile societăţii şi mijloacele instituţionalizate de atingere a acestora).

Tipologia modurilor individuale de adaptare, în viziunea lui Merton este următoarea[3]:

(1) *conformarea*, care presupune *acceptarea atât scopurilor, cât şi a mijloacelor*, şi care ar fi cel mai obişnuit mod de adaptare; el susţine că cei ce se adaptează prin conformare luptă pentru obţinerea bunăstării prin metodele aprobate de către societate şi vor continua acest lucru indiferent dacă vor reuşi ori nu;

(2) *inovarea*, care presupune *acceptarea scopurilor, dar respingerea mijloacelor*; el remarcă faptul că în momentul în care anumite persoane consideră că nu pot atinge bunăstarea prin mijloace legale scot la iveală noi metode pentru care pot atinge scopurile (metode nelegale) şi astfel „o virtute americană de bază (ambiţia) promovează un viciu american de bază (comportament deviant)"[4];

---

[1] Sandu F., Ioniţă G. I., *Criminologie…, op. cit.*, p. 88

[2] Merton R. K., *Social Structure and Anomie*, American Sociological Review, 3, 1938, p. 672-682.

[3] Sandu F., Ioniţă G. I.,*Criminologie…, op. cit.*, p. 89-90.

[4] Merton R. K., *Social Theory…, op. cit.*, p. 201.

(3) *ritualismul*, care presupune *respingerea scopurilor, dar acceptarea mijloacelor*; el apreciază că cei ce se adaptează prin ritualism abandonează idealurile despre care au crezut la un moment dat că sunt de neatins şi s-au resemnat modului lor de viaţă, şi că este adaptarea celor care vor să „meargă la sigur" deoarece au obţinut un nivel minim de succes prin mijloace legale şi sunt blocaţi de teama de a nu pierde chiar şi acest nivel minimal: „nu ridica capul mai sus, nu ţinti mai departe" etc.;

(4) *retragerea*, care presupune *respingerea atât a scopurilor cât şi a mijloacelor* (cea mai puţin comună dintre cele 5 moduri de adaptare), şi care ar aparţine tipului de persoană care este cu adevărat străină de societate; Merton sugerează că „retragerea" apare după ce o persoană a acceptat atât scopurile cât şi mijloacele dar a eşuat în mod repetat să-şi atingă scopurile prin mijloace legitime; în acelaşi timp, din cauza socializării anterioare, individul nu este capabil să adopte mijloace legitime; „ieşirea este completă, conflictul este eliminat şi individul este total asocializat"[1];

(5) *rebeliunea*, care presupune *respingerea scopurilor şi mijloacelor şi încercarea de a stabili o nouă ordine*; Merton sugerează că această adaptare este în mod clar diferită de celelalte şi reprezintă mai degrabă o încercare de a schimba structura socială, o încercare de a instituţionaliza noi scopuri şi mijloace pentru restul societăţii.

Merton susţine că aceste adaptări nu descriu tipuri de personalitate, ci o alegere individuală a comportamentelor ca răspuns la stresul anomiei şi că indivizii pot alege un anumit mod de adaptare sau pot folosi adaptări simultane[2].

Secţiunea a IV-a
Explicarea subculturilor criminalităţii informatice prin prisma tipologiei modurilor individuale de adaptare dezvoltată de Merton

Teoria lui Merton (mai sus prezentată) ***nu poate explica apariţia hacker-ilor***, care sunt produsul anomiei de afluenţă, şi care au ample mijloace de a atinge ţelurile succesului american dar, în schimb, ***poate explica involuţia acestora***.

Internet-ul, în acelaşi mod ca revoluţia industrială, a transformat fiecare aspect din viaţa noastră socială, inclusiv subculturile delincvente.

Istoria hacker-ilor[3] poate constitui un punct de plecare în analiza motivaţiei comiterii infracţiunilor din sfera criminalităţii informatice.

---

[1] *Ibidem*, p. 208.

[2] Merton R. K., *Social Theory…, op. cit.*, p. 201.

[3] A se vedea şi Wikipedia, *Timeline of computer security hacker history,* disponibil on-line la https://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history (ultima dată accesat la 29.01.2018).

Se consideră că hacking-ul este un produs de conflict şi contestaţie între grupuri sociale diverse[1], iar cercetările efectuate au confirmat spiritul etic al unora dintre aceştia, în sensul că aveau ca motivaţie primară dorinţa de a înţelege sistemele informatice, securitatea şi reţelele şi nu dorinţa de a comite infracţiuni.

Astfel, s-a concluzionat[2] în sensul că hacker-ii reprezintă un grup difuz, care doresc să înveţe şi să exploreze, mai degrabă să ajute decât să provoace daune, şi care au, adesea, standarde foarte ridicate.

În acest sens, prima generaţie de hacker-i a fost formată din tineri aparţinând celor mai influente şi educate segmente ale societăţii americane: studenţi, programatori, administratori de reţele şi antreprenori (ca Bill Gates).

Din nefericire, cultura hacking-ului etic a involuat, treptat, în subculturi care se diferenţiază şi devin tot mai complexe – cu valori culturale, norme şi practici proprii –, respectiv[3]:

- hacker-i „cu pălărie albă" („white hat" hackers), consideraţi hacker-i „buni", „oneşti", „etici", care ajung să fie implicaţi în îmbunătăţirea securităţii sistemelor informatice şi reţelelor şi chiar în combaterea fraudei informatice, fiind chiar şi angajaţi în acest scop;

- hacker-i „cu pălărie neagră" („black hat" hackers), consideraţi „infractori", „băieţi răi", „cracker-i", care compromit sisteme informatice doar pentru amuzament ori, adesea, pentru comiterea de infracţiuni ce au ca bază o motivaţie financiară;

- hacker-i „cu pălărie cenuşie" („grey hat" hackers), care compromit sisteme informatice vulnerabile, îl înştiinţează pe deţinător şi se oferă să „repare" stricăciunile în schimbul unei sume;

- hacker-i „cu pălărie albastră" („blue hat" hackers), experţi care sunt angajaţi să testeze vulnerabilităţile sistemelor/programelor înainte de lansare, în scopul identificării şi îmbunătăţirii securităţii acestora;

- „hack-tivişti" (hacktivists), care se infiltrează în sisteme informatice pentru a-şi promova ideile.

§ 1. Conformismul navigatorilor pe Internet

Conformarea, aşa cum precizam, presupune *acceptarea atât a scopurilor, cât şi a mijloacelor*.

---

[1] Taylor P. A., *Hackers: Crime in the Digital Sublime*, Routledge, New York, 1999, p. 15.

[2] Denning Dorothy. E., *Concerning Hackers Who Break into Computer Systems*, 13th National Computer Security Conference, Washington, D.C., (oct.), 1990, p. 653-664, disponibil on-line la http://faculty.nps.edu/dedennin/publications/ConcerningHackers-NCSC.txt (ultima dată accesat la 29.01.2018).

[3] A se vedea şi Stănescu Mihaela, *Hackerii – cine sunt, ce fac?*, disponibil on-line la http://www.descopera.ro/capcanele-internetului/9591007-hackerii-cine-sunt-ce-fac (ultima dată accesat la 30.01.2018).

Acest tip de adaptare este *specific majorității utilizatorilor* de Internet, pentru că *îl folosesc în scopuri legitime*: informare, comunicare, educație, comerț etc.

Se poate considera că primii hacker-i au utilizat intruziunile într-o modalitate „benefică" din punct de vedere social, respectiv ca o practică prin care să înțeleagă cum funcționează sistemul; la începutul anilor '60-'70, hacking-ul era pentru mulți studenți echivalentul funcțional al unui studiu avansat privind calculatorul.

§ 2. Inovația: hacking-ul pentru profit

Inovarea, așa cum precizam, presupune *acceptarea scopurilor, dar respingerea mijloacelor*.

Acest tip de adaptare este *specific celor care utilizează Internet-ul ca pe un instrument de câștig ilegal*.

A. *Inovația ca furt electronic.* S-a observat că, predominant, motivația primară a inovatorilor este câștigul și nu curiozitatea; astfel, site-urile sunt accesate pentru a sustrage informații confidențiale iar tururile pretins gratuite ale site-urilor pornografice sunt „oferite" pentru a face încasări neautorizate de pe card-urile vizitatorilor.

B. *Inovația ca spionaj comercial.* S-a susținut că spionajul comercial are ca țintă vulnerabilități cunoscute în sistem; astfel, vulnerabilitățile sunt exploatate pentru a desfășura acțiuni neautorizate în rețelele companiilor.

C. *Inovația ca „dușmanul din interior".* S-a constatat că una dintre cele mai mari amenințări la adresa siguranței sistemelor informatice este reprezentată nu de hacker-i, ci de dușmanii din interior – angajați de încredere, foști angajați, consultanți și alte persoane familiare cu rețeaua –; astfel, cunoștințele sunt „valorificate" pentru a sustrage bani sau alte informații confidențiale.

Teama companiilor de a-și pierde secretele și informațiile prețioase pe care le acestea le dețin, a fost valorificată de IBM pentru a impulsiona vânzarea unor produse de securitate și consultanță.

Într-o reclamă erau prezentați douăzeci de hacker-i care se infiltraseră într-o rețea ce conținea informații confidențiale privind primele unor directori; în acest context, o tânără din acel grup rămâne surprinsă de diferența semnificativă dintre câștigurile obținute de unul dintre vicepreședinți, comparativ cu ceilalți și apreciază că ceilalți vicepreședinți ar fi surprinși să afle cât câștigă acesta; un tânăr din acel grup o liniștește spunându-i: „Ei știu deja. Tocmai am trimis un e-mail tuturor din companie"[1].

[1] Rustad M., Daftary C., *E-Business Legal Handbook*, Aspen Law & Business Publishers, New York, 2001, p. 152.

§ 3. Ritualismul: hacking-ul ca obişnuinţă

Ritualismul, aşa cum precizam, presupune *respingerea scopurilor, dar acceptarea mijloacelor*.

Acest tip de adaptare este *specific profesioniştilor calculatoarelor*, absorbiţi în munca lor şi cu independenţă scăzută; s-a observat că aceştia au fost la un pas de a atinge ţelul american de succes, lucrează pentru un salariu mic şi nu au perspectiva unui succes financiar pe termen lung.

§ 4. Retragerea: hacking-ul ca dependenţă

Retragerea, aşa cum precizam, presupune *respingerea atât a scopurilor, cât şi a mijloacelor*.

Acest tip de adaptare este *specific celor care „bat în retragere"*; s-a constatat că aceştia sunt motivaţi, mai degrabă, de emoţia căutării decât de câştigul economic, calculatoarele şi Internet-ul reprezentând (pentru ei) o formă de dependenţă.

Astfel, în Manifestul hackerului[1], este utilizat limbajul unui *dependent*, pentru a *descrie relaţia sa cu sistemele informatice*: „... Astăzi am făcut o descoperire. Am găsit un calculator. Stai puţin, acesta este grozav ... Şi apoi s-a întâmplat ... s-a deschis o uşă către o lume ... grăbindu-se prin linia telefonică, la fel ca heroina prin venele unui dependent, un puls electronic este trimis, un refugiu de la incompetenţele de zi cu zi, îmi apare ... este găsită o graniţă ... acesta este locul de care aparţin ... Îi cunosc pe toţi aici ... Da, sunt un infractor. Infracţiunea mea este aceea a curiozităţii ... Sunt un hacker, iar acesta este manifestul meu. Poţi opri acest individ dar nu poţi să ne opreşti pe toţi ... la urma urmei, suntem toţi la fel".

§ 5. Rebeliunea: hacking-ul ca nesupunere la regulile societăţii

Rebeliunea, aşa cum precizam, presupune *respingerea scopurilor şi mijloacelor şi încercarea de a stabili o nouă ordine*.

Acest tip de adaptare este *specific celor care utilizează sistemele informatice şi reţelele de calculatoare de o manieră subversivă, pentru a promova o agendă politică sau o schimbare socială* („hack-tivism"); cu rădăcini în cultura şi etica hacker-ilor, scopurile hack-tivismului sunt adesea legate de libera exprimare, drepturile omului sau libera circulaţie a informaţiilor[2].

---

[1] The Mentor, *The Conscience of a Hacker*, disponibil on-line la http://archive.org/stream/The_Conscience_of_a_Hacker/hackersmanifesto.txt (ultima dată accesat la 30.01.2018).

[2] Wikipedia, *Hacktivism*, disponibil on-line la https://en.wikipedia.org/wiki/Hacktivism (ultima dată accesat la 30.01.2018).

La nivel oficial, politica hack-tiviştilor este privită ca un raţionament care le serveşte propriilor scopuri.

§ 6. Hackingul non-utilitar

Tipologia dezvoltată de Merton *nu explică* un fenomen destul de răspândit, respectiv desfăşurarea unor activităţi infracţionale cu o *motivaţie aparent lipsită de utilitate*, cum ar fi: demonstrarea abilităţilor informatice, pedepse sau represalii, voyeurism informatic etc.

Partea a II-a

PREOCUPĂRI ALE SOCIETĂȚII INTERNAȚIONALE PENTRU PREVENIREA ŞI COMBATEREA CRIMINALITĂȚII INFORMATICE

Capitolul I

Organizații internaționale şi regionale cu atribuții şi preocupări în prevenirea şi combaterea criminalității informatice şi principalele realizări

Secțiunea I
Considerații generale

La nivel internațional sunt organizații care se preocupă constant de analiza celor mai recente manifestări şi evoluții a criminalității informatice, creând grupuri de lucru pentru dezvoltarea strategiilor de prevenire şi combatere a infracțiunilor din sfera de manifestare a acesteia.

În plus față de aceste organizații internaționale, care acționează la nivel global, mai multe organizații se concentrează pe anumite regiuni, avansând în activități care tratează probleme legate de criminalitatea informatică.

Secțiunea a II-a
Organizația Națiunilor Unite (UN)

Organizația Națiunilor Unite (UN)[1] a fost înființată la 24 octombrie 1945, când reprezentanții unui număr de 50 de țări au semnat Carta ONU (inițial, Polonia, nu a fost reprezentată la conferință, semnând ulterior şi devenind al 51-lea membru)[2]; în prezent, aproape toate națiunile lumii sunt membre ONU, 193 de țări în total[3].

În anul *1990*, la ***Congresul al 8-lea privind prevenirea infracțiunilor şi tratamentul infractorilor*** (care a avut loc la Havana, Cuba, 27 august - 7 septembrie 1990), Adunarea Generală a adoptat o rezoluție referitoare la legislația criminalității informatice, ***Rezoluția nr. 45/121/14.12.1990***[4], în baza căreia ONU

---

[1] United Nations (UN), la http://www.un.org.

[2] *Idem*, *History of the United Nations*, disponibil on-line la http://www.un.org/en/sections/history/history-united-nations/index.html (ultima dată accesat la 22.01.2018).

[3] *Idem*, *Overview*, disponibil on-line la http://www.un.org/en/sections/about-un/overview/index.html (ultima dată accesat la 22.01.2018).

[4] United Nations, General Assembly, A/RES/45/121, disponibil on-line la http://www.un.org/documents/ga/res/45/a45r121.htm.

a publicat în 1994 un Manual privind prevenirea şi controlul infracţiunilor în legătură cu calculatorul[1].

În anul *2000*, Adunarea Generală a adoptat o rezoluţie referitoare la combaterea prin mijloace penale a abuzurilor privind tehnologiile informaţionale, ***Rezoluţia nr. 55/63/04.12.2000***[2], în care a identificat o serie de măsuri menite să împiedice utilizarea improprie a tehnologiei informaţiei.

În anul *2001*, Adunarea Generală a adoptat o altă rezoluţie referitoare la combaterea prin mijloace penale a abuzurilor privind tehnologiile informaţionale, ***Rezoluţia nr. 56/121/19.12.2001***[3], care face referire la abordările internaţionale existente, în lupta împotriva criminalităţii informatice şi subliniază diferite soluţii:

„Luând notă de activitatea organizaţiilor internaţionale şi regionale în combaterea criminalităţii de înaltă tehnologie, inclusiv aceea a Consiliului Europei în elaborarea Convenţiei privind criminalitatea informatică, precum şi aceea a acelor organizaţii în promovarea dialogului între guvern şi sectorul privat, pentru siguranţă şi încredere în spaţiul virtual.

1. Invită statele membre ca, în dezvoltarea legislaţiei naţionale, a politicilor şi practicilor de combatere prin mijloace penale a abuzurilor privind tehnologiile informaţionale, să ia în considerare, după caz, activitatea şi realizările Comisiei pentru Prevenirea Criminalităţii şi Justiţia Penală, precum şi a altor organizaţii internaţionale şi regionale;

2. Ia notă cu privire la măsurile de valoare prevăzute în Rezoluţia 55/63 şi invită, din nou, statele membre să le ia în considerare în eforturile lor de combatere prin mijloace penale a abuzurilor privind tehnologiile informaţionale;

3. Decide să amâne luarea în considerare a acestui subiect, aşteptând rezultatele activităţilor prevăzute în planul de acţiune împotriva criminalităţii în legătură cu calculatoarele şi de înaltă tehnologie, al Comisiei pentru Prevenirea Criminalităţii şi Justiţia Penală".

În anul *2005*, ***la cel de-al 11-lea Congres ONU cu privire la prevenirea criminalităţii şi justiţia penală***, în Bangkok, Thailanda, a fost adoptată o declaraţie[4] „***Sinergii şi răspunsuri: Alianţe strategice în prevenirea criminalităţii***

---

[1] United Nations Office at Vienna. Centre for Social development and Humainitarian Affair, *United Nations Manual on the prevention and control of computer-related crime*, în International Review of Criminal Policy, nr. 43 şi 44 (septembrie), 1994, disponibil on-line la http://www.org/Documents/irpc4344.pdf.

[2] United Nations, General Assembly, A/RES/55/63, disponibil on-line la http://www. unodc.org/pdf/crime/a_res_55/res5563e.pdf.

[3] United Nations, General Assembly, A/RES/56/121, disponibil on-line la http:// daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf?OpenElement.

[4] UN, *Bangkok Declaration, Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice*, disponibil on-line la: http://www.unodc.org/pdf/crime/congress11/Bangkok Declaration.pdf.

și justiția penală", care a subliniat nevoia de armonizare în lupta împotriva criminalității informatice:

„... 14. Reafirmăm importanța fundamentală a punerii în aplicare a instrumentelor existente, precum și dezvoltarea în continuare a măsurilor naționale și cooperarea internațională în materie penală, cum ar fi luarea în considerare a consolidării și a sporirii măsurilor, în special împotriva criminalității informatice, a spălării banilor și a traficului de proprietate culturală, precum și cu privire la extrădare, prin asistență juridică reciprocă și confiscarea, recuperarea și returnarea produselor infracțiunii.

15. Am luat act de faptul că, în actuala perioadă de globalizare, tehnologia informației și dezvoltarea rapidă a unor noi rețele de telecomunicații și de calculatoare, au fost însoțite de abuzul acestor tehnologii pentru scopuri criminale. Prin urmare, sunt bine venite eforturile de consolidare și suplimentare a cooperării existente pentru a preveni, investiga și incrimina criminalitatea în legătură cu calculatoarele și de înaltă tehnologie, inclusiv prin dezvoltarea de parteneriate cu sectorul privat. Recunoaștem contribuția importantă a Organizației Națiunilor Unite în plan regional și alte forumuri internaționale în lupta împotriva criminalității informatice și invităm Comisia pentru Prevenirea Criminalității și Justiție Penală, ținând cont de experiența sa, de a examina posibilitatea de a oferi asistență suplimentară în acest domeniu, sub egida Organizației Națiunilor Unite, în parteneriat cu alte organizații similare concentrate pe aceleași probleme ...".

În anul *2010*, ***la cel de-al 12-lea Congres ONU cu privire la prevenirea criminalității și justiția penală***, în Salvador, Brazilia, a fost adoptată o declarație[1] „***Strategii cuprinzătoare pentru provocări globale: Prevenirea criminalității și sistemul justiției penale și dezvoltarea lor într-o lume în schimbare***", care a subliniat:

„... 41. ... Biroul Organizației Națiunilor Unite pentru Droguri și Criminalitate, în cooperare cu Statele Membre, organizațiile internaționale relevante și sectorul privat, asigură, la cerere, asistență și formare profesională Statelor pentru îmbunătățirea legislației naționale și construirea capacității autorităților naționale, în scopul de a face față criminalității informatice, inclusiv prevenirea, detectarea, investigarea și incriminarea unor astfel de infracțiuni în toate formele, și de a spori securitatea rețelelor de calculatoare.

42. ... Comisia pentru Prevenirea Criminalității și Justiție Penală să ia în considerare convocarea unui grup interguvernamental deschis de experți pentru a efectua un studiu cuprinzător al problemei criminalității informatice și să răspundă

[1] UN, *Salvador Declaration on Comprenhensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World*, disponibil online la: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_ Declaration/Salvador_Declaration_E.pdf.

la ea Statelor Membre, comunității internaționale și sectorului privat, incluzând schimbul de informații cu privire la legislația națională, cele mai bune practici, asistență tehnică și cooperare internațională, cu scopul de a examina opțiuni pentru a consolida reglementările naționale și internaționale sau alte răspunsuri ori să propună altele noi".

În anul *2015*, ***la cel de-al 13-lea Congres ONU cu privire la prevenirea criminalității și justiția penală***, în Doha, Qatar, a fost adoptată „***Declarația de la Doha privind integrarea prevenirii criminalității și a justiției penale în Agenda mai largă a ONU pentru a aborda provocările sociale și economice și promovarea supremației legii la nivel național și internațional și participarea publicului***"[1], care a precizat eforturile care vor fi depuse pentru a răspunde în mod adecvat amenințărilor generate de formele noi și emergente de criminalitate, respectiv[2]:

- să analizeze măsurile specifice destinate să creeze un cyber-mediu sigur și rezilient;
- să prevină și să combată activitățile criminale desfășurate pe Internet (acordând o atenție deosebită furtului de identitate, recrutării în scopul traficului de persoane și protejării copiilor împotriva exploatării și abuzului on-line);
- să consolideze cooperarea în domeniul aplicării legii la nivel național și internațional (inclusiv cu scopul de a identifica și proteja victimele), printre altele, prin eliminarea de pe Internet a pornografiei infantile, în special imaginile privind abuzurile sexuale asupra copiilor);
- să sporească securitatea rețelelor de calculatoare și să protejeze integritatea infrastructurii relevante;
- să depună eforturi pentru a furniza asistență tehnică și consolidare a capacităților pe termen lung pentru a întări abilitatea autorităților naționale de a combate criminalitatea informatică, inclusiv prevenirea, depistarea, investigarea și urmărirea penală a acestor infracțiuni în toate formele lor.

Secțiunea a III-a
Grupul celor Șapte Națiuni (G7)

Grupul celor Șapte Națiuni (G7) se referă la un grup de șapte națiuni puternic industrializate, respectiv Franța, Germania, Italia, Marea Britanie, Japonia,

[1] UNODC, *Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation*, disponibil on-line la: http://www.unodc.org/documents/congress//Declaration/V1504151_English.pdf (ultima dată accesat la 22.01.2018).

