O ANALIZĂ COMPARATIVĂ A MODULUI ÎN CARE AU FOST IMPLEMENTATE, ÎN LEGISLAȚIILE NAȚIONALE, UNELE DINTRE MĂSURILE PREVĂZUTE DE CONVENȚIA PRIVIND CRIMINALITATEA INFORMATICĂ

Gheorghe-Iulian IONIȚĂ*

Abstract. A comparative analysis regarding the implementation of some CoE's Convention on Cybercrime provisions in the national legislations. *What is the role of the CoE's Convention on Cybercrime? Have the provisions of the Convention been transposed into the national legislations of the signatory parts? Can we discuss about a harmonization of those provisions? What are the repercussions of this process?*

Trough the present study I am trying to present some answers to those questions.

Rezumat. *Care este rolul Convenției Consiliului Europei privind criminalitatea informatică? Au fost implementate, în legislațiile naționale ale statelor semnatare, măsurile prevăzute de Convenție? Se poate vorbi de o armonizare a acestor dispoziții? Care sunt repercusiunile acestui proces?*

Prin prezentul studiu încerc să formulez răspunsuri la aceste întrebări.

Keywords: *cybercrime, convention, provisions, transpose, national legislations, harmonization.*

Cuvinte cheie: *criminalitate informatică, convenție, măsuri, implementare, legislații naționale, armonizare.*

1. Introducere

Convenția Consiliului Europei privind criminalitatea informatică[1] este inspirată de convingerea că noul fenomen al a criminalității informatice, luând în considerare dimensiunea transnațională a acestuia, poate fi contracarat eficient doar prin armonizarea legislațiilor naționale[2].

Cu toate criticile[3] aduse procesului de elaborare şi adoptare, Convenția rămâne cel mai important instrument internațional utilizat în lupta împotriva criminalității informatice, chiar dacă, 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*. Astfel, se observă că unele dintre reglementările naționale sunt în concordanță cu dispozițiile Convenției, în timp ce altele sunt încă departe de acest deziderat.

Prezenta analiză este parte a tezei de doctorat „Criminalitatea informatică" (susținută, în iulie, 2009, la Academia de Poliție „Alexandru Ioan Cuza")[4] şi a fost realizată pe baza profilurilor legislative[5] şi studiilor oferite de Consiliul Europei, dar şi a legislației, doctrinei şi jurisprudenței din țările incluse în studiu.

2. Analiza comparativă a modului în care au fost definiți termenii utilizați

Potrivit art. 1 din Convenție,

„În sensul prezentei convenții:

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, informații sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcții 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

(ii) orice altă entitate care prelucrează sau stochează date informatice pentru acest serviciu de comunicații 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 lanțului de comunicare, indicând originea, destinația, itinerarul, ora, data, mărimea, durata sau tipul de serviciu subiacent".

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

Paradoxal, în literatura de specialitate[6], se ridică problema că definirea conceptelor utilizate este prea amplă şi neclară față de conduita la care se referă aceasta.

Nu toate țările care au ratificat Convenția au introdus în întregime/părți din definițiile acestor termeni; spre exemplu: Albania, Armenia, Croația, Estonia, Franța, Ungaria, Lituania, fosta Republică Iugoslavă a Macedoniei, Ucraina, Slovacia.

Sunt foarte puține *țări* care definesc toate conceptele ce se regăsesc în art. 1 din Convenție, *aliniindu-şi* complet *dispozițiile interne*; spre exemplu: Austria[7], Bulgaria[8], Cipru[9], Sri Lanka[10].

Unele țări ca Italia[11], Republica Cehă[12], definesc doar conceptul de „date" sau „trafic de date".

Mai mult, legiuitorul german[13] defineşte noțiunea 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 definiție chiar mai apropiată decât aceea a noțiunii de „date informatice" adoptată de Convenție.

O definiție a sistemului informatic a fost introdusă în legislația internă a majorității statelor, spre exemplu: Austria[14], Bulgaria[15], Cipru[16], Portugalia[17], SUA[18].

În alte state, ca Italia, Franța sau Australia, o astfel de definiție legală lipseşte.

Acest fapt creează dificultăți 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 siguranță". De asemenea, ar trebui clarificate unele aspecte cum ar fi: „intenționat", „neautorizat", „fără drept", „fără încuviințare", etc.