[2] *Ibidem*, pct. 9 lit. b), p. 10.

Statele Unite și Canada care se întrunesc (din 1976, în această formulă), anual, la Summit-ul G7.

Din acest grup a făcut parte și Rusia, (oficial) din 1997 până în 2014 (când a anexat Crimeea), grupul numindu-se Grupul celor Opt Națiuni (G8).

În anul *1997*, cu ocazia ***întrunirii Miniștrilor de Justiție și Interne*** ai G8 (10 decembrie, Washington, DC)[1], au fost adoptate „***Principiile și Planul de acțiune pentru combaterea criminalității de înaltă tehnologie***", fiecare cu câte zece puncte, care au fost aprobate ulterior.

A. ***Declarația de principii*** cuprinde, printre altele:

I. Nu trebuie să existe paradisuri sigure pentru cei care abuzează de tehnologii informaționale;

II. Investigarea și incriminarea criminalității internaționale de înaltă tehnologie trebuie să fie coordonate între toate statele în cauză, indiferent de locul în care s-a comis infracțiunea;

III. Personalul de aplicare a legii trebuie să fie instruit și dotat pentru a se adresa infracțiunilor de înaltă tehnologie …

V. Sistemele judiciare ar trebui să permită conservarea și accesarea rapidă a datelor electronice, care sunt adesea critice pentru succesul investigării …".

B. ***Planul de acțiune*** (în sprijinul principiilor) cuprinde, printre altele:

„… 2. Luați măsuri adecvate pentru a vă asigura că un număr suficient de personal de aplicare a legii instruit și dotat este alocat pentru combaterea criminalității de înaltă tehnologie și pentru a asista agențiile de aplicare a legii din alte state

3. Revizuiți sistemele noastre judiciare pentru a asigura că acestea incriminează corespunzător abuzurile sistemelor de telecomunicații și informatice și pentru a promova investigarea criminalității de înaltă tehnologie …

10. Dezvoltați și angajați standarde compatibile de investigare criminalistică pentru obținerea și de autentificarea datelor electronice pentru utilizarea în anchete penale și incriminare".

În anul *1999*, la ***Conferința ministerială asupra combaterii criminalității organizate transnaționale*** (19-20 octombrie, Moscova)[2], G8 a precizat (pct. 14-23 din *Comunicatul conferinței*), planurile lor cu privire la lupta împotriva criminalității de înaltă tehnologie. Astfel, și-au exprimat punctul de vedere cu privire la

---

[1] G8 Information Centre, *G8 Justice and Interior Ministers*, disponibil on-line la http://www.g8.utoronto.ca/justice/index.html.

[2] *Idem, Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime (Moscow, October 19-20, 1999)*, disponibil on-line la http://www.g8.utoronto.ca/adhoc/crime99.htm.

unele infracțiuni (pct. 14-15), întărirea sistemului judiciar (pct. 16), principiile pentru accesarea transfrontieră a datelor stocate în calculator (pct. 17) rețeaua internațională de contact 27/7 (pct. 19) etc. O serie de principii în lupta împotriva criminalității informatice adoptate cu acea ocazie se regăsesc și astăzi într-o serie de strategii internaționale.

În anul *2001*, cu ocazia ***întrunirii miniștrilor de justiție și interne*** ai G8 (26-27 februarie, Milano)[1] au fost dezbătute (printre altele) și acțiunile împotriva criminalității de înaltă tehnologie, inclusiv utilizarea Internet-ului în pornografia infantilă, subliniindu-se (în *Comunicatul conferinței*) necesitatea finalizării Convenției Consiliului Europei privind criminalitatea informatică.

În anul *2004*, cu ocazia ***întrunirii miniștrilor de justiție și afaceri interne*** ai G8 (10-11 mai, Washington, DC), „Combaterea criminalității informatice și intensificarea investigațiilor informatice" a fost una dintre preocupările importante, accentuându-se (în *Comunicat*[2]) importanța protejării infrastructurii și dezvoltării de bune practici. Cu această ocazie au fost prezentate „***Bune practici pentru securitatea rețelelor, răspuns la incident și raportarea organelor de aplicare a legii***"[3] dezvoltate de Subgrupul pentru criminalitatea de înaltă tehnologie pentru a-i asista pe operatorii de rețele și administratorii de sisteme informatice atunci când răspund la incidentele informatice.

În anul *2006*, cu ocazia ***Reuniunii la nivel înalt*** G8 (15-17 iulie, St. Petersburg) a fost discutată problema terorismului informatic, reafirmându-se (pct. 4 al *Declarației reuniunii*)[4] implicarea în „… combaterea amenințării teroriste, inclusiv: … contracararea eficientă a încercărilor de a abuza de spațiul virtual pentru scopuri teroriste, inclusiv incitarea la comiterea de acte teroriste, comunicarea și planuirea de acte teroriste, precum și recrutarea și instruirea de teroriști".

În anul *2008*, cu ocazia ***întrunirii miniștrilor de justiție și interne*** ai G8 (11-13 iunie, Tokyo)[5], a fost lansat termenul de „infracțiune în legătură cu identitatea" (în *Declarația finală*), precizându-se că „… nu este un concept juridic formal

---

[1] *Idem*, *Conference of the G8 Ministers of Justice and Interior, Milano, 26-27 February 2001*, disponibil on-line la http://www.g8.utoronto.ca/adhoc/justice2001.htm.

[2] *Idem*, *Communiqué*, G8 Justice and Home Affair, Washington DC, May 11, 2004, disponibil on-line la http://www.g8.utoronto.ca/justice/justice040511_comm.htm.

[3] G8's Subgroup on High-Tech Crime, *Best Practices for Network Security, Incident Response and Reporting to Law Enforcement*, disponibil on-line la http://www.g8.utoronto.ca/justice/G8justice2004_networks.pdf.

[4] G8 Information Centre, *G8 Summit Declaration on Counter-Terrorism*, St. Petersburg, July 16, 2006, disponibil on-line la http://www.g8.utoronto.ca/summit/2006stpetersburg/counterterrorism. html.

[5] *Idem*, *G8 Ministers of Justice and Interior Concluding Declaration*, Tokyo, June 13, 2008, disponibil on-line la http://www.g8.utoronto.ca/justice/justice2008.htm.

… conduitele ilegale care implică abuz de identitate. Acesta include falsificarea, alterarea, precum şi dobândirea neautorizată, transferul, deținerea sau utilizarea de documente de identificare şi informaţii de identificare … au completat aceste abordări tradiționale incriminând în mod special anumite conduite … dobândirea, transferul sau stocarea datelor electromagnetice ale card-urilor de credit şi card-urilor bancare pentru scopuri ilicite …".

În anul *2016*, cu ocazia ***întrunirii miniştrilor de finanțe şi guvernatorilor băncilor centrale*** ai G7 (20-21 mai, Sendai)[1], a fost salutată activitatea, în domeniul financiar, a Grupului de experți în domeniul informatic al G7 (G7 CEG); câteva luni mai târziu (11 octombrie 2016), au fost aprobate, „***Elementele fundamentale ale securității informatice pentru sectorul financiar, ale G7***" (G7FE)[2], un set de 8 elemente – (1) „strategie şi cadru al securității informatice", (2) „guvernanță", (3) „evaluare a riscurilor şi controlului", (4) „monitorizare", (5) „răspuns", (6) „recuperare", (7) „schimb de informații", (8) „învățare continuă" –, fără caracter obligatoriu, care încorporează practici eficiente în domeniul securității informatice pentru entitățile publice şi private din sectorul financiar, concepute astfel încât să fie adaptate şi proporționale cu caracteristicile specifice fiecărei entități şi cu riscurile informatice cu care se confruntă.

Anul următor, în *2017*, cu ocazia ***întrunirii miniştrilor de finanțe şi guvernatorilor băncilor centrale*** ai G7 (12-13 mai, Bari)[3], a fost mandatat Grupul de experți în domeniul informatic al G7 (G7 CEG) să dezvolte (până în octombrie 2017) un set de elemente fundamentale, la nivel înalt şi fără caracter obligatoriu, pentru o evaluare eficientă a securității informatice până în octombrie 2017; la termenul stabilit, au fost transmise şi, ulterior (13 octombrie 2017), aprobate, „***Elementele fundamentale pentru evaluarea eficientă a securității informatice în sectorul financiar, ale G7***"[4], care promovează pe cele elaborate anterior [„Elementele fundamentale ale securității informatice pentru sectorul financiar, ale G7" (G7FE)] şi se concentrează asupra modului în

---

[1] G7 Information Centre, *Chair` Summary - G7 Finance Ministers and Central Bank Governors` Meeting*, Sendai, May 20-21 2016, disponibil on-line la http://www.mof.go.jp/english/international_policy/convention/g7/g7_160524.pdf (ultima dată accesat la 22.01.2018).

[2] *Idem*, *G7 Fundamental Elements of Cybersecurity for the Financial Sector*, October 11, 2016, disponibil on-line la http://www.g8.utoronto.ca/finance/cyber-guidelines-2016.html (ultima dată accesat la 22.01.2018).

[3] *Idem*, *Communiqué*, *G7 Finance Ministers and Central Bank Governors*, May 13, 2017, Bari, Italy, disponibil on-line la http://www.g8.utoronto.ca/finance/170513-communique.html (ultima dată accesat la 22.01.2018).

[4] *Idem*, *G7 Fundamental Elements for Effective Cybersecurity for the Financial Sector*, October 11, 2016, disponibil on-line la http://www.g8.utoronto.ca/finance/G7_Fundamental_Elements_of_Cybersecurity.pdf (ultima dată accesat la 22.01.2018).

care acestea sunt executate şi evaluate; în acest sens sunt dezvoltate cinci *rezultate de dorit* şi cinci *componente de evaluare*, după cum urmează:

(A) rezultate asociate cu o securitate informatică efectivă:

- elementele fundamentale (G7FE) sunt în vigoare;
- securitatea informatică influenţează procesul decizional organizaţional;
- există o înţelegere a faptului că se vor produce întreruperi;
- este adoptată o abordare adaptivă a securităţii informatice;
- există o cultură care conduce comportamente sigure;

(B) promovare a unor evaluări efective a securităţii informatice:

- stabiliţi obiective de evaluare clare;
- stabiliţi şi comunicaţi metodologia şi aşteptările;
- menţineţi un set diversificat de seturi de instrumente şi procese pentru selectarea instrumentelor;
- raportaţi concluzii clare şi acţiuni concrete de remediere;
- asiguraţi că evaluările sunt fiabile şi corecte.

Secțiunea a IV-a
Uniunea Internațională a Telecomunicațiilor (ITU)

Uniunea Internaţională a Telecomunicaţiilor (ITU)[1], este o agenţie specializată în cadrul Organizaţiei Naţiunilor Unite care, cu 193 de state membre, joacă un rol esenţial în dezvoltarea şi standardizarea telecomunicaţiilor, precum şi în probleme de securitate informatică.

De precizat că în ITU a deţinut un rol important în organizarea ***Reuniunii Mondiale la nivel înalt asupra Societăţii Informaţionale*** (WSIS), prin ***Rezoluţia*** Adunării Generale ***nr. 56/183/21.12.2001***[2], şi care a avut loc în două etape[3]:

- ***Geneva***, 10-12 dec. *2003*, a avut ca obiectiv să dezvolte şi să promoveze o declaraţie clară de voinţă politică şi să ia măsuri concrete pentru a stabili bazele unei societăţi informaţionale pentru toţi, care să reflecte toate interesele diferite puse în joc;
- ***Tunis*** (2005), 16-18 nov. *2005*, a avut ca obiectiv punerea în aplicare Planul de acţiune de la Geneva, precum şi de a găsi soluţii şi de a ajunge la acorduri în domeniile guvernării Internet-ului, mecanismelor de finanţare, şi în monitorizarea şi punerea în aplicare a documentelor de la Geneva şi Tunis.

---

[1] International Telecommunication Union (ITU), http://itu.int.

[2] United Nations, General Assembly, A/RES/56/183, disponibil on-line la http://www.un-documents.net/a56r183.htm.

[3] World Information Summit on the Information Society (WSIS), la http://www.itu.int/wsis/basic/about.html.

Guverne, politicieni şi experţi din întreaga lume au împărtăşit idei şi experienţe cu privire la modul cel mai potrivit de a aborda problemele emergente asociate cu dezvoltarea unei societăţi informaţionale globale, inclusiv dezvoltarea standardelor şi legilor compatibile.

Rezultatele Reuniunii sunt cuprinse în ***Declaraţia de principii de la Geneva***[1] ***şi Planul de acţiune de la Geneva***[2]; ***Angajamentul de la Tunis***[3] şi ***Agenda pentru Societatea Informaţională de la Tunis***[4].

A. ***Planul de acţiune de la Geneva*** subliniază importanţa măsurilor în lupta împotriva criminalităţii informatice:

„… C5. Construirea încrederii şi securităţii în utilizarea ICT

12. Încrederea şi securitatea sunt printre principalii piloni ai societăţii informaţionale …

b) Guvernele, în cooperare cu sectorul privat, ar trebui să prevină, să detecteze şi să răspundă la criminalitatea informatică şi abuzul de ICT prin: elaborarea de ghiduri care să ia în considerare eforturile în curs de desfăşurare în aceste domenii; luând în considerare legislaţia care permite investigarea şi incriminarea eficientă a abuzurilor; promovarea eficientă a eforturilor de asistenţă reciprocă; consolidarea sprijinului instituţional la nivel internaţional pentru prevenirea, detectarea şi recuperarea unor astfel de incidente, precum şi încurajarea educaţiei şi creşterea gradului de conştientizare ...".

B. ***Agenda pentru Societatea Informaţională*** subliniază nevoia de cooperare internaţională în lupta împotriva criminalităţii informatice şi face trimitere la abordări legislative existente:

„… 40. Subliniem importanţa incriminării criminalităţii informatice, inclusiv a criminalităţii informatice comise într-o singură jurisdicţie, dar având efecte în alta. Subliniem în continuare necesitatea unor instrumente şi acţiuni efective şi eficiente, la nivel naţional şi internaţional, pentru a promova, printre altele, cooperarea internaţională între agenţiile de aplicare a legii privind criminalitatea informatică. Facem un apel la guverne, pentru cooperarea cu alte părţi interesate să elaboreze legislaţia necesară pentru investigarea şi incriminarea criminalităţii

---

[1] WSIS-03/GENEVA/DOC/4-E, Declaration of Principles: Building the Information Society: a global challenge in the new Millennium, disponibil on-line la http://www.itu.int/wsis/docs/geneva/official/dop.html.

[2] WSIS-03/GENEVA/DOC/5-E, Plan of Action, disponibil on-line la http://www.itu.int/wsis/docs/geneva/official/poa.html.

[3] WSIS-05/TUNIS/DOC/7-E, Tunis Commitment, disponibil on-line la http://www. itu.int/wsis/docs2/tunis/off/7.html.

[4] WSIS-05/TUNIS/DOC/6(Rev.1)-E, Tunis Agenda for The Information Society, disponibil on-line la http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

informatice, observând coordonatele existente, de exemplu, Rezoluțiile 55/63 și 56/121 ale UNGA privind „Combaterea prin mijloace penale a abuzului de tehnologii informaționale" și a inițiativelor regionale, care includ, dar nu se limitează la, Convenția Consiliului Europei asupra criminalității informatice …".

Ca rezultat al WSIS, ITU a fost nominalizată ca unic facilitator pentru linia de acțiune C5 dedicată construirii încrederii și securității în utilizarea tehnologiei informației și comunicațiilor. În anul 2007, secretarul general ITU a lansat Agenda Globală privind Securitatea Informatică (GCA).

Agenda Globală privind Securitatea Informatică (GCA)[1] este construită pe cinci piloni strategici – măsuri legale, măsuri tehnice și procedurale, structuri organizaționale, creare de capacități și cooperare internațională – și este compusă din șapte obiective-cheie:

„1. Elaborarea de strategii de dezvoltare a unui model de legislație a criminalității informatice, care este aplicabil la nivel global și interoperabil cu măsurile legislative existente la nivel național și regional.

2. Elaborarea de strategii globale pentru crearea la nivel național și regional a unor structuri organizaționale și politici adecvate privind criminalitatea informatică.

3. Dezvoltarea unei strategii pentru stabilirea la nivel global a unor criterii minime de securitate acceptate și acreditarea schemelor pentru aplicații (software) și sisteme (hardware).

4. Dezvoltarea strategiilor de creare a unui cadru global pentru urmărire, avertizare și răspuns la incident pentru a se asigura coordonarea transfrontalieră între inițiativele noi și cele existente.

5. Dezvoltarea de strategii pentru crearea și aprobarea unui sistem digital de identitate, generic și universal, și de structuri organizatorice necesare pentru a asigura recunoașterea prerogativelor digitale pentru persoanele fizice peste granițele geografice.

6. Dezvoltarea unei strategii globale pentru a facilita crearea capacităților umane și instituționale pentru a spori cunoștințele și know-how-ul între sectoare și în toate domeniile menționate mai sus.

7. Recomandări cu privire la cadrul potențial pentru o strategie globală multi-direcțională de cooperare internațională, dialog și coordonare în toate domeniile menționate mai sus".

În anul *2008*, în cadrul ITU GCA (Agenda Globală privind Securitatea Informatică), ***ITU și Parteneriatul Internațional Multilateral împotriva Amenințărilor Informatice*** (IMPACT)[2], au stabilit (în mod formal) un *acord* prin care

[1] The ITU Global Cybersecurity Agenda (GCA), disponibil on-line la http://www.itu. int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[2] International Multilateral Partnership Against Cyber Threats (IMPACT), la http://www.impact-alliance.org/.

sediul acestuia (Cyberjawa, Malaezia) devenea (efectiv) locația (fizică) operațională a GCA.

Ulterior, la 20 mai *2011*, în cadrul Reuniunii Mondiale la nivel înalt asupra Societății Informaționale (WSIS), a fost semnat un *acord între ITU și IMPACT* – ce reunește experți guvernamentali, din mediul academic și industrie, pentru a spori capacitățile comunității globale față de amenințările criminalității informatice și oferă statelor membre ITU acces la expertiza, facilitățile și resursele pentru a se adresa acestor amenințări, dar și asistență organismelor ONU în protejarea propriilor infrastructuri ICT – care a devenit ***„brațul" de execuție al ITU pe linia securității informatice***[1].

Secțiunea a V-a
Consiliul Europei (CoE)

Consiliul Europei (CoE)[2] este o organizație interguvernamentală cu 47 de state membre (din care 27 sunt membre ale EU).

În anul *1976*, *problema criminalității în legătură cu calculatorul* a fost discutată în cadrul de lucru al Consiliului Europei, la a 12-a Conferință a Directorilor Institutelor de Cercetări Criminologice[3] și menționată ca *infracțiune nespecifică* în Proiectul de recomandare pentru criminalitatea economică, adoptat de Comitetul de Miniștri la a 335-a întrunire, din 25 iunie ***1981***, sub nr. ***R (81) 12***[4].

În anul *1985*, *problema criminalității în legătură cu calculatorul* a fost inclusă[5] în programul de lucru al Comitetului European pentru Probleme Penale (CDPC) pentru 1985-1986, Comitetul numind o Comisie de Experți pentru Criminalitatea în legătură cu Calculatorul (PC-R-CC) care să studieze această problemă. Comisia și-a început activitatea în 1985 și a încheiat-o în martie 1989. La ultima întrunire Comisia a adoptat raportul un proiect de recomandare care au fost transmise Comitetului pentru aprobare. Proiectul de recomandare și raportul a

---

[1] ITU-IMPACT Strategy, la http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Strategy.aspx.

[2] Council of Europe (CoE), la http://www.coe.int/.

[3] Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 1976.

[4] Council of Europe, Committee of Ministers, *Recommendation no. R (81) 12 of Committee of Ministers to Member States on Economic Crime* (adopted by the Committee of Ministers on 25 June 1981 at the 335th meeting of the Minister's Deputies), la https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=600157&SecMode=1&DocId=672338&Usage=2.

[5] Council of Europe, *Computer-related Crime, Recommendation No. R (89) 9 on computer-related crime and final report of the European Committie on Crime Problems*, Council of Europe Publishing and Documentation Service, Strasbourg, 1990, p. 9.

fost adoptat de Comitet în iunie 1989 și adoptat de Comitetul de Miniștri la a 428-a întrunire, din 13 septembrie ***1989***, sub nr. ***R (89) 9***[1].

În anul *1995*, Comitetul de Miniștri, la a 543-a întrunire adjuncților miniștrilor din 11 septembrie, a adoptat un alt proiect de recomandare privind problemele dreptului procesual penal în materia tehnologiei informației, sub nr. ***R (95) 13***[2].

În anul *1996*, Comitetului European pentru Probleme Penale (CDPC), prin Decizia nr. CDPC/103/211196, plecând de la unele considerații pragmatice – sugerate și de profesorul H.W.K. Kaspern (în raportul pregătit la solicitarea Comitetului) „… ar trebui gândim un alt instrument juridic, care ar angaja mai mult ca o recomandare, cum ar fi o convenție. O astfel de convenție nu ar trebui să se ocupe doar de problemele de drept penal substanțial, dar și cu probleme de procedură penală și acordurile internaționale" –, a înființat un Comitet de experți pentru a se ocupa de criminalitatea informatică.

Ca urmare a acestei decizii, Comitetul de Miniștrii, prin Decizia CM/Del/Dec (97) 583 (04.02.1997) a instituit un nou Comitet, „***Comitetul de Experți în Spațiul Cibernetic***" (PC-CY), care și-a început activitatea în aprilie 1997. Între anii 1997 și 2000, Comitetul a ținut zece întâlniri în plen, cincisprezece ale Grupului de Elaborare și încă trei sub egida CDPC. O versiune a Proiectului de convenției a fost declasificată și prezentată în aprilie 2000 în scopul de a permite consultările.

Proiectul de convenție, revizuit și finalizat, și expunerea de motive, au fost înaintate spre aprobare CDPC, la 50 de sesiune plenară din iunie 2001, după care textul Proiectului de convenție a fost prezentat Comitetului de Miniștri pentru adoptare și deschiderea spre semnare.

La ceremonia de semnare de la Budapesta din 23 noiembrie 2001, 30 de țări au semnat ***Convenția Consiliului Europei privind criminalitatea informatică***[3] (inclusiv patru non-membre ale Consiliului Europei, Canada, Statele Unite ale Americii, Japonia și Africa de Sud, care au participat la negocieri).

---

[1] Council of Europe, Committee of Ministers, *Recommendation no. R (89) 9 of Committee of Ministers to Member States on Computer-Related Crime* (adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Minister's Deputies), la https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2.