3. Analiza comparativă a modului în care au fost incriminate infracțiunile împotriva confidențialității, integrității şi disponibilității datelor

Infracțiunile definite în articolele 2-6 din Convenție sunt menite să protejeze confidențialitatea, integritatea şi disponibilitatea sistemelor informatice sau datelor, şi nu de a incrimina activitățile legitime şi obişnuite inerente în proiectarea rețelelor, ori activitățile de operare legitime şi obişnuite şi practicile comerciale[19].

3.1. Accesarea ilegală

Potrivit art. 2 din Convenție,

„Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, accesarea intenționată şi 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 şi un sistem informatic conectat la alt sistem informatic".

Această recomandare de incriminare reprezintă[20] infracțiunea de bază care include amenințările periculoase/atacurile la adresa/împotriva securității (de exemplu, confidențialitatea, integritatea şi disponibilitatea) sistemelor informatice şi a datelor. Nevoia de protecție reflectă interesele organizațiilor şi persoanelor fizice de a gestiona, opera şi controla propriile sisteme liber şi 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 şi datelor şi 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) şi 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, aşa cum s-a subliniat în literatura de specialitate[21], nu ar trebui incriminate activitățile obişnuite legate de utilizarea Internetului, activitățile inerente realizării rețelelor sau operațiunile comerciale obişnuite 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 fişierelor 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[22], Cipru[23], Estonia[24], Franța[25], Italia[26], Lituania[27], Mexic[28], Portugalia[29], Slovacia[30], Ungaria[31], SUA[32].

Din nefericire, niciuna dintre țări nu defineşte conceptele de „acces", „fără autorizație" şi „măsuri de siguranță". Această situație generează probleme grave în practică, în special cu privire la locul şi timpul comiterii infracțiunii.

Sunt câteva state[33] din cadrul SUA care definesc termenul de „acces". Trei dintre definițiile sunt mai comune: „a iniția, a comunica cu"; „a stoca datele în, a recepționa date de la"; „a utiliza orice resurse ale unui calculator, sistem informatic sau rețea informatică".

Potrivit art. 2, par. 2 din Convenție, statele membre pot condiționa incriminarea de:

- „violarea măsurilor de securitate", cum este, de exemplu, cazul Austriei[34] („măsuri specifice de securitate în cadrul sistemului informatic"), Ciprului[35] („măsuri de securitate"), Estoniei[36] („cod, parolă sau alte măsuri de protecție"), Germaniei[37] („mecanisme de securitate a accesului"), Lituaniei[38] („măsuri de securitate"), Mexicului[39] („mecanism de securitate"), Ungariei[40] („sistem sau echipament de protecție al calculatorului"). Cu toate acestea, nici una dintre țări, nu oferă o definiție a acestui concept.

- „intenția de a obține date informatice sau altă intenție delictuală", cum este, spre exemplu, cazul Portugaliei[41] şi Slovaciei[42].

- „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 legislații naționale conțin, în prezent, reglementări cu privire la infracțiuni de hacking sau cracking; ceea ce diferențiază aceste incriminări sunt elementele obiective şi subiecte, care diferă considerabil de la o țară la alta.

Astfel, unele țări ca Belgia[43], Franța[44], Italia[45], 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 țări au urmat o abordare mai restrânsă reclamând, suplimentar, mai multe circumstanțe calificate.

Câteva țări, ca Armenia[46] şi Austria[47], au mers chiar dincolo de reglementările Convenției atacând elemente diferite. Codul penal armean, de exemplu, în art. 251 alin. 1 incriminează chiar „neglijența care cauzează schimbarea, copierea, modificarea, izolarea informației sau stricarea echipamentelor informatice, a sistemelor informatice sau alte pagube semnificative".

Unele țări nu fac referire la accesarea ilegală a întregului calculator sau a unei părți a acestuia, ci, în general, la resursele unui calculator, care stabilesc nivelul incriminării. Spre exemplu, Armenia[48] pedepseşte „accesarea (penetrarea) informațiilor stocate într-un sistem informatic", Bulgaria[49] pedepseşte „accesul la resursele unui calculator", Croația[50] pedepseşte „accesul la date sau programe informatice", Regatul Unit[51] pedepseşte „accesul neautorizat la materialele informatice".

Câteva dintre *dispozițiile* legislațiilor interne care au fost *armonizate* cu dispozițiile art. 2 din Convenție:

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

- Art. 323-1 alin. 1 din Codul penal francez, pedepseşte „accesarea sau menținerea, 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 conținute în sistem sau alterarea funcționării acelui sistem".