[2] Council of Europe, Committee of Ministers, *Recommendation no. R (95) 13 of Committee of Ministers to Member States on Computer-Related Crime* (adopted by the Committee of Ministers on 11 September 1995 at the 543th meeting of the Minister's Deputies), la https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1900870&SecMode=1&DocId=528034&Usage=2.

[3] Council of Europe, *Convention on Cybercrime* (CETS no: 185), disponibil on-line la http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Până în prezent (ianuarie 2018), 60 de ţări au semnat Convenţia, din care 56 au aderat la/ratificat-o[1].

În anul *2003*, Convenţia a fost urmată de ***Protocolul adiţional referitor la incriminarea actelor de natură rasistă şi xenofobă săvârşite prin intermediul sistemelor informatice***[2], adoptat la Strasbourg la 28 ianuarie 2003.

Întrucât, în timpul negocierilor cu privire la textul Convenției, s-a dovedit că, în special, incriminarea distribuției de materialelor rasiste şi xenofobe a fost o chestiune controversată. Unele ţări, care au manifestat o puternică protecție a principiului libertății de exprimare şi-au exprimat îngrijorarea, că, dacă în Convenţie sunt incluse dispoziții care încalcă libertatea de exprimare, ar fi puse în imposibilitatea de a semna Convenția; în consecință, aceste aspecte au fost integrate, separat, în acest protocol.

În anul *2012*, Comitetul Convenției privind criminalitatea informatică (T-CY) a hotărât, la cea de-a opta întrunire (decembrie 2012), să emită ***note orientative***[3], care reprezintă înţelegerea comună a părților la aceasta în ce priveşte utilizarea convenției şi sunt menite să faciliteze utilizarea şi implementarea acestei convenții în lumina progreselor tehnologice, dar şi celor juridice şi politice[4].

Secțiunea a VI-a
Uniunea Europeană (EU)

Uniunea Europeană (EU)[5] este uniune economică şi politică care reuneşte 28 state membre[6].

În anul *1999*, Uniunea Europeană a lansat ***inițiativa „eEurope”***, prin adoptarea Comunicatului Comisiei Europene „eEurope 2005: O societate informațională

---

[1] Council of Europe, *Chart of Signature of Treaty 185 Convention on Cybercrime* (Status of 24/01/2018), disponibil on-line la https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=cLU29LDu (ultima dată accesat la 24.01.2018).

[2] Council of Europe, *Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* (ETS no. 189), disponibil on-line la http://www.conventions. coe.int/Treaty/EN/Treaties/Html/189.htm.

[3] Council of Europe (CoE), Cybercrime Convention Committee (T-CY), *T-CY Guidance Notes* T-CY (2013)29rev, adopted by the 8th, 9th and 12th Plenaries of T-CY, Strasbourg, France, 01 March 2017, disponibil on-line la https://rm.coe.int/16806f9471 (ultima dată accesat la 24.01.2018).

[4] Ioniță GI, *Trends and developments in use and implementation of Cybercrime Convention*, Law between Modernization and Tradition, International Conference, Bucharest, 21-23rd Aprilie 2015, Ed. Hamangiu, București, 2015, pp. 870-876.

[5] European Union (EU), la http://europa.eu.

[6] *Idem*, *The EU in brief*, disponibil on-line la https://europa.eu/european-union/about-eu/eu-in-brief_en (ultima dată accesat la 24.01.2018).

pentru toți”[1], potrivit căreia Europa trebuia să aibă până în anul 2005 serviciile de bază cu acces electronic.

În anul *2001*, Comisia Europeană a publicat o ***comunicare*** intitulată „***Crearea unei societăți informaționale sigure prin îmbunătățirea capacității de securitate a infrastructurii informatice și combaterea criminalității legate de calculatoare***”[2]. În această comunicare, Comisia a analizat și a abordat problema criminalității informatice și a subliniat necesitatea de acțiune eficientă pentru a face față amenințărilor la adresa integrității, disponibilității și fiabilității sistemelor și rețelelor informatice.

„Infrastructurile informatice și de comunicații au devenit o componentă critică a economiilor noastre. Din păcate, aceste infrastructuri au propriile lor vulnerabilități și oferă noi oportunități pentru conduita infracțională. Aceste activități criminale pot avea o mare varietate de forme și pot trece mai multe frontiere. Deși, pentru o serie de motive, nu există statistici credibile, este puțin îndoielnic că aceste infracțiuni constituie o amenințare pentru investițiile în industrie și active, precum și pentru siguranța și încrederea în societatea informațională …

Există posibilitatea de acțiune atât în ceea ce privește prevenirea activității criminale prin consolidarea infrastructurilor de securitate a informațiilor și prin asigurarea faptului că autoritățile de aplicare a legii dispun de mijloacele adecvate pentru a acționa și în același timp, să respecte pe deplin drepturile fundamentale ale indivizilor …

Comisia care a participat la ambele discuții, în CoE și G8, recunoaște complexitatea și dificultățile asociate cu probleme de drept procedural. Dar cooperarea efectivă în cadrul UE pentru combaterea criminalității informatice este un element esențial pentru o societate informațională sigură și de stabilire a unui spațiu de libertate, securitate și justiție …”.

În anul *2007*, Comisia Europeană a publicat o ***comunicare*** intitulată „***Spre o politică generală de luptă împotriva criminalității cibernetice***”[3], în care este

---

[1] Commission of The European Communities, Communication from The Commission to The Council, The European Parliament, The Economic and Social Committee and The Committee of The Regions, *eEurope 2005: An information society for all*, COM (2002) 263, Brussels, 2002, disponibil on-line la http://eur-lex.europa. eu/LexUriServ/LexUriServ.do?uri= COM:2002:0263:FIN:EN:PDF.

[2] Commission of The European Communities, Communication from The Commission to The Council, The European Parliament, The Economic and Social Committee and The Committee of The Regions, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, COM (2000) 890, disponibil on-line la http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF.

[3] Commission of The European Communities, Communication from The Commission to The European Parliament, The Council and The Committee of The Regions, *Toward a general policy on the fight against cybercrime*, COM (2007) 267 final, disponibil on-line la http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=COM:2007: 0267:FIN:EN:PDF.

precizat ca fiind obiectiv strategic general „întărirea luptei împotriva criminalității cibernetice la nivel național, european și internațional", obiectiv care poate fi divizat în trei mari direcții operaționale:

„- îmbunătățirea și facilitarea coordonării și cooperării dintre unitățile de combatere a criminalității informatice, alte autorități relevante și alți experți în Uniunea Europeană

- dezvoltarea în coordonare cu statele membre, organizații europene și internaționale relevante și alte părți interesate, un cadru coerent al politicilor UE în lupta împotriva criminalității informatice

- creșterea gradului de cunoaștere a costurilor și pericolelor reprezentate de criminalitatea informatică".

Ulterior, în anul *2013*, Comisia Europeană împreună cu Înaltul Reprezentant al Uniunii Europene pentru afaceri externe și politica de securitate, au prezentat, printr-o ***comunicare comună*** (către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor), o propunere privind „***Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat***"[1].

[1] European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication to The European Parliament, The Council, The European Economic and Social Committee and the Committee of The Regions, *Cybersecurity Strategy of the European Union: An Open, Seif and Secure Cyberspace*, JOIN(2013) 1 final, Bruxelles, 7.2.2013, disponibil on-line la http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN (ultima dată accesat la 25.01.2018).

Capitolul II

Principalele instrumente juridice şi recomandări cu vocaţie internaţională şi regională care conţin reglementări privind prevenirea şi combaterea criminalităţii informatice

Secţiunea I
Consideraţii generale

La nivel internaţional/regional, eforturile pentru prevenirea şi combaterea acestei forme de manifestare a criminalităţii s-au cristalizat prin câteva instrumente juridice, dintre care amintim:

- Convenţia de la Budapesta privind criminalitatea informatică, din 2001[1];

- Convenţia de la Berna privind protecţia operelor literare şi artistice, din 1886[2];

- Tratatul OMPI privind drepturile de autor, adoptat la Geneva în 1996[3];

- Regulamentul (UE) nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1999/93/CE[4];

- Directiva 2009/24/CE a Parlamentului European şi a Consiliului din 23 aprilie 2009 privind protecţia juridică a programelor pentru calculator[5];

- Directiva 2004/48/CE a Parlamentului European şi a Consiliului din 29 aprilie 2004 privind respectarea drepturilor de proprietate intelectuală[6];

---

[1] Council of Europe, *Convention on Cybercrime* (ETS no: 185), disponibil on-line la http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (ultima dată accesat la 25.01.2018).

[2] WIPO, *Berne Convention for the Protection of Literary and Artistic Works*, disponibil on-line la http://www.wipo.int/treaties/en/text.jsp?file_id=283698 (ultima dată accesat la 25.01.2018).

[3] *Idem*, *WIPO Copyright Treaty* (WCT), disponibil on-line la http://www.wipo.int/export/sites/www/treaties/en/ip/wct/pdf/trtdocs_wo033.pdf (ultima dată accesat la 25.01.2018).

[4] European Parliament and Council, *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, OJ L 257, vol. 57, 28 August 2014, pp. 73-114.

[5] European Parliament and Council, *Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs*, OJ L 111, vol. 52, 5 May 2009, pp. 16-22.

[6] European Parliament and Council, *Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights*, OJ L 157, vol. 47, 30 April 2004, pp. 45-86.

- Directiva 2001/29/CE a Parlamentului European şi a Consiliului din 22 mai 2001 privind armonizarea anumitor aspecte ale dreptului de autor şi drepturilor conexe în societatea informaţională[1];

- Directiva 2000/31/CE a Parlamentului European şi a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societăţii informaţionale, în special ale comerţului electronic, pe piaţa internă (directiva privind comerţul electronic)[2];

- Directiva 95/46/CE a Parlamentului European şi a Consiliului din 24 octombrie 1995 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date[3];

- Recomandarea nr. R (95) 13 a Comitetului de Miniştri către statele membre (ale Consiliului Europei) privind problemele dreptului procesual penal în materia tehnologiei informaţiei (adoptată de Comitetului Miniştrilor la 11 septembrie 1995 la a 543-a reuniune a adjuncţilor miniştrilor)[4];

- Recomandarea nr. R (89) 9 a Comitetului de Miniştri către statele membre (ale Consiliului Europei) asupra criminalităţii în legătură cu calculatorul (adoptată de Comitetului Miniştrilor la 13 septembrie 1989 la a 428-a reuniune a adjuncţilor miniştrilor)[5];

Dintre toate aceste instrumente juridice, am să supun analizei Recomandarea nr. R (89) 9 a Comitetului de Miniştri către statele membre (ale Consiliului Europei) asupra criminalităţii în legătură cu calculatorul (din 1989), Convenţia de la Budapesta privind criminalitatea informatică (din 2001) şi Protocolul

---

[1] European Parliament and Council, *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society*, OJ L 167, vol. 44, 22 June 2001, pp. 10-19.

[2] European Parliament and Council, *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market („Directive on electronic commerce")*, OJ L 178, vol. 43, 17 July 2000, pp. 1-16.

[3] European Parliament and Council, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, vol. 38, 22 November 1995, pp. 31-50.

[4] Council of Europe, Committee of Ministers, *Recommendation No. R (95) 13, of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology*, disponibil on-line la https://rm.coe.int/16804f6e76 (ultima dată accesat la 25.01.2018).

[5] Council of Europe, Committee of Ministers, *Recommendation no. R (89) 9 of The Committee of Ministers to Member States on Computer-Related Crime*, disponibil on-line la https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2 (ultima dată accesat la 25.01.2018).

adițional referitor la incriminarea actelor de natură rasistă și xenofobă săvârșite prin intermediul sistemelor informatice (din 2003)

Secțiunea a II-a
Recomandarea nr. R (89) 9 asupra criminalității în relație cu calculatorul[1]

Așa cum precizam și mai sus, în anul *1985*, *problema criminalității în legătură cu calculatorul* a fost *inclusă*[2] în programul de lucru al Comitetului European pentru Probleme Penale (CDPC) pentru 1985-1986, Comitetul numind o Comisie de Experți pentru Criminalitatea în legătură cu Calculatorul (PC-R-CC) care să studieze această problemă. Comisia și-a început activitatea în 1985 și a încheiat-o în martie 1989. La ultima întrunire Comisia a adoptat raportul un proiect de recomandare care au fost transmise Comitetului pentru aprobare. Proiectul de recomandare și raportul a fost adoptat de Comitet în iunie 1989 și adoptat de Comitetul de Miniștri la a 428-a întrunire, din 13 septembrie ***1989***, sub nr. ***R (89) 9***[3].

Acest document „recomandă Guvernelor statelor membre să ia în considerare, atunci când își revizuiesc legislația sau inițiază o nouă legislație, raportul privind infracțiunile informatice ... și în mod deosebit liniile directoare pentru legislațiile naționale ...".

Liniile directoare pentru legislațiile naționale *includ*[4] *o listă minimă* de infracțiuni, care reflectă consensul general al Comitetului privind anumite abuzuri realizate pe computer care ar trebui să cadă sub incidența normelor penale, precum și *o listă opțională* de infracțiuni, în care sunt descrise actele ce au fost deja incriminate penal în unele state, dar asupra cărora un consens internațional pentru incriminarea lor nu a fost realizat.

A. ***Lista minimă de infracțiuni*** cuprinde:

- sau *Frauda în legătură cu calculatorul*, respectiv introducerea, alterarea, ștergerea înlocuirea datelor sau programelor informatice, sau orice altă interferare

---

[1] Council of Europe, Committee of Ministers, *Recommendation no. R (89) 9 of Committee of Ministers to Member States on Computer-Related Crime* (adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Minister's Deputies), la https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2.

[2] Council of Europe, *Computer-related Crime, Recommendation No. R (89) 9 on computer-related crime and final report of the European Committie on Crime Problems*, Council of Europe Publishing and Documentation Service, Strasbourg, 1990, p. 9.

[3] Council of Europe, Committee of Ministers, *Recommendation no. R (89) 9 of Committee of Ministers to Member States on Computer-Related Crime* (adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Minister's Deputies).

[4] Sandu I. E., Sandu F., Ioniță G. I., *Criminologie, op. cit.*, p. 522-524.

în cursul procesării datelor care influențează rezultatul procesării datelor, prin aceasta cauzând pierderi economice sau orice altă pierdere în proprietatea unei alte persoane cu intenţia de a obţine un câştig economic ilegal pentru el însuşi sau pentru o altă persoană;

- *Falsificarea informatică*, respectiv introducerea, alterarea, ştergerea sau înlocuirea datelor sau programelor informatice, sau orice altă interferare în cursul procesării datelor într-o manieră sau în condiţii precum cele prevăzute în legea naţională încât s-ar constitui cu infracţiunea de fals dacă ar fi fost comise cu un obiect tradiţional al unui asemenea tip de infracţiune;

- *Deteriorarea datelor sau a programelor informatice*: Ştergerea, respectiv deteriorarea sau înlocuirea datelor sau programelor informatice fără drept;

- *Sabotajul informatic*, respectiv introducerea, alterarea, ştergerea sau înlocuirea datelor sau programelor informatice sau interferarea cu sistemele informatice, cu intenţia de a împiedica funcţionarea calculatorului sau a sistemului de telecomunicaţii;

- *Accesarea neautorizată*, respectiv accesarea fără drept a unui sistem informatic sau a unei reţele prin violarea măsurilor de securitate;

- *Interceptarea neautorizată*, respectiv interceptarea, făcută fără drept şi prin măsuri tehnice, a comunicaţiilor la, de la şi în cadrul unui sistem informatic sau a unei reţele;

- *Reproducerea neautorizată a programelor informatice protejate*, respectiv reproducerea, distribuirea sau comunicarea către public fără drept a unui program informatic care este protejat de lege;

- *Reproducerea neautorizată a unei topografii*, respectiv reproducerea fără drept a unei topografii protejată de lege, a unui produs semiconductor, sau o exploatare comercială sau importul pentru acest scop, făcute fără drept, a unei topografii sau a unui produs semiconductor realizat prin folosirea topografiei.

B. ***Lista opţională de infracţiuni*** cuprinde:

- *Alterarea datelor sau programelor informatice*, respectiv alterarea datelor sau programelor fără drept;

- *Spionaj informatic*, respectiv însuşirea prin mijloace improprii sau divulgarea, transferul sau folosirea unui secret comercial fără drept sau orice altă justificare legală, cu intenţia fie de a cauza o pierdere economică unei persoane ce are dreptul de a deţine acel secret fie de a obţine un avantaj economic ilegal pentru sine sau pentru o terţă persoană;

- *Utilizarea neautorizată a unui calculator*, respectiv folosirea unui sistem computerizat sau a unei reţele fără drept care fie:

i. este făcută cu acceptarea riscului unei pierderi semnificative cauzate persoanei îndreptăţite de a folosi sistemul sau dăunează sistemului sau funcţionării sale; sau

ii. este făcută cu intenția de a cauza pierderi persoanei îndreptățite de a folosi sistemul sau dăunează sistemului sau funcționării sale; sau

iii. produce pierderi persoanei îndreptățite de a folosi sistemul sau dăunează sistemului sau funcționarii sale;

- *Utilizarea neautorizată a unui program computerizat protejat*, respectiv folosirea fără drept a unui program informatic care este protejat de lege, cu intenția de a obține un câștig economic pentru sine sau pentru o altă persoană sau de a cauza daune deținătorului acestui drept.

Secțiunea a III-a
Convenția privind criminalitatea informatică[1]

Așa cum precizam mai sus, în anul *1996*, Comitetului European pentru Probleme Penale (CDPC), prin Decizia nr. CDPC/103/211196, plecând de la unele considerații pragmatice – sugerate și de profesorul H.W.K. Kaspern (în raportul pregătit la solicitarea Comitetului) „… ar trebui gândim un alt instrument juridic, care ar angaja mai mult ca o recomandare, cum ar fi o convenție. O astfel de convenție nu ar trebui să se ocupe doar de problemele de drept penal substanțial, dar și cu probleme de procedură penală și acordurile internaționale" –, a înființat un Comitet de experți pentru a se ocupa de criminalitatea informatică.

Ca urmare a acestei decizii, Comitetul de Miniștrii, prin Decizia nr. CM/Del/Dec (97) 583 (04.02.1997) a instituit un nou Comitet, „Comitetul de Experți în Spațiul Cibernetic" (PC-CY), care și-a început activitatea în aprilie 1997. Între anii 1997 și 2000, Comitetul a ținut zece întâlniri în plen, cincisprezece ale Grupului de Elaborare și încă trei sub egida CDPC. O versiune a Proiectului de convenției a fost declasificată și prezentată în aprilie 2000 în scopul de a permite consultările.

Proiectul de convenție, revizuit și finalizat, și expunerea de motive, au fost înaintate spre aprobare CDPC, la 50 de sesiune plenară din iunie 2001, după care textul Proiectului de convenție a fost prezentat Comitetului de Miniștri pentru adoptare și deschiderea spre semnare.

La ceremonia de semnare de la Budapesta din 23 noiembrie 2001, 30 de țări au semnat Convenția Consiliului Europei privind criminalitatea informatică (inclusiv patru non-membre ale Consiliului Europei, Canada, Statele Unite ale Americii, Japonia și Africa de Sud, care au participat la negocieri).

Aici nu am să analizez în detaliu dispozițiile Convenției, întrucât o fac într-un alt capitol, ci am să prezint doar *structura* acesteia.

---

[1] Convenția Consiliului Europei privind criminalitatea informatică, a fost ratificată de România prin Legea nr. 64/2004 publicată în M. Of. nr. 343 din 20 aprilie 2004.

Această convenție are preambul și 48 articole, structurate în 4 părți (capitole), după cum urmează:

În ***Preambul*** „Statele ... Convinse de nevoia de promovare, cu prioritate, a unei politici anti-infracționale comune orientate spre protejarea societății contra criminalității informatice, printre altele, pe calea adoptării unei legislații corespunzătoare și a promovării cooperării internaționale; ... Îngrijorate de riscul ca rețelele de computere și informațiile în format electronic să fie folosite la comiterea de infracțiuni, și ca probele în legătură cu aceste infracțiuni să fie păstrate și transferate de aceste rețele; Constatând că o combatere eficientă a criminalității informatice necesită o cooperare internațională sporită, rapidă și funcțională în probleme de drept penal ...".

În Capitolul I, „***Definiții***", este prezentat înțelesul expresiilor: „sistem informatic", „date informatice", „furnizor de servicii", „date referitoare la trafic";

În Capitolul II, „***Măsuri care trebui luate la nivel național***", sunt prezentate măsurile care vizează:

a. *Dreptul penal material* (Secțiunea 1), ce cuprinde

- Infracțiunile contra confidențialității, integrității și disponibilității datelor și sistemelor informatice (Titlul 1), respectiv Accesarea ilegală (art. 2), Interceptarea ilegală (art. 3), Afectarea integrității datelor (art. 4), Afectarea integrității sistemului (art. 5), Abuzurile asupra dispozitivelor (art. 6);

- Infracțiunile informatice (Titlul 2), respectiv Falsificarea informatică (art. 7), Frauda informatică (art.8);

- Infracțiuni referitoare la conținut (Titlul 3), respectiv Infracțiuni referitoare la pornografia infantilă (art. 9);

- Infracțiunile referitoare la atingerile aduse proprietății intelectuale și drepturilor conexe (Titlul 4), respectiv Infracțiuni referitoare la atingerile aduse proprietății intelectuale și drepturilor conexe (art. 10);

- Alte forme de răspundere și sancțiuni (Titlul 5), respectiv Tentativa și complicitatea (art. 11), Răspunderea persoanelor juridice (art. 12), Sancțiuni și măsuri (art. 13);

b. *Dreptul procedural* (Secțiunea a 2-a), ce cuprinde

- Dispozițiile comune (Titlul 1), respectiv Aria de aplicare a măsurilor procedurale (art. 14), Condiții și măsuri de protecție (art. 15);

- Conservarea rapidă a datelor informatice stocate (Titlul 2), respectiv Conservarea rapidă a datelor informatice stocate (art. 16), Conservarea și dezvăluirea parțială a datelor referitoare la trafic (art. 17);

- Ordinul de punere la dispoziție a datelor (Titlul 3), respectiv Ordinul de punere la dispoziție a datelor (art. 18);

- Percheziția și sechestrarea datelor informatice stocate (Titlul 4) respectiv Percheziția și sechestrarea datelor informatice stocate (art. 19);

- Colectarea în timp real a datelor informatice (Titlul 5), respectiv Colectarea în timp real a datelor referitoare la trafic (art. 20), Interceptarea datelor referitoare la conținut (art. 21);

c. *Competența* (Secțiunea a 3-a, respectiv art. 22);

În capitolul III, „***Cooperarea internațională***", sunt prezentate măsurile care vizează:

a. *Principii generale* (Secțiunea 1), ce cuprind

- Principiile generale referitoare la cooperarea internațională (Titlul 1), respectiv Principii generale referitoare la cooperarea internațională (art. 23);

- Principiile referitoare la extrădare (Titlul 2), respectiv Extrădarea (art. 24);

- Principiile generale referitoare la asistența mutuală (Titlul 3), respectiv Principii generale referitoare la asistența mutuală (art. 25), Informarea spontană (art. 26);

- Principiile referitoare la cererile de asistență mutuală în absența acordurilor internaționale aplicabile (Titlul 4), respectiv Principii referitoare la cererile de asistența mutuală în absența acordurilor internaționale aplicabile (art. 27), Confidențialitatea și restricția de utilizare (art. 28);

b. *Dispoziții speciale*, ce cuprind

- Asistența mutuală în materie de măsuri provizorii (Titlul 1), respectiv Conservarea rapidă a datelor informatice stocate (art. 29), Dezvăluirea rapidă a datelor conservate (art. 30);

- Asistența mutuală privind prerogativele de investigare (Titlul 2), respectiv Asistența mutuală privind accesarea datelor stocate (art. 31), Accesarea transfrontalieră a datelor stocate, cu consimțământ sau în cazul în care acestea sunt accesibile publicului (art. 32), Asistența mutuală pentru strângerea în timp real a datelor referitoare la trafic (art. 33), Asistența mutuală în domeniul interceptării datelor referitoare la conținut (art. 34);

- Rețeaua 24/7 (Titlul 3, respectiv art. 35).

În capitolul IV, „***Clauze finale***", sunt prezentate măsurile care vizează: Semnarea și intrarea în vigoare (art. 36); Aderarea la convenție (art. 37); Aplicarea teritorială (art. 38); Efectele convenției (art. 39); Declarații (art. 40); Clauza federală (art. 41); Rezervele (art. 42); Statutul și retragerea rezervelor (art. 43); Amendamente (art. 44); Reuniunea părților (art. 45); Denunțarea (art. 46); Denunțarea (art. 47); Notificarea (art. 48).

Secțiunea a IV-a
Protocolul adițional referitor la incriminarea actelor de natură rasistă şi xenofobă săvârşite prin intermediul sistemelor informatice[1]

Aşa cum precizam mai sus, în anul *2003*, Convenţia Consiliului Europei privind criminalitatea informatică a fost urmată de Protocolul adițional referitor la incriminarea actelor de natură rasistă şi xenofobă săvârşite prin intermediul sistemelor informatice[2], adoptat la Strasbourg la 28 ianuarie 2003.

Întrucât, în timpul negocierilor cu privire la textul Convenției, s-a dovedit că, în special, incriminarea distribuției de materialelor rasiste şi xenofobe a fost o chestiune controversată. Unele ţări, care au manifestat o puternică protecție a principiului libertății de exprimare şi-au exprimat îngrijorarea, că, dacă în Convenție sunt incluse dispoziții care încalcă libertatea de exprimare, ar fi puse în imposibilitatea de a semna Convenţia; în consecinţă, aceste aspecte au fost integrate, separat, în acest protocol.

Scopul declarat al protocolului (aşa cum este prezentat în art. 1) este de a completa dispozițiile Convenției privind criminalitatea informatică, privind incriminarea faptelor de natură rasistă şi xenofobă prin intermediul sistemelor informatice.

În sensul prezentului protocol (aşa cum se precizează în art. 2 pct. 1), ***material rasist şi xenofob*** înseamnă orice material scris, orice imagine sau orice altă reprezentare de idei ori teorii, care susține, încurajează sau incită la ură, discriminare ori violenţă împotriva oricărei persoane sau a unui grup de persoane, pe considerente de rasă, culoare, ascendenţă, naționalitate ori origine etnică, precum şi religie, dacă este folosit ca pretext pentru oricare dintre aceşti factori.

În ceea ce priveşte măsuri care trebuie luate la nivel național (aşa cum sunt prevăzute în capitolul II), sunt considerate ca ***infracțiuni*** următoarele fapte, comise în condițiile precizate pentru fiecare în parte:

(A) *Distribuirea materialelor rasiste şi xenofobe prin intermediul sistemelor informatice* (art. 3)

(1) Fiecare parte adoptă măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracțiuni, potrivit dreptului său intern, atunci când sunt comise cu intenție şi fără drept, următoarele fapte:

---

[1] Protocolul adițional Convenția Consiliului Europei privind criminalitatea informatică, referitor la incriminarea actelor de natură rasistă şi xenofobă săvârşite prin intermediul sistemelor informatice, a fost ratificat de România prin Legea nr 105/14.04.2009.

[2] Council of Europe, Additional *Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* (ETS no. 189) disponibil on-line la http://www.conventions.coe.int/Treaty/EN/Treaties/Html/189.htm.

- distribuirea sau alte forme de punere la dispoziția publicului, prin intermediul unui sistem informatic, a materialelor rasiste și xenofobe.

(2) O parte își poate rezerva dreptul de a nu prevedea răspunderea penală pentru faptele prevăzute la paragraful 1, atunci când materialul, așa cum este definit la art. 2 paragraful 1, susține, încurajează sau incită la o discriminare care nu este asociată urii ori violenței, cu condiția ca alte metode eficiente de răspuns să fie disponibile.

(3) Fără a prejudicia dispozițiile paragrafului 2, o parte își poate rezerva dreptul de a nu aplica paragraful 1, în cazul discriminărilor pentru care aceasta nu poate prevedea, ca urmare a principiilor stabilite în ordinea sa juridică internă referitoare la libertatea de exprimare, măsurile eficiente de răspuns prevăzute la paragraful 2.

(B) *Amenințarea bazată pe o motivație rasistă și xenofobă* (art. 4)

Fiecare parte adoptă măsurile legislative și alte măsuri considerate necesare pentru a incrimina ca infracțiuni, potrivit dreptului său intern, atunci când sunt comise cu intenție și fără drept, următoarele fapte:

- amenințarea, prin intermediul unui sistem informatic, cu săvârșirea unei infracțiuni grave, astfel cum este definită în dreptul intern, (i) a unor persoane pentru motivul apartenenței la un grup care se identifică prin rasă, culoare, ascendență, naționalitate ori origine etnică, precum și religie, dacă este folosită ca pretext pentru oricare dintre aceste motive, sau (ii) a unui grup de persoane care se distinge prin una dintre aceste caracteristici.

(C) *Insulta având la bază o motivație rasistă și xenofobă* (art. 5)

(1) Fiecare parte adoptă măsurile legislative și alte măsuri considerate necesare pentru a incrimina ca infracțiuni, potrivit dreptului său intern, atunci când sunt comise cu intenție și fără drept, următoarele fapte:

- insultarea în public, prin intermediul unui sistem informatic, (i) a unor persoane, pe motivul apartenenței la un grup care se identifică prin rasă, culoare, ascendență, naționalitate ori origine etnică, precum și religie, dacă este folosită ca pretext pentru oricare dintre aceste motive, sau (ii) a unui grup de persoane care se distinge prin una dintre aceste caracteristici.

(2) O parte poate:

(a) fie să solicite ca infracțiunea prevăzută la paragraful 1 să aibă ca efect expunerea la ură, dispreț sau ridicol a persoanei ori a grupului de persoane menționat la paragraful 1;

(b) fie să își rezerve dreptul de a nu aplica, în totalitate sau în parte, paragraful 1.

(D) *Negarea, minimalizarea grosolană, aprobarea sau justificarea genocidului ori a crimelor împotriva umanității* (art. 5)

(1) Fiecare parte adoptă măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiuni, potrivit dreptului său intern, atunci când sunt comise cu intenție şi fără drept, următoarele fapte:

- distribuirea sau alte forme de punere la dispoziţia publicului, prin intermediul unui sistem informatic, a materialelor ce neagă, minimalizează în mod grosolan, aprobă ori justifică actele constitutive ale genocidului sau ale crimelor împotriva umanității, astfel cum sunt definite în dreptul internațional şi recunoscute ca atare printr-o hotărâre definitivă a Tribunalului Militar Internațional înființat prin Acordul de la Londra la data de 18 aprilie 1945 sau a oricărui alt tribunal internațional înființat prin instrumente internaționale relevante şi a cărui competență a fost recunoscută de către acea parte.

(2) O parte poate:

(a) fie să solicite că negarea sau minimalizarea grosolană, prevăzute la paragraful 1, este comisă cu intenția de a incita la ură, discriminare sau violență împotriva unei persoane ori a unui grup de persoane, pe considerente de rasă, culoare, ascendență, naționalitate sau origine etnică ori de religie, dacă este folosită ca pretext pentru oricare dintre aceste motive;

(b) fie să îşi rezerve dreptul de a nu aplica, în totalitate sau în parte, paragraful 1.

(E) Complicitatea (art. 6)

Fiecare parte adoptă măsurile legislative şi de altă natură care se dovedesc necesare pentru a incrimina ca infracţiune, potrivit dreptului intern, când este comisă în mod intenționat şi fără drept, complicitatea la comiterea oricăreia dintre infracțiunile prevăzute de prezentul protocol, cu intenția ca o asemenea infracţiune să fie comisă.

Capitolul III

Analiză comparativă a modului în care legislatorii naționali au implementat măsurile prevăzute de Convenția privind criminalitatea informatică

Secțiunea I
Considerații generale[1]

Aşa cum precizam mai sus, cu toate că această Convenție (privind criminalitatea informatică) este cel mai important instrument internațional utilizat în lupta împotriva criminalității informatice, (din nefericire) ea *stabileşte doar anumite standarde* şi permite ca acestea (standardele) ***să fie „ajustate" conform necesităților fiecărui stat***.

Din acest motiv, *nu toate ţările au implementat-o în acelaşi mod*.

Cu toate că în unele cazuri legislația internă nu este în concordanță cu recomandările Convenției, totuşi, mai ales în ceea ce priveşte ţările cu un sistem de drept tip „Common Law", interpretările făcute de judecători se apropie mai mult de aceste recomandări.

Această stare de fapt pune sub semnul întrebării însuşi procesul de armonizare a legislației penale deoarece doar aderarea la/ratificarea şi implementarea Convenției, de un număr cât mai mare de ţări, ar permite o armonizarea globală efectivă (nu la nivel declarativ) a legislației cu privire la infracțiunile din sfera criminalității informatice.

Armonizarea dispozițiilor privind infracțiunile din sfera criminalității informatice, pe de o parte, oferă autorităților naționale de aplicare a legii, puterea şi instrumentele necesare pentru investigarea şi urmărirea penală a acestor infracţiuni, şi, pe de altă parte, permite organizarea unui sistem internațional de cooperare rapid şi eficient.

Această armonizare ar fi utilă nu numai pentru autoritățile de aplicare a legii, ci şi pentru sectorul public şi privat.

---

[1] Ioniță G.I., *A comparative analysis regarding the implementation of some CoE's Convention on Cybercrime provisions in the national legislations*, în Revista „Studia Universitatis Babeş-Bolyai Iurisprudentia", ianuarie-martie 2011, nr. 1/2011, Cluj University Press, Cluj-Napoca, 2011, p. 58-88.

Un studiu[1], solicitat de Consiliul Europei şi pregătit de Picotti Lorenzo şi Salvadori Ivan (doi profesori din cadrul Universităţii din Verona), *a analizat legislaţia* ***cu privire la criminalitatea informatică*** *din 24 de ţări europene* – Austria, Albania, Armenia, Bulgaria, Cipru, Croaţia, Republica Cehă, Estonia, Letonia, Lituania, Franţa, Germania, Ungaria, Italia, Olanda, Portugalia, România, Serbia, Slovacia, Spania, fosta Republică Iugoslavă a Macedoniei, Turcia, Ucraina şi Regatul Unit – *şi 9 ţări din afara spaţiului european* – Australia, Brazilia, Egipt, India, Mexic, Philipine, Africa de Sud, Sri Lanka şi Statele Unite ale Americii –, pe baza profilurilor legislative şi studiilor oferite de Consiliul European, incluzând şi traducerea legilor ataşate la aceste documente[2].

Secțiunea a II-a
Analiza comparativă a modului în care au fost definiți termenii utilizați[3]

Potrivit art. 1 din Convenție,

„În sensul prezentei convenţii:

a) expresia *sistem informatic* desemnează orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură, care asigură ori dintre care unul sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor;

b) expresia *date informatice* desemnează orice reprezentare de fapte, informaţii sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcţii de către un sistem informatic;

c) expresia *furnizor de servicii* desemnează:

(i) orice entitate publică sau privată care oferă utilizatorilor serviciilor sale posibilitatea de a comunica prin intermediul unui sistem informatic;

şi

---

[1] Council of Europe, Economic Crime Division, Directorate General of Human Rights and Legal Affairs, *National legislation implementing the Convention on Cybercrime - Comparative Analysis and good practices*, Discussion paper, v. 28 aug 2008, disponibil on-line la http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study2-d-version8%20_28%20august%2008.pdf.

[2] Aceste profiluri legislative au fost elaborate în cadrul de lucru al Proiectului Consiliului Europei asupra criminalităţii informatice, având în vedere schimbul de informaţii cu privire la legislaţia criminalităţii informatice şi evaluarea stadiului actual de implementare a Convenţiei privind criminalitatea informatică în legislaţia naţională; sunt disponibile la http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp.

[3] Ioniță G.I., *A comparative analysis …, op. cit.*

(ii) orice altă entitate care prelucrează sau stochează date informatice pentru acest serviciu de comunicaţii sau pentru utilizatorii săi;

d) datele referitoare la trafic desemnează orice date având legătură cu o comunicare transmisă printr-un sistem informatic, produse de acest sistem în calitate de element al lanţului de comunicare, indicând originea, destinaţia, itinerarul, ora, data, mărimea, durata sau tipul de serviciu subiacent".

De precizat că părţile nu sunt obligate să adopte în legislaţia internă aceleaşi definiţii ca cele prezentate în Convenţie, având puterea de a decide modul în care implementează aceste concepte. Totuşi, conceptele formulate în legislaţiile interne trebuie să fie consecvente principiilor fixate prin acest articol 1 din Convenţie.

Paradoxal, în literatura de specialitate[1], se ridică problema că definirea conceptelor utilizate este prea amplă şi neclară faţă de conduita la care se referă aceasta.

Nu toate ţările care au ratificat Convenţia au introdus în întregime/părţi din definiţiile acestor termeni; spre exemplu: Albania, Armenia, Croaţia, Estonia, Franţa, Ungaria, Lituania, fosta Republică Iugoslavă a Macedoniei, Ucraina, Slovacia.

Sunt foarte puţine *ţări* care definesc toate conceptele ce se regăsesc în art. 1 din Convenţie, *aliniindu-şi* complet *dispoziţiile interne*; spre exemplu: Austria[2], Bulgaria[3], Cipru[4], Sri Lanka[5].

Unele ţări ca Italia[6], Republica Cehă[7], definesc doar conceptul de „date" sau „trafic de date".

---

[1] A se vedea şi Hopkins. S., *Cybercrime Convention A Positive Beginning to a Long Road Ahead*, disponibil on-line la: http://www.law.suffolk.edu/highlights/stuorgs/jhtl/publications/V2N1/SHOPKINSV2N1N.pdf (ultima dată accesat la 30.08.2010).

[2] Secţ. 74 par. 1-2 Cod penal austriac (Strafgesetzbuch) disponibil on-line la: http://www.i4j.at/ gesetze/bg_stgb2008.htm#§_145. (ultima dată accesat la 24.08.2010).

[3] Art. 93 pct. 21-23 Cod penal bulgar (Наказателен Кодекс) disponibil on-line la: http://www.mvr.bg/NR/rdonlyres/74A62C79-FBBE-4619-9854-7897B24638D2/0/NK_BG.pdf (ultima dată accesat la 24.08.2010).

[4] Art. 2 Legea cipriotă nr. 22(III)/2004 (Ο περί της Σύμβασης κατά του Εγκλήματος μέσω του Διαδικτύου (Κυρωτικός) Νόμος του 2004 (22(III)/2004)) disponibil on-line la: http://www.police.gov.cy/police/police.nsf/All/F68C2910055AE565C22574C9002FA68B?OpenDocument (ultima dată accesat la 29.08.2010).

[5] Art. 38 Legea sri lankeză nr. 24/2007 (Computer Crime Act) disponibil on-line la: http://www.documents.gov.lk/Acts/2007/Computer%20Crime%20-%20Act%2024/Act%20No.%2024E.pdf (ultima dată accesat la 24.08.2010).

[6] Secţ. 4 pct.1 lit. b-e şi n şi secţ. 2 lit. h DL italian 196/2003 (Dlgs. 196/2003 Codice della Privacy) disponibil on-line la: http://www.altalex.com/index.php?idnot=6355 (ultima dată accesat la 28.08.2010).

[7] Secţ. 90(1) Legea cehă nr. 127/2005 (Electronic Communications Act) disponibil on-line la: http://www.rrtv.cz/en/static/laws/Electronic_Communications_Act.pdf (ultima dată accesat la 24.08.2010).

Mai mult, legiuitorul german[1] defineşte noţiunea de „date" ca fiind „acelea care sunt stocate sau transmise electronic sau magnetic sau prin alte mijloace de o manieră care nu este imediat perceptibilă", o definiţie chiar mai apropiată decât aceea a noţiunii de „date informatice" adoptată de Convenţie.

O definiţie a sistemului informatic a fost introdusă în legislaţia internă a majorităţii statelor, spre exemplu: Austria[2], Bulgaria[3], Cipru[4], Portugalia[5], SUA[6].

În alte state, ca Italia, Franţa sau Australia, o astfel de definiţie legală lipseşte.

Acest fapt creează dificultăţi în determinarea tipurilor de dispozitive care pot fi incluse; ca exemplu, telefoanele mobile moderne (care oferă acces la Internet) sau alte sisteme de procesare, dispozitive optice, dispozitive de procesare de viteză mare, etc. În acelaşi context, ar trebui definite şi alte concepte tehnice folosite, ca, spre exemplu, „măsuri de siguranţă". De asemenea, ar trebui clarificate unele aspecte cum ar fi: „intenţionat", „neautorizat", „fără drept", „fără încuviinţare" etc.

Secțiunea a III-a
Analiza comparativă a modului în care au fost incriminate infracțiunile împotriva confidențialității, integrității şi disponibilității datelor[7]

Infracţiunile definite în articolele 2-6 din Convenţie sunt menite să protejeze confidenţialitatea, integritatea şi disponibilitatea sistemelor informatice sau datelor, şi nu de a incrimina activităţile legitime şi obişnuite inerente în proiectarea reţelelor, ori activităţile de operare legitime şi obişnuite şi practicile comerciale[8].

§ 1. Accesarea ilegală

Potrivit art. 2 din Convenție,

„Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, accesarea

---

[1] Secţ. 202a(2) Cod penal german (Strafgesetzbuch) disponibil on-line la: http://bundesrecht.juris.de/stgb/index.html (ultima dată accesat la 24.08.2010).

[2] Secţ. 74 par. 1 pct. 8 şi par. 2 Cod penal austriac.

[3] Art. 93 pct. 21-23 Cod penal bulgar.

[4] Art. 2 Legea cipriotă nr. 22(III)/2004.

[5] Art. 2 Legea portugheză nr. 109/1991 (Lei nº 109/91 - Sobre a criminalidade informática) disponibil on-line la: http://www.cnpd.pt/bin/legis/nacional/lei_10991.htm.

[6] Titlul 18 partea I cap. 47 § 1030(e) Cod penal federal american (US Code) disponibil on-line la: http://codes.lp.findlaw.com/uscode/ (ultima dată accesat la 24.08.2010).

[7] Ioniță G. I., *A comparative analysis …, op. cit*.

[8] Council of Europe, Convention on Cybercrime (ETS No. 185) *Explanatory Report*, pct. 33, disponibil on-line la: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (ultima dată accesat la 29.08.2010).

intenționată și fără drept a ansamblului ori a unei părți a unui sistem informatic. O parte poate condiționa o astfel de incriminare de comiterea încălcării respective prin violarea măsurilor de securitate, cu intenția de a obține date informatice ori cu altă intenție delictuală, sau de legătura dintre încălcarea respectivă și un sistem informatic conectat la alt sistem informatic".

Această recomandare de incriminare reprezintă[1] infracțiunea de bază care include amenințările periculoase/atacurile la adresa/împotriva securității sistemelor informatice și a datelor(de exemplu, confidențialitatea, integritatea și disponibilitatea). Nevoia de protecție reflectă interesele organizațiilor și persoanelor fizice de a gestiona, opera și controla propriile sisteme liber și netulburat. Simpla pătrundere neautorizată (adică „hacking", „cracking" sau „pătrunderea în calculator") ar trebui, în principiu, să fie ilegală, în sine, întrucât poate genera impedimente pentru utilizatorii legitimi ai sistemelor și datelor și poate provoca alterarea sau distrugerea acestora, cu costuri ridicate pentru reconstrucție. De asemenea, astfel de pătrundere poate conferi acces la date confidențiale (incluzând parole, informații despre sistemul de țintă) și secrete, poate conduce la utilizarea sistemului fără plată sau poate chiar încuraja hackerii să comită forme mai periculoase de infracțiuni în legătură cu utilizarea calculatorului, cum ar fi frauda sau falsul.

Cu toate acestea, așa cum s-a subliniat în literatura de specialitate[2], nu ar trebui incriminate activitățile obișnuite legate de utilizarea Internet-ului, activitățile inerente realizării rețelelor sau operațiunile comerciale obișnuite cum ar fi: trimiterea de mesaje electronice fără a fi solicitate de către destinatar, accesarea unei pagini web sau a unui protocol de transfer al fișierelor care a fost creată pentru accesul public, utilizarea legăturilor hipertext sau utilizarea programelor de tip „cookies" sau „bots" pentru a localiza sau a obține informații prin care anumite programe să fie filtrate sau respinse de server-ul primitor.

Sunt câteva *țări* care au introdus în legislația internă *reglementări în concordanță* cu dispozițiile art. 2 din Convenție; spre exemplu: Brazilia[3], Cipru[4], Estonia[5], Franța[6],

---

[1] *Ibidem*, pct. 44.

[2] A se vedea și Baron, R., *A Critique of the International Cybercrime Traty*, 2002, CommLaw Conspectus: Journal of Communication Law and Policy, vol. 10, p. 268.

[3] Art. 154A-B Cod penal brazilian (Código Penal) disponibil on-line la: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm (ultima dată accesat la 24.08.2010).

[4] Art. 4 Legea cipriotă nr. 22(III)/2004.

[5] Art. 217 Cod penal eston (Penal Code) disponibil on-line la: http://www.legaltext.ee/text/en/X30068K8.htm (ultima dată accesat la 24.08.2010).

[6] Art. 323-1 Cod penal francez (Code pénal) disponibil on-line la: http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 (ultima dată accesat la 24.08.2010).

Italia[1], Lituania[2], Mexic[3], Portugalia[4], Slovacia[5], Ungaria[6], SUA[7].

Din nefericire, niciuna dintre ţări nu defineşte conceptele de „acces", „fără autorizaţie" şi „măsuri de siguranţă". Această situaţie generează probleme grave în practică, în special cu privire la locul şi timpul comiterii infracţiunii.