- Art. 615-ter („Accesarea abuzivă a unui sistem informatic şi de telecomunicații") din Codul penal italian incriminează „pătrunderea abuzivă într-un sistem informatic sau de telecomunicații protejat de măsuri de siguranță", dar şi „menținerea împotriva voinței 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 infracțiunilor contra inviolabilității domiciliului (Dei delitti contro

la inviolabilità del domicilio). În acelaşi sens pronunțându-se şi Curtea Supremă de Casație italiană, Camera a Șasea Penală, care prin decizia nr. 3067 din 04 octombrie 1999, a statuat că prin dispozițiile art. 615-ter din Codul penal italian introdus prin Legea nr. 547 din 23 decembrie 1993 legislatorul a asigurat protecția „domiciliului informatic" în calitate de loc ideal (fizic, în acelaşi timp, unde sunt conținute datele informatice) care se încadrează în sfera individuală[52].

3.2. Interceptarea ilegală

Potrivit art. 3 din Convenție,

„Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, interceptarea intenționată 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 condiționa o astfel de incriminare de comiterea încălcării respective cu intenție delictuală sau de legătura dintre încălcarea respectivă şi un sistem informatic conectat la alt sistem informatic".

Această recomandare de incriminare urmăreşte[53] să protejeze dreptul la confidențialitatea comunicațiilor de date. Ea reprezintă aceeaşi 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 fişiere.

Exemple de *țări* care au introdus în legislația internă *reglementări în concordanță* cu dispozițiile art. 3 din Convenție: Austria[54], Croația[55], Cipru[56], Germania[57], Italia[58], Portugalia[59], Slovacia[60], Sri Lanka[61].

În unele state, interceptarea ilegală nu se referă numai la transmiterea privată a datelor, ci şi 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[62], foloseşte expresia „mesaj" în loc de „transmitere a datelor informatice"; Portugalia[63] face referire la „toate tipurile de comunicare din cadrul unui sistem informatic"; SUA[64] iau în calcul „orice comunicare orală, prin cablu sau electronică".

O cerință a art. 3 este ca interceptarea să fi fost făcută „fără drept" şi prin „utilizarea unor mijloace tehnice". Totuşi, 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[65],

Croația[66], Cipru[67], Estonia[68], Lituania[69]. Doar câteva din aceste legislații solicită ca infracțiunea să fie comisă cu intenție; spre exemplu Austria[70]. În plus, nicio legislație nu solicită ca infracțiunea să se realizeze în legătură cu un sistem informatic conectat la un altul, aşa cum se menționează în art. 3, alin. 2 din Convenție.

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 şi 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 şi 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") şi art. 623bis („Alte comunicații şi conversații") din Codul penal italian se aplică tuturor tipurilor de comunicații, fără diferențiere între transmisiile de date private sau publice. Art. 617-quinquies din acelaşi cod sancționează şi „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 şi emisiile electromagnetice), realizată prin intermediul unor dispozitive tehnice.

3.3. Afectarea integrității datelor

Potrivit art. 4 din Convenție,

„1. Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, fapta comisă intenționat şi fără drept de a distruge, şterge, deteriora, modifica sau elimina date informatice.

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

Scopul[71] acestei propuneri de incriminare este de a furniza datelor şi programelor informatice o protecție similară celor de care beneficiază obiectele corporale împotriva prejudicierii intenționate. Interesul legal protejat este integritatea şi 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[72].

Exemple de *țări* care au introdus în legislația internă *reglementări în concordanță* cu dispozițiile art. 4 din Convenție: Austria[73], Croația[74], Cipru[75], Germania[76], Italia[77], Slovacia[78], Sri Lanka[79].

Unele state precum Bulgaria[80], Estonia[81], Lituania[82], incriminează afectarea integrității datelor numai în cazuri semnificative, solicitând, ca respectiva conduită să aibă drept consecințe prejudicii grave.

În unele țări precum Croația[83], Slovacia[84], Turcia[85], reglementările sunt implementate integral cu excepția elementelor „intenționat" sau „fără drept". Suplimentar, alte state precum Armenia[86], incriminează nu numai comiterea intenționată, dar şi „neglijența care a cauzat consecințe grave".

Nu toate reglementările naționale acoperă toate formele de afectare a integrității 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 conține".

Unele state nu folosesc, în legislația internă, aceiaşi termeni ca cei folosiți în art. 4 din Convenție, ci numai o expresie generică precum „imixtiune în orice fel"[87], „ştergere, izolare şi inutilizare"[88], „accesare, modificare, deteriorare"[89], „acțiuni neautorizate"[90], 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 Convenție.

Alte state precum Slovacia[91], Ucraina[92], nu incriminează imixtiunea în datele informatice, ci asupra „informațiilor".