Sunt câteva state[8] din cadrul SUA care definesc termenul de „acces". Trei dintre definiţiile sunt mai comune: „a iniţia, a comunica cu"; „a stoca datele în, a recepţiona date de la"; „a utiliza orice resurse ale unui calculator, sistem informatic sau reţea informatică".

Potrivit art. 2, par. 2 din Convenţie, statele membre pot condiţiona incriminarea de:

- „violarea măsurilor de securitate", cum este, de exemplu, cazul Austriei[9] („măsuri specifice de securitate în cadrul sistemului informatic"), Ciprului[10] („măsuri de securitate"), Estoniei[11] („cod, parolă sau alte măsuri de protecţie"), Germaniei[12] („mecanisme de securitate a accesului"), Lituaniei[13] („măsuri de securitate"), Mexicului[14] („mecanism de securitate"), Ungariei[15] („sistem sau echipament de protecţie al calculatorului"). Cu toate acestea, nici una dintre ţări, nu oferă o definiţie a acestui concept.

- „intenţia de a obţine date informatice sau altă intenţie delictuală", cum este, spre exemplu, cazul Portugaliei[16] şi Slovaciei[17].

---

[1] Art. 615-ter Cod penal italian (Codice penale) disponibil on-line la: http://www.altalex.com/index.php?tag=Y&qs=codice+penale (ultima dată accesat la 24.08.2010).

[2] Art. 198 şi 198-1 Cod penal lituanian (Kriminãllikums) disponibil on-line la: http://www.ttc.lv/export/sites/default/docs/LRTA/Likumi/The_Criminal_Law.doc (ultima dată accesat la 24.08.2010).

[3] Art. 211bis 1-2 şi 4 Cod penal federal mexican (Código Penal para el Distrito Federal) disponibil on-line la: http://www.ordenjuridico.gob.mx/Documentos/Estatal/Distrito %20Federal/wo29085.pdf (ultima dată accesat la 24.08.2010).

[4] Art. 7 Legea portugheză nr. 109/1991.

[5] Art. 247 (1) Cod penal slovac (Trestný Zákon) disponibil on-line la: http://www.minv.sk/swift_data/source/policia/finpol/300_2005.pdf (ultima dată accesat la 24.08.2010).

[6] Art. 300/C (1) Cod penal ungar (a Büntető Törvénykönyvről) disponibil on-line la: http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=97800004.TV (ultima dată accesat la 26.08.2010).

[7] Titlul 18, partea I, cap. 47, § 1030(a)(1)-(5) Cod penal federal american.

[8] Alabama, Arkansas, Conneticut, Delaware, Iowa, Kansas, New Hampshire.

[9] Secţ. 118a Cod penal austriac.

[10] Art. 4 Legea cipriotă nr. 22(III)/2004.

[11] Art. 217 Cod penal eston.

[12] Secţ. 202a Cod penal german.

[13] Art. 198(1) Cod penal lituanian.

[14] Art. 211 bis1 Cod penal federal mexican.

[15] Art. 300/C(1) Cod penal ungar.

[16] Art. 7 Legea portugheză nr. 109/91

[17] Art. 247(1) Cod penal slovac.

- „legătura dintre încălcarea respectivă şi un sistem informatic conectat la alt sistem informatic", care, până în prezent, se pare că nu a fost încă reglementată.

Multe legislaţii naţionale conţin, în prezent, reglementări cu privire la infracţiuni de hacking sau cracking; ceea ce diferenţiază aceste incriminări sunt elementele obiective şi subiecte, care diferă considerabil de la o ţară la alta.

Astfel, unele ţări ca Belgia[1], Franţa[2], Italia[3], şi în conformitate cu Recomandarea Consiliului Europei nr. R (89) 9, nu incriminează doar accesul într-un sistem informatic, ci şi rămânerea în aceste sisteme.

Mai multe ţări au urmat o abordare mai restrânsă reclamând, suplimentar, mai multe circumstanţe calificate.

Câteva ţări, ca Armenia[4] şi Austria[5], au mers chiar dincolo de reglementările Convenţiei atacând elemente diferite. Codul penal armean, de exemplu, în art. 251 alin. 1 incriminează chiar „neglijenţa care cauzează schimbarea, copierea, modificarea, izolarea informaţiei sau stricarea echipamentelor informatice, a sistemelor informatice sau alte pagube semnificative".

Unele ţări nu fac referire la accesarea ilegală a întregului calculator sau a unei părţi a acestuia, ci, în general, la resursele unui calculator, care stabilesc nivelul incriminării. Spre exemplu, Armenia[6] pedepseşte „accesarea (penetrarea) informaţiilor stocate într-un sistem informatic", Bulgaria[7] pedepseşte „accesul la resursele unui calculator", Croaţia[8] pedepseşte „accesul la date sau programe informatice", Regatul Unit[9] pedepseşte „accesul neautorizat la materialele informatice".

Câteva dintre *dispoziţiile* legislaţiilor interne care au fost *armonizate* cu dispoziţiile art. 2 din Convenţie:

- Art. 4 din Legea cipriotă nr. 22(III)/2004 sancţionează „orice persoană care intenţionat şi fără autoritate accesează un sistem informatic prin încălcarea măsurilor de securitate".

---

[1] Art. 550-bis §1 Cod penal belgian (Code penal) disponibil on-line la: http://www.ejustice.just.fgov.be/wet/wet.htm (ultima dată accesat la 25.08.2010).

[2] Art. 323-1 Cod penal francez.

[3] Art. 615-ter Cod penal italian.

[4] Art. 251 Cod penal armean (Criminal Code of the Republic of Armenia) disponibil on-line la: http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=eng (ultima dată accesat la 25.08.2010).

[5] Secţ. 118a Cod penal austriac.

[6] Art. 251 Cod penal armean.

[7] Art. 319a Cod penal bulgar.

[8] Art. 223(1) OG croată 105/04.

[9] Art. 1 Legea abuzului asupra calculatorului (Computer Misuse Act 1990 c.18) disponibil on-line la: http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm (ultima dată accesat la 25.08.2010).

- Art. 323-1 alin. 1 din Codul penal francez, pedepseşte „accesarea sau menţinerea, în mod fraudulos, în sau într-o parte dintr-un sistem informatic de procesare automată a datelor" iar potrivit alin. 2, pedeapsa este mai gravă dacă „accesarea determină eliminarea sau modificarea datelor conţinute în sistem sau alterarea funcţionării acelui sistem".

- Art. 615-ter („Accesarea abuzivă a unui sistem informatic şi de telecomunicaţii") din Codul penal italian incriminează „pătrunderea abuzivă într-un sistem informatic sau de telecomunicaţii protejat de măsuri de siguranţă", dar şi „menţinerea împotriva voinţei exprese sau tacită a celui care are dreptul de excludere".

De precizat faptul că legislatorul italian a introdus ideea inedită, de „domiciliu informatic", norma mai sus citată (art. 615-ter din Codul penal italian) făcând parte din grupa infracţiunilor contra inviolabilităţii domiciliului (Dei delitti contro la inviolabilità del domicilio). În acelaşi sens pronunţându-se şi Curtea Supremă de Casaţie italiană, Camera a Şasea Penală, care prin decizia nr. 3067 din 04 octombrie 1999, a statuat că prin dispoziţiile art. 615-ter din Codul penal italian introdus prin Legea nr. 547 din 23 decembrie 1993 legislatorul a asigurat protecţia „domiciliului informatic" în calitate de loc ideal (fizic, în acelaşi timp, unde sunt conţinute datele informatice) care se încadrează în sfera individuală[1].

§ 2. Interceptarea ilegală

Potrivit art. 3 din Convenţie,

„Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, interceptarea intenţionată şi fără drept, efectuată prin mijloace tehnice, a transmisiilor de date informatice care nu sunt publice, destinate, provenite sau aflate în interiorul unui sistem informatic, inclusiv a emisiilor electromagnetice provenind de la un sistem informatic care transportă asemenea date. O parte poate condiţiona o astfel de incriminare de comiterea încălcării respective cu intenţie delictuală sau de legătura dintre încălcarea respectivă şi un sistem informatic conectat la alt sistem informatic".

---

[1] A se vedea şi Sarzana C., *Aperçu des stratégies normatives italiennes de droit matériel au sujet de la lutte a la cybercriminalité et des applications jurisprudentielles correpondantes. Comparasion avec les dispositions contenues dans la Convention de Budapest*, Octopus Interface Conference, Strasbourg 11-12 June 2007, p. 2-3, disponibil on-line la: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20interface2007/567%20if-pres%20sarzana.pdf (ultima dată accesat la 31.08.2010).

Această recomandare de incriminare urmărește[1] să protejeze dreptul la confidențialitatea comunicațiilor de date. Ea reprezintă aceeași încălcare a confidențialității comunicațiilor ca tradiționala înregistrare a convorbirilor telefonice între persoane, aplicând acest principiu la toate formele de transfer electronic de date, indiferent că se realizează prin telefon, fax, e-mail sau transfer de fișiere.

Exemple de *țări* care au introdus în legislația internă *reglementări în concordanță* cu dispozițiile art. 3 din Convenție: Austria[2], Croația[3], Cipru[4], Germania[5], Italia[6], Portugalia[7], Slovacia[8], Sri Lanka[9].

În unele state, interceptarea ilegală nu se referă numai la transmiterea privată a datelor, ci și la toate modalitățile de comunicare.

De asemenea, multe țări folosesc o gamă variată de expresii care nu sunt în perfectă armonie cu prevederile Convenției. De exemplu, Bulgaria[10], folosește expresia „mesaj" în loc de „transmitere a datelor informatice"; Portugalia[11] face referire la „toate tipurile de comunicare din cadrul unui sistem informatic"; SUA[12] iau în calcul „orice comunicare orală, prin cablu sau electronică".

O cerință a art. 3 este ca interceptarea să fi fost făcută „fără drept" și prin „utilizarea unor mijloace tehnice". Totuși, nu toate legislațiile țărilor care au ratificat Convenția solicită în mod explicit că interceptarea ilegală trebuie comisă utilizând instrumente tehnice (ex. utilizarea de parole sau programe); spre exemplu: Armenia[13], Croația[14], Cipru[15], Estonia[16], Lituania[17]. Doar câteva din aceste legislații solicită ca infracțiunea să fie comisă cu intenție; spre exemplu Austria[18]. În plus, nicio legislație nu solicită ca infracțiunea să se realizeze în legătură cu un sistem informatic conectat la un altul, așa cum se menționează în art. 3, alin. 2 din Convenție.

---

[1] Council of Europe, *Explanatory Report*, *op. cit.*, pct. 51.
[2] Secț. 119 și 119a Cod penal austriac.
[3] Art. 223 par. 4 OG croată 105/04.
[4] Art. 5 Legea cipriotă nr. 22(III)/2004.
[5] Sect. 202b Cod penal german.
[6] Art. 617-quater, 617-quinquies, 617-sexies, 623-bis Cod penal italian.
[7] Art. 8 Legea portugheză nr. 109/1991.
[8] Art. 247(2) Cod penal slovac.
[9] Art. 8 Legea sri lankeză nr. 24/2007.
[10] Art. 171(1) Cod penal bulgar.
[11] Art. 8 Legea portugheză nr. 109/1991.
[12] Titlul 18, partea I, cap. 119, § 2511 Cod penal federal american.
[13] Art. 254(1) Cod penal armean.
[14] Art. 223(4) OG croată 105/04.
[15] Art. 5 Legea cipriotă nr. 22(III)/2004.
[16] Art. 137 Cod penal eston.
[17] Art. 198 Cod penal lituanian.
[18] Secț. 119a Cod penal austriac.

Astfel, nu toate țările care au ratificat Convenția au implementat complet art. 3; spre exemplu art. 226-15, alin. 2 din Codul penal francez incriminează, comiterea cu rea-credință: „interceptarea, deturnarea, utilizarea sau divulgarea corespondenței emise, trimise sau primite prin telecomunicație sau instalarea dispozitivelor concepute să permită astfel de interceptări".

Exemple de *dispoziții* ale legislațiilor interne care au fost *armonizate* cu dispozițiile art. 3 din Convenție:

- Art. 223 alin. 4 din OG. croată 105/04, incriminează pe „Oricine interceptează sau înregistrează o transmisie privată de date electronice către, între sau de la un sistem informatic, care nu îi este destinată, incluzând transmisiile electromagnetice a datelor în sistemele informatice, sau oricine care permite unei persoane neautorizate să acceseze aceste date".

- Art. 5 alin. 1 din Legea cipriotă nr. 22(III)/2004 incriminează „orice persoană care, cu intenție și fără autoritate, interceptează transmisii private de date informatice de la sau între calculatoare".

- Secț. 202b („Interceptarea datelor") din Codul penal german prevede că „oricine, fără autorizație și cu ajutorul mijloacelor tehnice, obține pentru sine sau pentru altă parte accesul la date ce nu îi sunt adresate (Secțiunea 202a, subsecțiunea (2)) de la transmisiuni private de date sau de la emisiile electromagnetice ale echipamentelor de procesare a datelor".

- Art. 617-quarter („Interceptarea, împiedicarea sau întreruperea ilicită de comunicații informatice sau telecomunicații"), art. 617-quinquies („Instalarea de echipamente de interceptare, împiedicare sau întrerupere a comunicațiilor informatice sau telecomunicațiilor"), art. 617-sexies („Falsificarea, alterarea sau eliminarea conținutului comunicațiilor informatice sau telecomunicațiilor") și art. 623bis („Alte comunicații și conversații") din Codul penal italian se aplică tuturor tipurilor de comunicații, fără diferențiere între transmisiile de date private sau publice. Art. 617-quinquies din același cod sancționează și „instalarea, în afara cazurilor permise de lege, a dispozitivelor adaptate să intercepteze, împiedice sau să întrerupă comunicarea între sisteme informatice sau de telecomunicații".

Pentru a evita incriminarea excesivă, este recomandabil ca țările să incrimineze numai interceptarea transmisiilor de date informatice care nu sunt publice (incluzând aici și emisiile electromagnetice), realizată prin intermediul unor dispozitive tehnice.

§ 3. Afectarea integrității datelor

Potrivit art. 4 din Convenție,

„1. Fiecare parte va adopta măsurile legislative și alte măsuri considerate necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, fapta

comisă intenționat și fără drept de a distruge, șterge, deteriora, modifica sau elimina date informatice.

2. O parte va putea să își rezerve dreptul de a condiționa incriminarea comportamentului descris la paragraful 1 de producerea unor daune grave".

Scopul[1] acestei propuneri de incriminare este de a furniza datelor și programelor informatice o protecție similară celor de care beneficiază obiectele corporale împotriva prejudicierii intenționate. Interesul legal protejat este integritatea și corecta funcționare sau utilizare a datelor informatice stocate sau programelor de calculator.

Partea a doua a propunerii de incriminare (art. 4, paragraful 2 Convenție) permite statelor părți să incrimineze numai conduita ce cauzează „prejudicii grave". Fiecare stat parte având posibilitatea să definească în mod autonom măsura în care prejudiciul provocat poate fi considerat „grav", în baza propriilor criterii ale legislației interne[2].

Exemple de *țări* care au introdus în legislația internă *reglementări în concordanță* cu dispozițiile art. 4 din Convenție: Austria[3], Croația[4], Cipru[5], Germania[6], Italia[7], Slovacia[8], Sri Lanka[9].

Unele state precum Bulgaria[10], Estonia[11], Lituania[12], incriminează afectarea integrității datelor numai în cazuri semnificative, solicitând, ca respectiva conduită să aibă drept consecințe prejudicii grave.

În unele țări precum Croația[13], Slovacia[14], Turcia[15], reglementările sunt implementate integral cu excepția elementelor „intenționat" sau „fără drept". Suplimentar, alte state precum Armenia[16], incriminează nu numai comiterea intenționată, dar și „neglijența care a cauzat consecințe grave".

---

[1] Council of Europe, *Explanatory Report*, *op. cit.*, pct. 60.

[2] *Ibidem*, pct. 64.

[3] Secț. 126a Cod penal austriac.

[4] Art. 223 par. 3 OG croată 105/04.

[5] Art. 6 Legea cipriotă nr. 22(III)/2004.

[6] Secț. 303 a Cod penal german.

[7] Art. 635-bis și 635-ter Cod penal italian.

[8] Art. 247(1)b Cod penal slovac.

[9] Art. 5(a) Legea sri lankeză nr. 24/2007.

[10] Art. 319b Cod penal bulgar.

[11] Art. 206 Cod penal eston.

[12] Art. 196 Cod penal lituanian.

[13] Art. 223(3), OG croată 105/04.

[14] Art. 247(1)b Cod penal slovac.

[15] Art. 244(2) Cod penal turc (Türk Ceza Kanunu) disponibil on-line la: http://www.tbmm.gov.tr/kanunlar/k5237.html (ultima dată accesat la 26.08.2010).

[16] Art. 253 Cod penal armean.

Nu toate reglementările naţionale acoperă toate formele de afectare a integrităţii datelor informatice. Spre exemplu, art. 323-3 din Codul penal francez acoperă doar „introducerea frauduloasă de date într-un sistem automat de procesare sau suprimarea ori modificarea frauduloasă a datelor pe care acesta le conţine".

Unele state nu folosesc, în legislaţia internă, aceiaşi termeni ca cei folosiţi în art. 4 din Convenţie, ci numai o expresie generică precum „imixtiune în orice fel"[1], „ştergere, izolare şi inutilizare"[2], „accesare, modificare, deteriorare"[3], „acţiuni neautorizate"[4], şi, din aceste motive, ar putea fi îndoielnic, în anumite cazuri, dacă aceste expresii pot include toate actele de distrugere, ştergere, deteriorare, modificare sau eliminare, aşa cum sunt reglementate de art. 4 din Convenţie.

Alte state precum Slovacia[5], Ucraina[6], nu incriminează imixtiunea în datele informatice, ci asupra „informaţiilor".

Exemple de *implementare integrală* în legislaţia internă a dispoziţiilor art. 4 din Convenţie:

- Art. 233, par. 3 din OG croată nr. 105/04 incriminează pe „Oricine prejudiciază, alterează, şterge, distruge sau face în vreun alt fel inutilizabile sau inaccesibile date electronice sau programe informatice ale altcuiva".

- Potrivit art. 6 din Legea cipriotă nr. 22(III)/2004, infracţiunea este comisă de către „Orice persoană care, în mod intenţionat şi fără autoritate, distruge, şterge, alterează ori suprimă (ascunde) date informatice".

- Secţ. 303a („Alterarea datelor") din Codul penal german pedepseşte pe oricine care „în mod ilegal şterge, suprimă, face inutilizabil sau alterează datele informatice (secţiunea 202a subsecţiunea (2))".

Aproape toate statele au reglementări ce corespund parţial sau total cu prevederile art. 4 din Convenţie.

O diferenţă majoră apare între diferitele tipuri de infracţiuni la nivel naţional privind descrierea actelor de imixtiune.

§ 4. Afectarea integrităţii sistemului

Potrivit art. 5 din Convenţie,

„Fiecare parte va adopta măsurile legislative şi alte măsuri care sunt necesare pentru a incrimina ca infracţiune, în conformitate cu dreptul intern, afectarea

---

[1] Art. 192/b Cod penal albanez (Kodi Penal I Republikës Së Shqipërisë) disponibil on-line la: http://www.mpcs.gov.al/dpshb/images/stories/files/kodet/3.3.5._Kodi_ Penal.pdf (ultima dată accesat la 26.08.2010).

[2] Art. 253 Cod penal armean.

[3] Art. 477.1 şi art. 477.2 Cod penal australian.

[4] Art. 362 alin.1. Cod penal ucrainean.

[5] Art. 247(1) b Cod penal slovac.

[6] Art. 362(1) Cod penal ucrainean (Кримінальний Кодекс України) disponibil on-line la: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2341-14 (ultima dată accesat la 26.08.2010).

gravă, intenționată și fără drept a funcționării unui sistem informatic, prin introducerea, transmiterea, periclitarea, ștergerea, deteriorarea, alterarea sau suprimarea datelor informatice".

Propunerea de incriminare vizează[1] o împiedicare intenționată a utilizării licite a sistemelor informatice, inclusiv a instalațiilor de telecomunicații, prin utilizarea sau influențarea datelor informatice. Interesul legal protejat este interesul operatorilor și utilizatorilor de sisteme informatice sau sisteme de telecomunicații de a le avea în bună stare de funcționare. Textul este formulat într-un mod neutru, astfel încât toate tipurile de funcții să poată fi protejate.

Sunt câteva țări care au introdus în legislația internă *reglementări în concordanță* cu dispozițiile art. 5 din Convenție; spre exemplu: Austria[2], Cipru[3], Franța[4], Germania[5], Italia[6], Slovacia[7], Sri Lanka[8].

Unele state precum Austria[9], Croația[10], Portugalia[11] exemplifică infracțiunile utilizând expresii ca „a interfera cu un sistem" sau „a face inutilizabil".

Alte state, cum ar fi Franța, incriminează (art. 323-2 C. pen.) simpla „împiedicare sau interferare în funcționarea unui sistem de procesare automată a datelor"; „suprimarea sau modificarea datelor", iar „accesarea sau rămânerea într-un sistem de procesare automată a datelor" este incriminată (în art. 323-1C. pen.) ca infracțiune de sine stătătoare.

Astfel, aceste reglementări sunt mai cuprinzătoare decât art. 5 din Convenție deoarece acoperă toate încercările de imixtiune și nu doar „afectarea gravă".

Fiecare stat parte are libertatea de a determina un nivel minim al prejudiciului cauzat ce poate fi definit ca „grav" și, în funcție de nivelul prejudiciului (parțial, total, temporar), ar putea alege o sancțiune administrativă, civilă sau penală.

Incriminarea producerii unui „prejudiciu grav" este adecvată întrucât se evită supra-incriminarea. Spre exemplu, transmiterea unui mesaj de poștă electronică nesolicitat (tip „spam") ar putea cauza un disconfort destinatarului însă ar putea să nu prejudicieze calculatorul. Situația este diferită în cazul în

[1] Council of Europe, *Explanatory Report*, *op. cit.*, pct. 65.
[2] Secț. 126b Cod penal austriac.
[3] Art. 7 Legea cipriotă nr. 22(III)/2004.
[4] Art. 323-2 Cod penal francez.
[5] Secț. 303b Cod penal german.
[6] Art. 635-quater și 635-quinquies Cod penal italian.
[7] Art. 247(1) Cod penal slovac.
[8] Art. 5a Legea sri lankeză nr. 24/2007.
[9] Secț. 126b Cod penal austriac.
[10] Art. 223(3) OG croată 105/04.
[11] Art. 5 și 6 Legea portugheză nr. 109/91.

care transmiterea unui astfel de mesaj ar fi însoțită de un cod maliţios sau când s-ar transmite un număr foarte mare de mesaje nesolicitate care ar putea cauza întreruperea unui sistem informatic şi, în consecinţă, astfel de situaţii ar trebui pedepsite.

Exemple de *implementare integrală* în legislaţia internă a dispoziţiilor art. 5 din Convenţie:

- Art. 7 din Legea cipriotă 22(III)/2004 incriminează pe „Orice persoană care în mod intenţionat şi fără autoritate cauzează împiedicarea gravă a funcţionării unui sistem informatic, prin introducerea, transmiterea, distrugerea, ştergerea, alterarea, adăugarea ori suprimarea datelor informatice".

- Secţ. 303b („Sabotarea calculatoarelor") din Codul penal german incriminează pe „(1) Oricine interferează cu procesarea datelor care sunt deosebit de importante pentru afacerea sau întreprinderea unei alte părţi sau pentru o autoritate publică prin: 1. comiterea unui act prevăzut în secţiunea 303a subsecţiunea (1); sau 2. distrugerea, deteriorarea, compromiterea, ştergerea sau alterarea sistemelor de procesare sau de transport a datelor".

Aşa cum se poate constata, foarte multe ţări nu incriminează afectarea gravă a funcţionării sistemelor informatice.

§ 5. Abuzurile asupra dispozitivelor

Potrivit art. 6 din Convenţie,

„1. Fiecare parte va adopta măsurile legislative şi alte măsuri necesare pentru a incrimina ca infracţiuni, conform dreptului său intern, atunci când se comit în mod intenţionat şi fără drept:

a) producerea, vânzarea, obţinerea pentru utilizare, importarea, difuzarea sau alte forme de punere la dispoziţie:

(i) a unui dispozitiv, inclusiv un program informatic, conceput special sau adaptat pentru a permite comiterea uneia dintre infracţiunile stabilite în conformitate cu art. 2-5;

(ii) a unei parole, a unui cod de acces sau a unor date informatice similare care să permită accesarea în tot sau în parte a unui sistem informatic, cu intenţia ca acestea să fie utilizate în vederea comiterii uneia dintre infracţiunile vizate la art. 2-5; şi

b) posesia unui element vizat la subparagrafele a) (i) sau a) (ii) sus-menţionate, cu intenţia de a fi utilizat în vederea comiterii uneia dintre infracţiunile vizate la art. 2-5. O parte va putea solicita, în conformitate cu dreptul intern, ca un anumit număr dintre aceste elemente să fie deţinute pentru a fi atrasă răspunderea penală.

2. Prezentul articol nu va fi interpretat în sensul impunerii unei răspunderi penale atunci când producerea, vânzarea, obținerea pentru utilizare, importarea, difuzarea sau alte forme de punere la dispoziție, menționate la paragraful 1 din prezentul articol, nu au ca scop comiterea unei infracțiuni stabilite în conformitate cu art. 2-5, cum ar fi situația testării sau protecției autorizate a unui sistem informatic.

3. Fiecare parte își va putea rezerva dreptul de a nu aplica paragraful 1 al prezentului articol, cu condiția ca această rezervă să nu privească vânzarea, distribuția sau orice altă formă de punere la dispoziție a elementelor menționate la paragraful 1 subparagraful a) (ii) din prezentul articol".

Această dispoziție propune[1] ca infracțiune separată și independentă, săvârșirea intenționată a actelor ilegale specifice, cu privire la anumite dispozitive sau date de acces, pentru a fi utilizate în mod abuziv în scopul comiterii infracțiunilor descrise mai sus (art. 2-5 Convenție) împotriva confidențialității, integrității și disponibilității sistemelor sau datelor informatice. Întrucât comiterea acestor infracțiuni necesită adesea posesia mijloacelor de acces („instrumente de hacker") sau alte instrumente, există un puternic stimulent pentru dobândirea acestora în scopuri criminale care pot duce apoi la crearea unui fel de piața neagră pentru producerea și distribuirea lor. Pentru a combate astfel de pericole mai eficient, legea penală ar trebui să interzică actele specifice potențial periculoase la sursă, înainte de comiterea infracțiunilor prevăzute la articolele 2 - 5.

Această propunere de incriminare a fost una dintre cele mai controversate[2]. Organizațiile internaționale care militează pentru libertatea pe Internet[3] au insistat asupra faptului că propunerea de incriminare și conceptul folosit/folosită nu este suficient de clar/clară pentru a garanta că nu va deveni o bază propriu-zisă pentru investigarea persoanelor angajate în activități legale și că descurajează dezvoltarea unor noi instrumente de securitate, conferind guvernului un rol impropriu de poliție a inovațiilor științifice.

Exemple de *țări* care au *reglementări* introduse în legislația internă *în concordanță* cu dispozițiile art. 6 din Convenție: Austria[4], Croația[5], Italia[6], Sri Lanka[7].

---

[1] Explanatory Report, *op. cit.*, pct. 71.

[2] A se vedea și Baron, R., *op .cit.*, p. 269.

[3] A se vedea și Global Internet Liberty Campaign, *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime*, disponibil on-line la: http://gilc.org/privacy/coe-letter-1000.html (ultima dată accesat la 30.08.2010).

[4] Secț. 126c Cod penal austriac.

[5] Art. 223 alin. 6-7 OG croată 105/04.

[6] Art. 615-quater și 615-quinquies Cod penal italian.

[7] Art. 9 Legea sri lankeză nr. 24/2007.

Multe dintre prevederile naţionale nu acoperă toate acţiunile ilegale incriminate de art. 6 din Convenţie; spre exemplu art. 323-3-1 din Codul penal francez incriminează „importul, deţinerea, oferirea, cedarea sau punerea la dispoziţie, fără motive legitime, a unui echipament, instrument, program informatic sau date concepute sau adaptate special pentru comiterea uneia sau mai multor infracţiuni prevăzute la articolele 323-1 la 323-3".

Nu toate statele asigură incriminarea tuturor „uneltelor" specifice folosite de infractori; marea majoritate incriminează numai producerea sau vânzarea de programe informatice, nu şi deţinerea de dispozitive de acces.

Exemple de *aliniere completă* a dispoziţiilor legislaţiilor interne cu prevederile art. 6 din Convenţie:

- Secţ. 126c („Utilizarea abuzivă a programelor informatice pentru accesarea datelor") din Codul penal austriac, prevede:

„(1) Oricine produce, importă, distribuie, vinde sau face accesibil în vreun fel

1. un program informatic sau un echipament comparabil care a fost evident creat ori adaptat datorită naturii sale particulare pentru a comite un acces ilegal la un sistem informatic (secţ. 118a), o încălcare a secretului telecomunicaţiilor (secţ. 119), o interceptare ilegală a datelor (secţ. 119a), o deteriorare a datelor (secţ. 126a) sau o interferare cu funcţionarea unui sistem informatic (secţ. 126b), sau

2. o parolă, un cod de acces sau date similare care fac posibil accesul la un sistem informatic sau la o parte a acestuia, cu intenţia de a fi utilizate pentru comiterea oricăreia din infracţiunile menţionate la par. 1 …

(2) O persoană nu va fi pedepsită conform prevederilor par. (1) dacă voluntar previne folosirea în scopurile menţionate în paragraful 118a, 119, 119a, 126a sau 126b a programului informatic menţionat la par. (1) sau echipamentul comparabil ori parolei, codului de acces sau datelor similare. Dacă nu există pericolul unei astfel de utilizări sau dacă a fost înlăturat fără vreo acţiune a infractorului, acesta nu va fi pedepsit în cazul când, inconştient de acest lucru, face de bună voie un efort serios pentru înlăturarea pericolului".

- Art. 223, par. 6 din OG croată 105/04 incriminează pe: „Oricine, fără autorizaţie, produce, procură, vinde, deţine ori pune la dispoziţie altei persoane dispozitive speciale, echipamente, programe informatice sau date electronice create sau adaptate pentru săvârşirea infracţiunilor menţionate în paragrafele 1, 2, 3 şi 4 ale acestui articol …".

- Art. 615-quarter („Deţinerea şi difuzarea abuzivă de coduri de acces la sistemele informatice sau de telecomunicaţii") alin. 1 din Codul penal italian incriminează pe „Oricine, în scopul obţinerii unui profit pentru sine sau pentru altul sau producerii altuia unui prejudiciu, în mod abuziv procură, reproduce, difuzează, comunică sau livrează coduri, parole, chei sau alte mijloace pentru

accesarea sistemelor informatice sau de telecomunicaţii, protejate prin măsuri de siguranţă, sau orice fel de indicaţii sau instrucţiuni adecvate acestui scop"; în art. 615-quinquies incriminează pe „Oricine, în scopul deteriorării ilicite a unui sistem informatic sau de telecomunicaţii, a informaţiilor, datelor sau programelor conţinute de acestea sau care le aparţin, sau în vederea întreruperii, totale sau parţiale, sau alterării funcţionării acestuia, procură, produce, reproduce, importă, difuzează, comunică, livrează sau pune la dispoziţie în orice fel altor persoane, echipamente, dispozitive sau programe informatice".

Este recomandabil ca toate ţările să prevadă expres că dispozitivele trebuie să fie special create sau adaptate pentru comiterea infracţiunilor prevăzute de Convenţie la art. 2-5, pentru evitarea unei supra-incriminări.

Secțiunea a IV-a
Analiza comparativă a modului în care au fost incriminate infracțiunile informatice[1]

Articolele 7-10 se referă la infracţiunile obişnuite care sunt frecvent comise prin intermediul unui sistem informatic. Cele mai multe state au incriminat deja aceste infracţiuni obişnuite, iar legile lor existente pot/nu pot fi suficient de cuprinzătoare pentru a acoperi şi situaţiile care implică reţele de calculatoare (de exemplu, legile existente care incriminează pornografia infantilă din unele state nu pot acoperi şi situaţiile în care imaginile sunt în format digitale). Prin urmare, în cursul implementării acestor articole, statele trebuie să-şi analizeze legile existente pentru a stabili dacă acestea se aplică la situaţiile în care sistemele informatice sau reţelele sunt implicate iar în cazul în care infracţiunile existente acoperă deja un astfel de comportament, nu există nicio obligaţie de a modifica infracţiunile existente sau de a adopta altele noi[2].

§ 1. Falsificarea informatică

Potrivit art. 7 din Convenţie,

„Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, introducerea, alterarea, ştergerea sau suprimarea intenţionată şi fără drept a datelor informatice, din care să rezulte date neautentice, cu intenţia ca acestea să fie luate în considerare sau utilizate în scopuri legale ca şi cum ar fi autentice,

[1] Ioniță G. I., *A comparative analysis …, op. cit.*

[2] Council of Europe, *Explanatory Report, op. cit.*, pct. 79.

chiar dacă sunt sau nu sunt în mod direct lizibile şi inteligibile. O parte va putea condiţiona răspunderea penală de existenţa unei intenţii frauduloase sau a unei alte intenţii delictuale".

Scopul[1] acestei propuneri de incriminare este de a crea o infracţiune paralelă cu falsificarea de documente tangibile pentru acoperirea lacunelor în dreptul penal legate de falsificarea tradiţională, care necesită lizibilitatea unui text încorporat într-un document şi care nu se aplică datelor stocate pe suport electronic. Manipularea acestor date cu valoare probatorie poate avea aceleaşi consecinţe grave ca şi actele tradiţionale de fals în cazul în care o terţă parte este astfel indusă în eroare. Falsificarea în legătură cu utilizarea calculatorului implică crearea sau modificarea neautorizată a datelor stocate, astfel încât acestea să dobândească o valoare probatorie diferită în cursul operaţiunilor juridice care se bazează pe autenticitatea informaţiilor conţinute în date şi face obiectul unei înşelăciuni. Interesul legal protejat constă în securitatea şi fiabilitatea datelor informatice care pot avea consecinţe pentru relaţiile juridice.

Conceptul de falsificare informatică variază destul de frecvent în legislaţiile naţionale. Pot fi evidenţiate două concepte diferite de falsificare informatică: primul se bazează pe autenticitatea autorului documentului, în timp ce al doilea se bazează pe veridicitatea conţinutului documentului. Oricum, elementul de bază comun trebuie să fie legat de alterarea autenticităţii şi veridicităţii conţinutului datelor.

Sunt câteva *ţări* care au introdus în legislaţia internă *reglementări în concordanţă* cu dispoziţiile art. 7 din Convenţie; spre exemplu: Austria[2], Croaţia[3], Cipru[4], Italia[5], Macedonia[6], Portugalia[7], Slovacia[8].

Multe dintre legislaţiile naţionale ale unor state ca Albania[9], Armenia[10], Bulgaria[11], Estonia[12], Turcia[13], Ucraina[14] nu acoperă toate activităţile ilegale, aşa

[1] *Ibidem*, pct. 81.
[2] Secţ. 225a Cod penal austriac.
[3] Art. 223a OG croată 105/04.
[4] Art. 9 Legea cipriotă nr. 22(III)/2004.
[5] Art. 491-bis Cod penal italian.
[6] Art. 379-a Cod penal macedonean (Кривичниот законик) disponibil on-line la: http://www.mlrc.org.mk/zakoni/Z1996033.htm (ultima dată accesat la 26.08.2010).
[7] Art. 4 Legea portugheză nr. 109/91.
[8] Art. 247(1)d Cod penal slovac.
[9] Art. 186-189 Cod penal albanez.
[10] Art. 252 Cod penal armean.
[11] Art. 319b şi 319c Cod penal bulgar.
[12] Art. 344 Cod penal eston.
[13] Art. 244 par. 2 Cod penal turc.
[14] Art. 362(1) Cod penal ucrainean.

cum sunt descrise în art. 7 din Convenție; totuși, majoritatea cazurilor de falsificare informatică pot intra sub incidența prevederilor tradiționale.

Unele țări incriminează nu numai modificarea sau alterarea datelor, dar și a programelor. Această deosebire nu pare să fie necesară deoarece programele sunt o parte a conceptului mai larg de date, conform art. 1 lit. b din Convenție.

Foarte puține țări incriminează actul comis cu o intenție calificată; spre exemplu, secț. 269 („Falsificarea datelor juridice relevante") din Codul penal german incriminează „stocarea sau modificarea datelor juridice relevante", în scopul „înșelării în relațiile juridice" printr-un „document contrafăcut sau falsificat".

Modele de *dispoziții naționale aliniate* la dispozițiile art. 7 din Convenție:

- Secț. 225a „Falsificarea datelor", din Codul penal austriac incriminează „(1) O persoană care produce date false prin introducerea, alterarea, ștergerea ori suprimarea datelor ori falsifică date autentice cu intenția de a le utiliza în scopuri juridice ca dovadă a unui drept, relație sau fapt juridic …".

- Art. 223a din OG croată 105/04 incriminează pe „(1) Oricine, fără autorizație, dezvoltă, instalează, alterează, șterge sau face inutilizabile date ori programe care sunt de însemnătate pentru relațiile juridice în scopul de a fi folosite ca autentice, sau oricine folosește astfel de date sau programe"

- Art. 379a „Falsificarea informatică", din Codul penal macedonean incriminează, în par. (1), pe „Acela care fără autorizație va produce, introduce, schimba, șterge sau face inutilizabile, cu intenția de a le utiliza ca fiind reale, date ori programe informatice care sunt determinante sau potrivite pentru a servi ca dovadă a faptelor cu importanță pentru relațiile juridice ori acela care va folosi astfel de date sau programe ca reale"; în par. (2) al aceluiași articol este prevăzută o agravantă „Dacă infracțiunea stipulată la paragraful (1) este săvârșită asupra datelor sau programelor informatice care sunt folosite în activități ale autorităților statului, instituțiilor publice, întreprinderi sau alte persoane fizice sau juridice care desfășoară activități de interes public sau în relații juridice cu țări străine sau dacă se produc prejudicii grave prin utilizarea lor".

Până acum câțiva ani, o mare parte a documentelor aveau o natură tangibilă, dar dezvoltarea noilor tehnologii a determinat, atât în sectorul public cât și în cel privat, o creștere exponențială a documentelor electronice, majoritatea legislațiilor naționale recunoscând aceeași relevanță juridică ca cea a documentelor tradiționale.

Pentru a garanta o desfășurare sigură și corectă a relațiilor economice, sociale și juridice, este recomandabil ca țările care până în prezent nu au o reglementare specifică împotriva falsificărilor informatice, să introducă infracțiuni conform celor prevăzute în art. 7 din Convenție.

De remarcat că, înainte de anul 2001, așa cum a reținut și Curtea Supremă de Casație italiană, Camera a Cincea Penală, prin decizia nr. 11930 din 25 martie 1999[1], în lipsa unei reglementări speciale, instanțele italiene au extins dispoziţiile de drept comun existente (care incriminau falsul) pentru a acoperi situațiile de falsificare a unor documente sau arhive electronice.

§ 2. Frauda informatică

Potrivit art. 8 din Convenție,

„Fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, fapta intenționată și fără drept de a cauza un prejudiciu patrimonial unei alte persoane:

a) prin orice introducere, alterare, ștergere sau suprimare a datelor informatice;

b) prin orice formă care aduce atingere funcționării unui sistem informatic, cu intenția frauduloasă sau delictuală de a obține fără drept un beneficiu economic pentru el însuși sau pentru altă persoană".

Scopul[2] acestei propuneri de incriminare este de a incrimina orice manipulare nejustificată în cursul prelucrării datelor cu intenția de a efectua un transfer ilegal de proprietate. Odată cu revoluția tehnologică, oportunitățile pentru comiterea infracțiunilor economice, cum ar fi frauda (inclusiv frauda cu cărți de credit), s-au multiplicat. Activele reprezentate sau administrate de sistemele informatice (fonduri electronice, depozite de bani) au devenit ținta manipulărilor ca formele tradiționale de proprietate. Aceste infracțiuni constau în principal în manipulări de intrare (în cazul în care datele incorecte sunt introduse în calculator) sau prin manipulări de program și alte interferențe cu cursul de prelucrare a datelor.

Exemple de *țări* care au introdus în legislația internă *reglementări în concordanță* cu dispozițiile art. 8 din Convenție: Austria[3], Cipru[4], Germania[5], Italia[6], Portugalia[7], SUA[8].

---

[1] A se vedea și Sarzana C., *op. cit.*, p. 10.

[2] Council of Europe, *Explanatory Report*, *op. cit.*, pct. 86.

[3] Sect. 148a Cod penal austriac.

[4] Art. 10 Legea cipriotă nr. 22(III)/2004.

[5] Secț. 263a Cod penal german.

[6] Art. 640-ter Cod penal italian.

[7] Art. 221 Cod penal portughez (Código Penal) disponibil on-line la: http://www.aacs.pt/legislacao/codigo_penal.htm (ultima dată accesat la 26.08.2010).

[8] Titlul 18 partea I cap. 47 § 1030(a)(4) și § 1343 Cod penal federal american.

Unele țări ca Albania, Armenia[1], Bulgaria[2], Croația[3], Estonia[4], Lituania[5], Macedonia[6], Ucraina[7], Ungaria[8], cu toate că au ratificat Convenția, nu au acoperit sau implementat adecvat dispozițiile art. 8 din Convenție. Spre exemplu, Codul penal francez nu prevede o incriminare specifică a fraudei informatice. Actele incriminate prin art. 8 din Convenție pot fi încadrate (în parte) în prevederile altor infracțiuni incriminate conform Convenției (cartea III, titlul II, cap. III „Atentatele la sistemele de procesare automată a datelor" art. 323-1 – 323-4 C. pen.) și (în parte) în prevederile altor infracțiuni de drept comun (cartea III, titlul I, cap. III, secț. 1 „Escrocheria" art. 313-1 și 313-2 C. pen.).

Nu toate țările care au introdus infracțiuni privind frauda informatică incriminează toate formele de manipulare comise în cursul procesării datelor. În plus, unele legislații nu reclamă ca actele frauduloase să fie comise „fără drept".

Exemple de *reglementări* din legislațiile naționale *aliniate* dispozițiilor art. 8 din Convenție:

- Secț. 148a „Abuzul fraudulos de procesare a datelor" din Codul penal austriac incriminează: „O persoana care, cu intenția de a se îmbogăți pe sine sau altă persoană în mod ilegal, cauzează un prejudiciu economic proprietății unei alte persoane prin influențarea rezultatelor procesării automatizate a datelor prin modificarea programului, introducerea, alterarea sau ștergerea datelor (secț. 126a, par. 2) ori prin alte interferențe în cursul procesării datelor".

- Art. 10 din Legea cipriotă 22(III)/2004 incriminează „Orice persoană care intenționat și fără autoritate și cu intenția de a înșela cauzează pierderea de proprietate altei persoane prin a. orice introducere, alterare, ștergere ori suprimare a datelor informatice; b. orice interferență cu funcționarea unui sistem informatic; cu intenția de a obține fără drept un beneficiu economic pentru sine sau pentru altă persoană".

- Prin alin. (1) din secț. 263a „Frauda informatică" a Codului penal german este pedepsită „Orice persoană care, cu intenția de a obține un beneficiu material ilegal, pentru sine sau pentru o terță persoană, prejudiciază bunurile altuia prin influențarea rezultatelor unei operațiuni de procesare a datelor prin configurarea incorectă a unui program, utilizarea unor date incorecte sau incomplete,

[1] Art. 252 Cod penal armean.
[2] Art. 212a și 319b(2) Cod penal bulgar.
[3] Art. 224a Cod penal croat.
[4] Art. 213 Cod penal eston.
[5] Art. 182, 196 și 197 Cod penal lituanian.
[6] Art. 251(4-5) Cod penal macedonean.
[7] Art. 190(3) Cod penal ucrainean.
[8] Art. 300/C și 300/E Cod penal ungar.

utilizarea neautorizată a datelor sau altă influenţare neautorizată a ordinii evenimentelor".

- Art. 640-ter „Frauda informatică" din Codul penal italian, incriminează pe „Oricine, alterează în orice mod funcționarea unui sistem informatic sau de telecomunicații sau intervine fără drept în orice mod asupra datelor, informațiilor sau programelor conținute într-un sistem informatic sau de telecomunicații şi prin aceasta obține pentru sine sau altul un profit injust în dauna altuia".

Şi de această dată, de punctat faptul că, încă din anul 1999, aceeaşi Curte Supremă de Casație italiană, Camera a Şasea Penală, prin decizia nr. 3065 din 14 decembrie 1999[1], a stabilit că este infracțiune de înşelăciune şi atunci când activitatea frauduloasă nu se răsfrânge asupra unei persoane, care nu este indus în eroare, ci asupra unui sistem informatic al unei persoane, prin manipularea frauduloasă a acelui sistem, infracțiunea consumându-se în momentul obținerii avantajului injust şi producerii prejudiciului.

Este recomandabil, dat fiind caracterul transnațional al acestei infracțiuni (în special), dar şi frecvența comiterii, ca statele să implementeze în legislațiile naționale prevederile art. 8 din Convenție, pentru a incrimina, în mod unitar, frauda informatică.

Secțiunea a V-a
Analiza comparativă a modului în care au fost incriminate infracțiunile referitoare la conținut[2]

§ 1. Infracțiuni referitoare la pornografia infantilă

Potrivit art. 9 din Convenție,

„1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, următoarele comportamente, atunci când acestea sunt comise în mod intenționat şi fără drept:

a) producerea de materiale pornografice având ca subiect copii, în vederea difuzării acestora prin intermediul unui sistem informatic;

b) oferirea sau punerea la dispoziție de materiale pornografice având ca subiect copii, prin intermediul unui sistem informatic;

c) difuzarea sau transmiterea de materiale pornografice având ca subiect copii, prin intermediul unui sistem informatic;

---

[1] A se vedea şi Sarzana C., *op. cit.*, p. 12.

[2] Ioniță G.I., *A comparative analysis …, op. cit.*

d) fapta de a-şi procura sau de a procura pentru alte persoane materiale pornografice având ca subiect copii, prin intermediul unui sistem informatic;

e) posesia de materiale pornografice având ca subiect copii, într-un sistem informatic sau într-un mijloc de stocare de date informatice.

2. În sensul paragrafului 1 sus-menţionat, termenul materiale pornografice având ca subiect copii desemnează orice material pornografic care reprezintă într-un mod vizual:

a) un minor care se dedă unui comportament sexual explicit;

b) o persoană majoră, prezentată ca o persoană minoră, care se dedă unui comportament sexual explicit;

c) imagini realiste reprezentând un minor care se dedă unui comportament sexual explicit.

3. În sensul paragrafului 2 sus-menţionat, termenul minor desemnează *orice persoană în vârstă de mai puţin de 18 ani*. Totuşi o parte poate solicita o limită de vârstă inferioară, care trebuie să fie de cel puţin 16 ani.

4. O parte îşi va putea rezerva dreptul de a nu aplica, în totalitate sau parţial, paragraful 1 subparagrafele d) şi e) şi paragraful 2 subparagrafele b) şi c)".

Propunerea de incriminare caută[1] să consolideze măsurile de protecţie pentru copii, inclusiv protecţia acestora împotriva exploatării sexuale, prin modernizarea dispoziţiilor de drept penal pentru a circumscrie mai eficient utilizarea sistemelor informatice în comiterea infracţiunilor sexuale împotriva copiilor. Această dispoziţie incriminează diferite aspecte ale producţiei, deţinerea şi distribuirea de materiale de pornografie infantilă electronice. Majoritatea statelor incriminează deja producţia tradiţională şi distribuţia fizică a pornografiei infantile, dar cu utilizarea tot mai mare a Internet-ului ca instrument principal de tranzacţionare a unor astfel de materiale, s-a resimţit tot mai puternic că dispoziţii specifice într-un instrument juridic internaţional sunt esenţiale pentru a combate această nouă formă de exploatare sexuală şi punere în pericol a copiilor. Se consideră că astfel de materiale şi practici on-line, cum ar fi schimbul de idei, fantezii şi consiliere în rândul pedofililor, joacă un rol în sprijinirea, încurajarea sau facilitarea infracţiunilor sexuale împotriva copiilor.

În literatura de specialitate sunt, de asemenea, exprimate păreri[2] conform cărora nu era necesară o asemenea propunere de incriminare întrucât distribuţia şi posesia de materiale pornografice cu minori sunt deja infracţiuni în majoritatea ţărilor, iar definiţiile utilizate în legătură cu pornografia infantilă sunt prea

[1] Council of Europe, *Explanatory Report*, *op. cit.*, pct. 91 şi 93.

[2] A se vedea Taylor, G., *The Council of Europe Cybercrime Convention A civil liberties perspective*, disponibil on-line la: http://www.crime-research.org/library/CoE_Cybercrime.html (ultima dată accesat la 28.08.2010).

generale, deoarece incriminează posesia de imagini a căror producție nu implică copii reali.

Exemple de *țări* care au introdus în legislația internă *reglementări în concordanță* cu dispozițiile art. 10 din Convenție: Austria[1], Cipru[2], Franța[3] Italia[4], Spania[5], SUA[6].

Nu toate statele care au ratificat deja Convenția au acoperit sau implementat în mod adecvat art. 9 din Convenție.

În legislațiile unor țări ca Albania[7], Armenia[8], Croația[9], Franța[10], Lituania[11], Slovacia[12], Turcia[13] nu sunt definiți termenii „pornografie infantilă" și „minor".

Unele state ca Estonia[14], Germania[15], Portugalia[16], stabilesc, pentru ca o persoană să fie considerată minor, vârsta de 16 ani sau mai mică.

Cu toate că art. 9 din Convenție acoperă o listă mai largă de acte care ar trebui incriminate, și precizează în mod expres ca acestea să fie comise prin intermediul unui sistem informatic, doar câteva legislații naționale solicită în mod expres ca infracțiunea să fie comisă prin intermediul acestuia.

Modele de *dispoziții naționale aliniate* la dispozițiile art. 9 din Convenție:

- Art. 227-23 din Codul penal francez, incriminează în primele două alineate „distribuirea, fixarea, înregistrarea sau transmiterea imaginii sau reprezentării unui minor în cazul în care această imagine sau reprezentare are un caracter pornografic", dar și „oferirea, punerea la dispoziție sau distribuirea unei astfel de imagini sau reprezentări, prin orice mijloace"; în alin. 3 și 6 sunt incriminate două forme agravate „atunci când a fost folosită, pentru transmiterea imaginii sau reprezentării unui minor la un public nedeterminat, o rețea de comunicații electronice" și „atunci când sunt comise în bande organizate". Prin alin. 5, incriminarea

---

[1] Secț. 207a Cod penal austriac.

[2] Art. 12(1) Legea cipriotă nr. 22(III)/2004.

[3] Art. 227-23 Cod penal francez.

[4] Art. 600-ter, 600-quater, 600-quinquies Cod penal italian.

[5] Art. 189 Cod penal spaniol (Código Penal) disponibil on-line la: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html (ultima dată accesat la 26.08.2010).

[6] Titlul 18, partea I, cap. 110, § 2252 Cod penal federal american.

[7] Art. 117 Cod penal albanez.

[8] Art. 263 Cod penal armean.

[9] Art. 197 OG croată 105/04.

[10] Art. 227-23 și 227-24 Cod penal francez.

[11] Art. 162 și 309 Cod penal lituanian.

[12] Secț. 368-370 Cod penal slovac.

[13] Art. 226 Cod penal turc.

[14] Art. 177 Cod penal eston.

[15] Secț. 184b Cod penal german.

[16] Art. 172 Cod penal portughez.

depășește scopul art. 9 din Convenție, sancționând chiar și „consultarea obișnuită a unui serviciu de comunicare on-line care pune la dispoziție sau deține prin orice mijloace a unei astfel de imagine sau reprezentări".

- Secț. 184b („Răspândirea, procurarea și deținerea de materiale pornografice implicând minori") din Codul penal german pedepsește în primele două subsecțiuni pe „(1) Oricine în legătură cu materiale pornografice (secțiunea 11, subsecțiunea (3)) ce au ca obiect abuzuri sexuale ale copiilor (secțiunile 176 și 176b) (materiale pornografice implicând minori): 1. răspândește; 2. afișează public, postează, prezintă ori fac în vreun fel accesibile; ori 3. produce, obține, furnizează, stochează, oferă, anunță, comandă sau se angajează să le importe sau să le exporte, pentru a le folosi sau face copii ale acestora în înțelesul numerelor 1 și 2 ori face posibilă o astfel de utilizare de către altcineva" și pe „(2) Oricine se angajează să obțină posesia pentru altcineva a materialelor pornografice implicând copii ce reproduc un eveniment real sau adevărat". În subsecțiunea (3) este incriminată o formă agravată „când autorul acționează pe o bază comercială sau ca membru al unei bande care le-a combinat pentru comiterea neîntreruptă a unor astfel de acte și materiale pornografic implicând copii ce reproduc un eveniment real sau adevărat".

- Art. 600-ter („Pornografia infantilă") din Codul penal italian pedepsește, în alin. 1 și 2, pe „Oricine realizează spectacole pornografice sau produce materiale pornografice utilizând minori de optsprezece ani sau provoacă minorii de optsprezece ani să participe la spectacole pornografice" și pe „cei care comercializează materialele pornografice"; în următoarele două alineate (alin. 3 și 4) sunt incriminate două forme atenuate „Oricine ... prin orice mijloace, chiar și prin telecomunicații, distribuie, divulgă, difuzează sau face publice materiale pornografice ... distribuie sau difuzează știri sau informații finalizate cu ademenirea sau exploatarea sexuală de minori de optsprezece ani" și „Oricine ... oferă sau cedează altora, chiar și cu titlu gratuit, materiale pornografice". Prin art. 600-quater („Deținerea de materiale pornografice") din același cod, este pedepsit „Oricine ... conștient procură sau deține materiale pornografice realizate utilizând minori de optsprezece ani". Potrivit dispozițiilor art. 600-quater.1 („Pornografia virtuală") din același cod, dispozițiile mai sus citate (art. 600-ter și 600-quater) „se aplică chiar și atunci când materialele pornografice reprezintă imagini virtuale realizate utilizând imagini de minori de optsprezece ani sau parte din acestea". Prin art. 600-quinquies („Inițiative turistice în scopul exploatării prostituției infantile") din același cod, legislația italiană depășește scopul art. 9 din Convenție incriminând pe „Oricine organizează sau face propagandă pentru călătorii finalizate cu activități de prostituție în dauna minorilor".

Este de dorit ca toate țările să adopte o definiție comună pentru termenii de „minor" și „pornografie infantilă".

În plus, ar trebui luată în considerație și incriminarea posesiei, ofertării, punerii la dispoziție, distribuirii, transmiterii sau procurării de materiale pornografice care descriu „o persoană ce pare a fi minor angajată în activități sexuale" sau „imagini realiste reprezentând un minor angajat în activități sexuale".

Secțiunea a VI-a
Analiza comparativă a modului în care au fost incriminate infracțiunile referitoare la atingerile aduse proprietății intelectuale şi drepturilor conexe[1]

Potrivit art. 10 din Convenție,

„1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, atingerile aduse proprietății intelectuale, definite de legislația acestei părți, în conformitate cu obligațiile pe care le-a subscris în aplicarea Actului de la Paris din 24 iulie 1971 care revizuiește Convenția de la Berna pentru protecția operelor literare şi artistice, a Acordului privind aspectele comerciale ale drepturilor de proprietate intelectuală şi a Tratatului OMPI privind proprietatea intelectuală, cu excepția oricărui drept moral conferit de aceste convenții, atunci când astfel de acte sunt comise deliberat, la scară comercială şi prin intermediul unui sistem informatic.

2. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, atingerile aduse drepturilor conexe definite de legislația acestei părți în conformitate cu obligațiile pe care le-a subscris în aplicarea Convenției internaționale pentru protecția artiştilor interpreți sau executanți, a producătorilor de fonograme şi a organismelor de radiodifuziune (Convenția de la Roma), a Acordului privind aspecte comerciale ale drepturilor de proprietate intelectuală şi a Tratatului OMPI privind interpretările şi fonogramele, cu excepția oricărui drept moral conferit de aceste convenții, atunci când astfel de acte sunt comise deliberat, la scară comercială şi prin intermediul unui sistem informatic.

3. O parte va putea, în circumstanțe bine delimitate, să îşi rezerve dreptul de a nu impune răspunderea penală în baza paragrafelor 1 şi 2 ale prezentului articol, cu condiția ca alte recursuri eficiente să fie disponibile şi cu condiția ca o astfel de rezervă să nu aducă atingere obligațiilor internaționale care incumbă acestei părți în aplicarea instrumentelor internaționale menționate la paragrafele 1 şi 2 ale prezentului articol".

---

[1] Ioniță G.I., *A comparative analysis …, op. cit.*

Încălcări ale drepturilor de proprietate intelectuală, în special a dreptului de autor, sunt printre cele mai frecvente infracţiuni comise pe Internet, care produc îngrijorare atât pentru titularii drepturilor de autor şi celor care lucrează cu reţele de calculatoare. Reproducerea şi difuzarea pe internet a operelor protejate (literare, fotografice, muzicale, audio-vizuale etc.), fără acordul deţinătorului drepturilor de autor, sunt extrem de frecvente. Uşurinţa cu care pot fi făcute copii neautorizate datorită tehnologiei digitale şi amploarea reproducerii şi difuzării în cadrul reţelelor a făcut necesară includerea unor dispoziţii în dreptul penal şi consolidarea cooperării internaţionale în acest domeniu[1].

Cu toate acestea se susţine[2] în literatura de specialitate că acest articol (art. 10 din Convenţie) nu-şi are locul aici, întrucât protecţia proprietăţii intelectuale este o problemă complicată care atinge ambele probleme, libera exprimare şi viaţa privată, şi în care legea este încă în curs de dezvoltare; în plus, există alte foruri internaţionale, în care aceste aspecte sunt abordate într-un mod mai corespunzător.

Exemple de *ţări* care au introdus în legislaţia internă *reglementări în concordanţă* cu dispoziţiile art. 10 din Convenţie: Albania[3], Armenia[4], Cipru[5], Franţa[6], Germania[7], Italia[8], SUA[9].

Reglementările interne pentru protecţia drepturilor de autor şi a drepturilor conexe nu fac trimitere la sistemul informatic, ca mijloc de comitere a infracţiunilor. Doar câteva ţări, ca Armenia[10], Cipru[11], prevăd în legislaţia internă, în mod expres, ca aceste infracţiuni să fie comise prin intermediul unui sistem

---

[1] Council of Europe, *Explanatory Report*, *op. cit.*, pct. 107.

[2] A se vedea Taylor, G., *op. cit*.

[3] Art. 148-149 Cod penal albanez art. 13 şi 75-83 Legea albaneză cu privire la drepturile de autor şi drepturile conexe (Ligj nr. 9380, datë 28.04.2005 për të drejtën e autorit dhe të drejtat e tjera, të lidhura me të) disponibil on-line la: http://www.zshda. gov.al/kuadriligjor/ligji.doc (ultima dată accesat la 26.08.2010).

[4] Art. 158 Cod penal armean.

[5] Art. 12 Legea cipriotă nr. 22(III)/2004.

[6] Art. L112-1 şi L112-1 Cod proprietate intelectuală francez (Code de la propriété intellectuelle) disponibil on-line la: http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069414 (ultima dată accesat la 26.08.2010).

[7] Secţ. 106 Legea germană cu privire la drepturile de autor şi drepturile conexe (Gesetz über Urheberrecht und verwandte Schutzrechte) disponibil on-line la: http://www.gesetze-im-internet.de/urhg/index.html (ultima dată accesat la 26.08.2010).

[8] Art. 171-bis, 171-ter, 171-octies, 174-ter Legea italiană cu privire la drepturile de autor şi drepturile conexe nr. 633/1941 (Legge 22 aprile 1941, n. 633, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio) disponibil on-line la: http://www.altalex.com/index.php?idstr=12&idnot=34610 (ultima dată accesat la 28.08.2010).

[9] Titlul 17, cap. 5, § 506 şi titlul 18, partea I, cap. 47, § 2319 Cod penal federal american.

[10] Art. 158 Cod penal armean.

[11] Art. 12 Legea cipriotă nr. 22(III)/2004.

informatic. Cu toate acestea, folosirea unor expresii generale ca „în vreun fel" sau „în orice alt mod", în legislația internă a unor țări ca: Bulgaria[1], Croația[2], Turcia[3], Ungaria[4], ar putea extinde aplicabilitatea prevederilor și acoperi (astfel) dispozițiile art. 10 din Convenție.

Însă, nici o țară nu pare să condiționeze conduita, ca acestea să fie comise la scară comercială. Doar Germania, spre exemplu, prevede în art. 108a („Exploatarea neautorizată la scară comercială") din Legea cu privire la drepturile de autor și drepturile conexe, ca o variantă agravantă, situația „când persoana comite actele la care se referă secțiunile 106-108 la scară comercială". Alte țări, ca Cipru[5], Estonia[6], Lituania[7], condiționează incriminarea de comiterea acestor acte „în scopuri comerciale".

Exemple de *dispoziții* ale legislațiilor naționale *în concordanță* cu prevederile art. 10 din Convenție:

- Secț. 106 („Exploatarea neautorizată a lucrărilor protejate") din Legea germană cu privire la drepturile de autor și drepturile conexe, incriminează pe „(1) Oricine reproduce, distribuie ori comunică public o lucrare sau o adaptare ori transformare a lucrării, într-o altă manieră decât cea permisă de lege și fără permisiunea deținătorului drepturilor", iar secț. 108 („Încălcarea drepturilor conexe") din aceeași lege, incriminează pe „(1) Oricine, într-o altă manieră permisă de lege și fără permisiunea deținătorului drepturilor:

1. reproduce, distribuie ori comunică public o ediție științifică (secțiunea 70) sau o adaptare ori transformare a unei astfel de ediții

2. exploatează o operă postumă sau o adaptare ori transformare a unei astfel de opere contrar secțiunii 71

3. reproduce, distribuie ori comunică public o fotografie sau o adaptare ori transformare a fotografiei …

5. exploatează o înregistrare audio contrar secțiunii 85

6. exploatează o difuzare contrar secțiunii 87

7. exploatează un film ori o înregistrare video și audio contrar secțiunii 94 sau secțiunii 95 coroborată cu secțiunea 94

8. folosește o bază de date contrar secțiunii 87b (1)".

---

[1] Art. 172a Cod penal bulgar.

[2] Art. 230 OG croată 110/97.

[3] Art. 72-73 Legea turcă cu privire la operele intelectuale și artistice nr. 5846/1951 (Fikir Ve Sanat Eserleri Kanunu) disponibil on-line la: http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.3.5846&MevzuatIliski=0&sourceXmlSearch= (ultima dată accesat la 28.08.2010).

[4] Art. 329/A și 329/C Cod penal ungar.

[5] Art. 12 Legea cipriotă nr. 22(III)/2004.

[6] Art. 223 și 225 Cod penal eston.

[7] Art. 192 Cod penal lituanian.

Secț 108b („Interferența neautorizată cu măsurile tehnice de protecție și informații necesare managementului drepturilor") din aceiași lege incriminează pe

(1) Orice persoană care,

1. cu intenția de a permite accesul la ori utiliza o operă protejată de această lege sau alte materii protejate de această lege, eludează o măsură tehnică efectivă fără permisiunea deținătorului drepturilor sau

2. cu bună știință fără autorizație

a) elimină sau modifică informațiile de management a drepturilor provenite de la titularii de drepturilor, dacă oricare din aceste informații este aplicată reproducerii unei opere ori altei materii protejate sau este publicată în legătură cu o comunicare publică a unei astfel de opere sau materii protejate, sau

b) diseminează, pregătește diseminarea, transmite, comunică public sau face disponibil publicului o operă sau altă materie protejată când informațiile de management a drepturilor au fost eliminate sau modificate fără autorizație și astfel cel puțin prin imprudență induce, permite, facilitează ori ascunde încălcarea drepturilor de autor sau drepturilor conexe, dacă infracțiunea nu a fost comisă pentru uzul privat exclusiv al făptuitorului ori persoanei asociată personal cu făptuitorul sau nu este legată de o astfel de utilizare

(2) … orice persoană care, încălcând secțiunea 95a subsecțiunea (3), produce, importă, diseminează, vinde ori închiriază un echipament, produs ori component în scopuri comerciale

(3) Când o persoană comite actele la care se referă subsecțiunea (1) la scară comercială"

- Art. 12, alin. 1 din Legea cipriotă 22(III)/2004, incriminează „Orice persoană care înfăptuiește intenționat în scopuri comerciale orice act prin intermediul unui sistem informatic care potrivit Legii privind proprietatea intelectuală și drepturile conexe din 1976 încalcă dreptul de proprietate intelectuală sau drepturile conexe".

- Art. 171-bis din Legea italiană nr. 633/1941 pedepsește pe „1. Oricine în mod abuziv multiplică, pentru profit, programe sau în același scop importă, distribuie, vinde, deține în scop comercial sau de afaceri ori leasing programe conținute pe suporturi nemarcate de Societatea italiană a autorilor și editorilor (SIAE) … prin orice mijloace urmărește doar permiterea sau facilitarea eliminării arbitrare sau eludarea funcționării dispozitivelor pentru protejarea unui program … 2. Oricine, pentru profit, pe suporturi care nu sunt marcate de SIAE reproduce, transferă pe un alt suport, distribuie, comunică, prezintă sau expune în public conținutul unei baze de date încălcând dispozițiile articolelor 64-quinquies și 64-sexies, sau efectuează extragerea ori reutilizarea bazei de date încălcând dispozițiile articolelor 102-bis și 102-ter, sau distribuie, vinde sau închiriază o bancă de date". Art. 171-ter din aceiași lege incriminează

„1. … atunci când fapta este comisă pentru uzul nepersonal … în scop lucrativ:

a) în mod abuziv multiplică, reproduce, transmite ori distribuie în public prin orice mijloc, în tot sau în parte, o operă intelectuală destinată televiziunii, cinematografiei, vânzării ori închirierii, discuri, casete ori suporturi analoge sau orice alte suporturi care conţin înregistrări audio sau video a operelor muzicale, cinematografice ori audiovizuale asimilate sau secvenţe de imagini în mişcare;

b) în mod abuziv reproduce transmite sau difuzează în public, prin orice mijloc, opere ori părţi din opere literare, dramatice, ştiinţifice ori didactice, muzicale ori dramatico-muzicale, sau multimedia, chiar dacă sunt incluse în opere colective ori compuse sau în bănci de date;

c) … introduce pe teritoriul ţării, deţine pentru vânzare ori distribuire, sau distribuie, pune în vânzare, închiriază sau dispune în orice alt mod cu orice titlu, proiectează în public, transmite prin intermediul televiziunii prin orice mijloc, difuzează audio în public multiplicările ori reproducerile abuzive menţionate la literele a) şi b);

d) deţine pentru vânzare sau distribuire, pune în vânzare, vinde, închiriază sau dispune cu orice titlu, proiectează în public, transmite prin intermediul radioului sau televiziunii prin orice mijloc, casete video, casete audio, orice suport care conţine înregistrări audio ori video ale operelor muzicale, cinematografice ori audiovizuale sau secvenţe de imagini în mişcare, sau alte suporturi pentru care este prevăzută, în sensul prezentei legi, aplicarea marcajului Societăţii italiene a autorilor şi editorilor (SIAE), lipsite de acelaşi marcaj ori cu marcaje falsificate sau modificate;

e) în lipsa unui acord cu distribuitorul legitim, retransmite sau difuzează prin orice mijloace un serviciu criptat recepţionat prin intermediul aparatelor sau părţilor din aparatele pentru decodarea transmisiunilor cu acces condiţionat;

f) introduce pe teritoriul ţării, deţine pentru vânzare ori distribuire, distribuie, vinde, închiriază sau dispune cu orice titlu, promovează, instalează dispozitive ori elemente de decodificare speciale care să permită accesul la un serviciu criptat fără plata taxei datorate;

f-bis) produce, importă, distribuie, vinde, închiriază, dispune cu orice titlu, promovează pentru vânzare ori închiriere, sau deţine în scopuri comerciale, echipamente, produse ori componente sau prestează servicii … eludarea măsurilor tehnologice eficace prevăzute la art. 102-quarter sau sunt proiectate, produse, adaptate ori realizate în scopul de a permite şi facilita eludarea unor astfel de măsuri …

h) în mod abuziv elimină sau modifică informaţiile electronice prevăzute la articolul 102-quinquies, sau distribuie, importă pentru distribuire, difuzează prin radio ori televiziune, comunică sau pune la dispoziţia publicului opere ori

alte materiale protejate de la care au fost eliminate sau modificate aceleaşi informaţii electronice.

2. … oricine

a) reproduce, multiplică, transmite ori difuzează abuziv, vinde sau introduce în alt mod în comerţ, dispune cu orice titlu ori importă abuziv peste cincizeci de copii sau exemplare de opere protejate de drepturi de autor sau alte drepturi conexe;

a-bis) prin încălcarea art. 16, în scop lucrativ, comunică publicului printr-un sistem de reţele telematice, prin intermediul conexiunilor de orice fel, o operă protejată de dreptul de autor, sau o parte din aceasta;

b) exercită sub formă de afacere a reproducerii, distribuirii, vânzării ori comercializării, importării operelor protejate de drepturi de autor sau de drepturi conexe …

c) promovează sau organizează activităţile ilicite menţionate la alineatul 1".

Este de dorit incriminarea penală a încălcării drepturilor de autor prin intermediul sistemelor informatice în maniera propusă de art. 10 din Convenţie deoarece s-ar putea evita incriminarea reproducerii fişierelor făcută de utilizatorii privaţi de Internet. În aceste cazuri ar putea fi aplicate sancţiuni mai uşoare – cum ar fi sancţiunile civile sau administrative – sau ar putea fi implementate remedii eficiente – cum ar fi mecanisme tehnice noi – în scopul prevenirii copierii şi difuzării ilegale a acestor reproduceri.

Capitolul IV

Puncte de vedere exprimate în literatura şi doctrina de specialitate cu privire la metodele, tehnicile şi procedurile de cercetare a infracțiunilor din sfera criminalității informatice

Secțiunea I
Considerații generale

Problematica cercetării/investigării infracţiunilor din sfera criminalității informatice, procedurile care trebuie urmate, activitățile care trebuie desfăşurate, paşii care trebuie parcurşi este încă în faza dezbaterilor.

Este firesc, dat fiind caracteristicile acestei forme de manifestare a criminalităţii dar şi faptului că este relativ recentă, să mai dureze până când aceste activităţi să se cristalizeze şi să fie general acceptate.

Secțiunea a II-a
Principalele modele de cercetare a infracțiunilor din sfera criminalității informatice prezentate în literatura de specialitate[1]

În literatura de specialitate sunt prezentate mai multe puncte de vedere cu privire la cercetarea infracţiunilor din sfera criminalităţii informatice.

Primele modele şi proceduri dezvoltate nu sunt nici coerente şi nici standardizate; se accentuează detaliile tehnice în dauna procesului general de investigare.

În continuare, am să prezint cele mai semnificative şi mai des citate modele dezvoltate în domeniu.

§ 1. Pollit M. Mark, Paradigma digitală[2]

Unul dintre primele modele care descrie procesul de obţinere a dovezilor digitale a fost prezentat, de către Mark M. Pollit (la acea dată agent special în cadrul

---

[1] Ioniță G. I., *Principalele modele de cercetare a infracțiunilor din sfera criminalității informatice prezentate în literatura de specialitate*, în volumul „Instituţii juridice contemporane în contextul integrării României în Uniunea Europeană" ed. a IV-a, Editura Pro Universitaria, Bucureşti, 2010, p. 515-527.

[2] Pollit M. M., *Computer Forensics: An Approach to Evidence in Cyberspace*, în The Proceedings of the 18th National Information System Conference, vol. II, Baltimore, MD, (oct.) 1995, p. 487-491, disponibil on-line la http://www.digitalevidencepro.com/Resources/Approach.pdf (ultima dată accesat la 19.09.2010).

US FBI), la a 18-a Conferință Națională pentru Securitatea sistemelor Informatice (fosta Conferință Națională de Securitate a Computerelor)[1] convocată la sediul din Baltimore în perioada 10-13 octombrie 1995.

Autorul prezintă câteva exemple de activități infracționale clasice în care dovezi importante au fost găsite în calculatoarele autorilor și consideră[2] că „Organele de aplicare a legii și înfăptuire a justiției se confruntă cu o nouă provocare ... Este important ca profesioniștii securității calculatoarelor să fie conștienți de unele dintre cerințele sistemului juridic și să înțeleagă domeniul de dezvoltare a criminalisticii digitale".

El definește[3] criminalistica digitală ca fiind aplicarea științei și ingineriei, problemelor juridice ale dovezilor digitale" și consideră[4] că „Este o sinteză a științei și a dreptului. La o extremă este pură știință de unu și zero ... La cealaltă extremă este curtea de judecată".

Procesul de obținere a dovezilor consideră[5] că „... poate fi rezumat după cum urmează: achiziție → identificare → evaluare → admitere ca dovezi", iar „calea" obținerii dovezilor digitale poate fi descrisă după cum urmează[6] „mediu de stocare (context material) → date (context logic) → informații (context legal) → dovezi".

Este uimitoare capacitatea de sintetizare a unui proces extrem de complex: obținerea informațiilor și transformarea acestora în mijloace de probă.

La fel de surprinzătoare este și concluzia[7] pe care acesta o desprinde în final și care este la fel de actuală în prezent (după 14 ani) „În timp ce legea va evolua încet și acceptă din ce în ce mai multe chestiuni tehnice, specialiștii criminaliști digitali vor continua procesul de pregătire pentru toate părțile implicate în proces (legal n.n.)".

§ 2. Farmer Dan, Venema Wietse, Analiza criminalistică a computerelor UNIX[8]

Farmer și Venema au susținut, pe 06.08.1999, o prelegere despre analiza criminalistică a computerelor cu sistem de operare UNIX sponsorizată de Centrul de Cercetări T.J. Watson[9] din cadrul IBM.

---

[1] The 18th National Information Systems Security Conferrence la http://www.ieee-security.org/Cipher/ConfReports/Conf-rep-Niss95.html.

[2] Pollit M. M., *Computer Forensics ...*, *op. cit.*, p. 487.

[3] *Ibidem*, p. 488.

[4] *Ibidem*.

[5] *Ibidem*, p. 489.

[6] *Ibidem*, p. 450.

[7] *Ibidem*, p. 451.

[8] Farmer D., Venema W., *UNIX Computer Forensics Analysis*, 1999, disponibil on-line la http://www.porcupine.org/forensics/handouts.html (ultima dată accesat la 19.09.2010).

[9] IBM T.J. Watson Research Center, http://www.watson.ibm.com/index.shtml.

În prezentarea „Crimă pe Internet Express”[1] propun ca „Atunci când ne confruntăm cu o situație ...

- Asigură și izolează
- Înregistrează scena
- Efectuează o căutare sistematică de dovezi
- Colectează și ambalează dovezile
- Menține lanțul custodiei”.

Cu toate că aceste recomandări au caracter general fiind formulate pentru „detectivii digitali”, restul prelegerii este centrată pe specificul platformelor UNIX.

În fapt, lipsa instrumentelor de programare specifică platformelor UNIX, i-au determinat să creeze propria suită de utilizare cunoscută drept „Coroner`s Toolkit”[2] pentru realizarea activităților specifice, cu accent pe căutarea sistematică și analiza criminalistică a dovezilor.

Cu toate acestea, conceptul lor despre investigarea criminalistică, cât și explicațiile prezentate mai sus descrise pot fi abstractizate pentru a fi aplicabile sistemelor informatice, în general.

§ 3. Primul Atelier de lucru de cercetare criminalistică digitală (DFRWS), Procesul de investigație în raport cu știința criminalistică digitală

În perioada 7-8 august 2001 a fost ținut în Utica, primul Atelier de lucru anual de cercetare criminalistică digitală, la care au participat pe 50 cercetători universitari, examinatori criminaliști ai computerelor și analiști. Acest prim atelier de lucru a avut ca obiective crearea unei comunități de persoane interesate și inițierea unui dialog semnificativ pentru definirea domeniului și identificarea dificultăților și provocărilor (de înaltă prioritate) care se află în față.

Principalul scop a fost **stabilirea unei comunități de cercetare** care să aplice metode științifice concentrate pe găsirea la termen a soluțiilor comandate de cerințele practicienilor și abordarea necesităților pe termen mai lung, luând în considerare, dar nefiind constrânse de, paradigmele curente.

Două *realizări majore* ale acestui prim atelier de lucru trebuie precizate:
- definirea conceptului „știință criminalistică digitală” și
- stabilirea „procesului de investigație în raport cu știința criminalistică digitală”.

---

[1] Farmer D., Venema W., *Murder on the Internet Express*, 1999, p. 11, disponibil on-line la http://www.neoprag.com/dcm/Murder_on_the_Internet_Express.pdf (ultima dată accesat la 10.11.2010).

[2] The Coroner`s Toolkit (TCT), disponibil on-line la http://www.porcupine.org/forensics/tct.html.

Astfel, *știința criminalistică digitală* a fost ***definită***[1] ca fiind „utilizarea metodelor derivate și dovedite științific față de conservarea, colectarea, validarea, identificarea, analiza, interpretarea, documentarea și prezentarea dovezilor digitale provenite din surse digitale în scopul facilitării sau continuării construcției evenimentelor descoperite ca fiind penale, sau ajutării anticipării acțiunilor neautorizate arătate ca fiind perturbatoare pentru operațiunile planificate".

Procesul de investigație în raport cu știința criminalistică digitală, stabilit conform definiției formulate, ***cuprinde***[2] 7 categorii majore sau clase de activități[3] și mai multe tehnici sau metode propuse pentru fiecare dintre acestea:

a) *identificare*:
- detectare a evenimentului/infracțiunii;
- rezolvare a semnăturii;
- detectare a profilului;
- detectare a anomaliilor;
- plângere;
- monitorizare a sistemului;
- analiză de audit.

b) *conservare*:
- management de caz;
- tehnologii pentru duplicare;
- lanț de custodie;
- sincronizare a timpului.

c) *colectare*:
- conservare;
- metode aprobate;
- programe aprobate;
- echipamente (componente) aprobate;
- autoritate legală;
- reducere a pierderilor;
- prelevare de probe;
- compresie a datelor;
- tehnici de recuperare.

d) *examinare*:
- conservare;
- trasabilitate;
- tehnici de validare;

---

[1] Digital Forensic Research Workshop (DFRWS), *A Road Map*…, *op. cit.*, p. 16.

[2] *Ibidem*, p. 17, tabelul 2 - Procesul de investigație în raport cu știința criminalistică.

[3] Descrierea claselor din model este preluată din teza de doctorat „*Structured Investigation of Digital Incident in Complex Computing Environments*" (nepublicată) a lui Peter Peterson susținută la Oxford Broakes University, Oxford, UK.

- tehnici de filtrare;
- potrivire a modelului;
- descoperire a datelor ascunse;
- extragere a datelor ascunse.

e) *analiză*:
- conservare;
- trasabilitate;
- statistic;
- protocoale;
- extragere a modelului ascuns din date;
- linie a timpului;
- legătură;
- spațial.

f) *prezentare*:
- documentare;
- mărturie a expertului;
- clasificare;
- declarație de impact a misiunii;
- contramăsuri recomandate;
- interpretare statistică.

g) *decizie.*

De precizat, de asemenea, că multe dintre celelalte modele/proceduri dezvoltate ulterior au avut ca bază categoriile/clasele mai sus descrise şi au fost concepute/prezentate pentru/la celelalte ateliere de lucru desfăşurate anual, în diverse locații, din 2001 până în prezent.

§ 4. Reith Mark, Carr Clint, Gunsch Gregg, Un model criminalistic digital abstract[1]

Autorii, în formularea modelului propus, consideră[2], după ce amintesc unele modele sau proceduri, că „...există paşi comunicare care pot fi definiți abstract pentru a produce un model care este independent de o tehnologie anume sau de o infracțiune electronică". Modelul propus de aceştia poate fi considerat o extindere a modelului DFRWS (modelul dezvoltat de primul Atelier de lucru de Cercetare Criminalistică Digitală) din moment ce se inspiră din el, aşa cum de altfel, precizează şi autorii.

---

[1] Reith M., Carr C., Gunsch G., *An Examination of Digital Forensic Models*, International Journal of Digital Evidence, vol. 1, nr. 3, (sept) 2002, disponibil on-line la http://www.utica.edu/academic/Institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf (ultima dată accesat la 19.09.2010).

[2] *Ibidem*, p. 6.

Componentele cheie ale modelului, includ:

- identificare, ce presupune recunoaşterea incidentului, pe baza indicatorilor şi stabilirea tipului său;

- pregătire, ce presupune pregătirea instrumentelor, tehnicilor, mandatelor de percheziţie şi autorizaţiilor de monitorizare, dar şi sprijin de management;

- formulare a unei strategii, ce presupune formularea unei strategii dinamice bazate pe impactul potenţial cu privire la standardele şi specificul tehnologiei în cauză;

- conservare, ce presupune izolarea, asigurarea şi conservarea stării dovezilor materiale şi digitale;

- colectare, ce presupune înregistrarea scenei fizice a infracţiunii şi duplicare a dovezilor digitale folosind procedurile standardizate şi acceptate;

- examinare, ce presupune o căutare sistematică şi aprofundată de dovezi în legătură cu infracţiunea respectivă;

- analiză, ce presupune determinarea semnificaţiei, reconstrucţia fragmentelor de date şi conturarea unor concluzii pe baza dovezilor găsite;

- prezentare, ce presupune formularea unui rezumat şi furnizarea de explicaţii pentru concluziile desprinse;

- returnare a dovezilor, ce presupune asigurarea că bunurile materiale şi datele digitale sunt returnate deţinătorului real şi, de asemenea, stabilirea căror dovezi şi a modalităţii de înlăturare.

Modelul propus prezintă unele avantaje şi dezavantaje, de altfel, relevate[1] chiar de autori.

Printre *avantaje*, de precizat: o metodologie generală ce poate fi utilizată de organele judiciare în legătură cu tehnologiile respective şi posibilitatea, integrării unor tehnologii non-digitale în cadrul modelului.

Printre *dezavantaje*, se numără şi formularea prea generală pentru a putea fi folosită în practică.

§ 5. Gordon R. Gary, Hosmer D. Chet, Siedma Christine, Rebovich Dan, Metodologia investigării criminalistice digitale[2]

Autorii au prezentat în ianuarie 2003 un raport intitulat „Evaluarea tehnologiei, metodelor şi informaţiei pentru comiterea şi combaterea criminalităţii informatice", al unui studiu sponsorizat de Institutul Naţional de justiţie al SUA, prin grantul nr. 2000-9614-NY-IJ.

---

[1] *Ibidem*, p. 9-10.

[2] Gordon G. R., Hosmer C. D., Siedma C., Rebovich D., *Assesing Technology, Methods and Information for Commiting and Combating CyberCrime*, disponibil on-line la http://www.ncjr.gov/pdffiles1/nij/grants/198421.pdf (ultima dată accesat la 19.09.2010).

Raportul este foarte bine documentat, atât teoretic, cât şi practic, este structurat în trei mari teme, în care sunt evaluate atât instrumentele utilizate de infractori în comiterea infracţiunilor din sfera criminalităţii informatice (tema 1), cât şi tehnologiile disponibile pentru organele de aplicare a legii (tema 2), dar şi decalajul între tehnologiile existente şi nevoile prezente şi viitoare ale organelor de aplicare a legii pentru combaterea criminalităţii informatice (tema 3).

În cadrul temei 2 este prezentată şi ***metodologia*** (actuală, la acea dată) investigării unui calculator suspectat de a fi implicat într-o infracţiune, care include[1]:

- *identificarea surselor de dovezi;*
- *conservarea dovezilor;*
- *extragerea dovezilor;*
- *examinarea/analizarea dovezilor;*
- *organizarea/raportarea rezultatelor*.

Cu toate că autorii precizează că metodologia descrisă mai sus se aplică atât infracţiunilor considerate tradiţionale, cât şi celor considerate netradiţionale, meritul deosebit al acestora este că identifică 3 proceduri specifice investigării criminalistice a computerelor, a incidentelor şi a reţelelor, cât şi a activităţilor şi instrumentelor specifice fiecăreia.

a) În ce priveşte ***investigarea criminalistică a computerelor***, autorii consideră[2] că sunt 4 „paşi" care trebuie parcurşi, „paşi" care sunt folosiţi atât în investigarea infracţiunilor „tradiţionale", cât şi în investigarea „post-mortem" a sistemelor compromise, şi care includ:

- *colectarea şi conservarea;*
- *extragerea;*
- *examinarea;*
- *organizarea*.

b) În ce priveşte ***investigarea criminalistică a incidentului***, autorii consideră[3] că aceasta implică investigarea unui compromis sau atac care a avut loc într-un sistem şi că, în legătură cu această analiză, există două abordări:

- *analiza sistemului activ*, care include ca etape: colectarea dovezilor volatile, documentarea proceselor care rulează, listarea porturilor deschise şi detectarea instrumentului folosit pentru atacarea sistemului;

- *analiza sistemului inactiv*, care[4] „... foloseşte aceeaşi metodologie de bază asociată cu procesul investigării criminalistice a computerului, dar cu un set diferit de obiective, acestea fiind identificarea şi recuperarea fişierelor şi proceselor sistemului modificate".

---

[1] *Ibidem*, p. 42.
[2] *Ibidem*, p. 44.
[3] *Ibidem*, p. 71.
[4] *Ibidem*.

c) În ce privește ***investigarea criminalistică a rețelei***, autorii consideră[1] că „pașii", care trebuie parcurși în încercarea identificării sursei unui atac sau compromis, includ:

- *analiza traficului;*
- *analiza conținutului pachetelor, reconstruirea sesiunii;*
- *analiza jurnalelor sistemului și parafocului;*
- *analiza sistemelor de detectare a pătrunderii;*
- *urmărirea;*
- *corelarea informațiilor descoperite*.

Trebuie subliniate meritele autorilor în ce privește documentarea și explicarea activităților și instrumentelor prezentate, care au menirea „... de a reduce discrepanțele de abilități dintre ceea ce infractorii digitali au învățat pentru a comite cu succes infracțiunile și ceea ce organele de aplicare a legii trebuie să cunoască pentru a aduce cu succes acești infractori în fața justiției".

§ 6. Carrier Brian, Spafford H. Eugene, Un proces integrat de investigație digitală[2]

Pentru argumentarea modelului propus, la început, autorii prezintă 3 modele: un model de răspuns la incident (Prosise și Mandia), un model al autorității de aplicare a legii (US Departament of Justice) și un model abstract care s-ar aplica ambelor (US Air Force), apoi prezintă etapele clasice ale investigației scenei infracțiunii.

Ei folosesc multe dintre fazele descrise de modelele pe care le prezintă, dar abordează problema dintr-un alt punct de vedere, considerând „... calculatorul ca fiind el însuși o scenă a infracțiunii, denumită scenă digitală a infracțiunii"[3], iar teoria investigației scenei materiale a infracțiunii este aplicată investigației digitale.

Procesul rezultat este descris în 17 faze organizate în 5 grupe:

– ***faza pregătirii scenei materiale a infracțiunii***, care include: faza pregătirii operațiunilor scenei materiale a infracțiunii și faza pregătirii infrastructurii scenei materiale a infracțiunii;

– ***faza desfășurării scenei materiale a infracțiunii***, care include: faza detectării și notificării și faza confirmării și autorizării;

– ***faza investigării scenei materiale a infracțiunii***, care include: faza conservării scenei materiale a infracțiunii, faza studierii scenei materiale a infracțiunii,

---

[1] *Ibidem*, p. 79.

[2] Carrier B., Spafford Eugene H., *Getting Physical with the Digital Investigation Process*, International Journal of Digital Evidence, vol.2, nr.2, (toamna) 2003, disponibil on-line la http:// www.utica.edu/academic/institutes/ecii/publications/articles/AOAC5A7AFB6C-325D-BF515A44FDEE7459. pdf (ultima dată accesat la 19.09.2010).

[3] *Ibidem*, p. 5.

faza documentării scenei materiale a infracţiunii, faza căutării şi colectării dovezilor materiale, faza reconstrucţiei „scenei materiale a infracţiunii" şi faza prezentării unei „teorii complete" scenei materiale a infracţiunii;

– ***faza investigării scenei digitale a infracţiunii***, care include: faza conservării scenei digitale a infracţiunii, faza studierii scenei digitale a infracţiunii, faza documentării scenei digitale a infracţiunii, faza căutării şi colectării dovezilor digitale, faza reconstrucţiei scenei digitale a infracţiunii şi faza prezentării „teoriei scenei digitale".

– ***faza revizuirii***.

Modelul dezvoltat este foarte bine documentat, fiecărei grupe stabilindu-se obiectivul, fazele incluse fiind explicate în amănunţit, iar în final fiind prezentate două studii de caz – intruziune într-un server şi posesie de materiale pornografice cu minori – pentru ilustrarea activităţilor care apar în fazele descrise în model.

Autorii sesizează[1] că „Scena fizică a infracţiunii este bine înţeleasă pentru investigaţiile autorităţii de aplicare a legii ... este mai puţin înţeleasă pentru investigaţiile digitale conduse de investigatorii corporativi" care, de cele mai multe ori, „... nu au dezvoltate proceduri formale pentru examinarea locaţiei fizice a unui server compromis" şi, astfel, pot fi pierdute multe dovezi materiale dacă nu sunt valorificate la timp.

§ 7. Baryamureeba Venansuis, Tushabe Florence, Un model avansat/ îmbunătăţit al procesului integrat de investigare digitală[2]

Autorii, pentru modelul propus, folosesc ca bază procesul integrat de investigaţie digitală dezvoltat de Carrier şi Spafford, pe care îl „îmbunătăţesc" căutând să redefinească procesul de cercetare criminalistică şi progresul acestuia.

Modelul propus constă în 5 faze majore şi 14 faze:

– ***fazele de pregătire***, care includ: faza pregătirii operaţiunilor şi faza pregătirii infrastructurii;

– ***fazele de desfăşurare***, care includ: faza detectării şi notificării, faza investigării materiale a scenei infracţiunii, faza investigării digitale a scenei infracţiunii, faza confirmării şi faza prezentării;

– ***fazele de urmărire***, care includ: faza investigării digitale a scenei infracţiunii şi faza autorizării, faza documentării scenei materiale a infracţiunii, faza

[1] *Ibidem*, p. 13.

[2] Baryamureeba V., Tushabe F., *The Enhanced Digital Investigation Process Model*, disponibil on-line la http://www.dfrws.org/2004/day1/D1-Tushabe-EDIPm.ppt (ultima dată accesat la 19.09.2010).