Exemple de *implementare integrală* în legislația internă a dispozițiilor art. 4 din Convenție:

- 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, infracțiunea este comisă de către „Orice persoană care, în mod intenționat şi fără autoritate, distruge, şterge, alterează ori suprimă (ascunde) date informatice".

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

Aproape toate statele au reglementări ce corespund parțial sau total cu prevederile art. 4 din Convenție.

O diferență majoră apare între diferitele tipuri de infracțiuni la nivel național privind descrierea actelor de imixtiune.

3.4. Afectarea integrității sistemului

Potrivit art. 5 din Convenție,

„Fiecare parte va adopta măsurile legislative şi alte măsuri care sunt necesare pentru a incrimina ca infracțiune, în conformitate cu dreptul intern, afectarea gravă, intenționată şi fără drept a funcționării unui sistem informatic, prin introducerea, transmiterea, periclitarea, ştergerea, deteriorarea, alterarea sau suprimarea datelor informatice".

Propunerea de incriminare vizează[93] 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 şi 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[94], Cipru[95], Franța[96], Germania[97], Italia[98], Slovacia[99], Sri Lanka[100].

Unele state precum Austria[101], Croația[102], Portugalia[103] 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 şi nu doar „afectarea gravă".

Fiecare stat parte are libertatea de a determina un nivel minim al prejudiciului cauzat ce poate fi definit ca „grav" şi, 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 poştă electronică nesolicitat (tip „spam") ar putea cauza un disconfort destinatarului însă ar putea să nu prejudicieze calculatorul. Situația este diferită în cazul în care transmiterea unui astfel de mesaj ar fi însoțită de un cod malițios sau când s-ar transmite un număr foarte mare de mesaje nesolicitate care ar putea cauza întreruperea unui sistem informatic şi, în consecință, astfel de situații ar trebui pedepsite.

Exemple de *implementare integrală* în legislația internă a dispozițiilor art. 5 din Convenție:

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

- Secț. 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 părți sau pentru o autoritate publică prin: 1. comiterea unui act prevăzut în secțiunea 303a subsecțiunea (1); sau 2. distrugerea, deteriorarea, compromiterea, ştergerea sau alterarea sistemelor de procesare sau de transport a datelor".

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

3.5. Abuzurile asupra dispozitivelor

Potrivit art. 6 din Convenție,

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

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

(i) a unui dispozitiv, inclusiv un program informatic, conceput special sau adaptat pentru a permite comiterea uneia dintre infracțiunile 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 intenția ca acestea să fie utilizate în vederea comiterii uneia dintre infracțiunile vizate la art. 2-5; şi

b) posesia unui element vizat la subparagrafele a) (i) sau a) (ii) sus-menționate, cu intenția de a fi utilizat în vederea comiterii uneia dintre infracțiunile vizate la art. 2-5. O parte va putea solicita, în conformitate cu dreptul intern, ca un anumit număr dintre aceste elemente să fie deținute 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 îşi 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[104] ca infracțiune separată şi independentă, săvârşirea 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 şi 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 şi 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[105]. Organizațiile internaționale care militează pentru libertatea pe Internet[106] au insistat asupra faptului că propunerea de incriminare şi 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 şi că descurajează dezvoltarea unor noi instrumente de securitate, conferind guvernului un rol impropriu de poliție a inovațiilor ştiințifice.

Exemple de *țări* care au *reglementări* introduse în legislația internă *în concordanță* cu dispozițiile art. 6 din Convenție: Austria[107], Croația[108], Italia[109], Sri Lanka[110].

Multe dintre prevederile naționale nu acoperă toate acțiunile ilegale incriminate de art. 6 din Convenție; spre exemplu art. 323-3-1 din Codul penal francez incriminează „importul, deținerea, oferirea, cedarea sau punerea la dispoziție, fără motive legitime, a unui echipament, instrument, program informatic sau date concepute sau adaptate special pentru comiterea uneia sau mai multor infracțiuni 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 deținerea de dispozitive de acces.

Exemple de *aliniere completă* a dispozițiilor legislațiilor interne cu prevederile art. 6 din Convenție:

- Secț. 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 (secț. 118a), o încălcare a secretului telecomunicațiilor (secț. 119), o interceptare ilegală a datelor (secț. 119a), o deteriorare a datelor (secț. 126a) sau o interferare cu funcționarea unui sistem informatic (secț. 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 intenția de a fi utilizate pentru comiterea oricăreia din infracțiunile menționate la par. 1 …

(2) O persoană nu va fi pedepsită conform prevederilor par. (1) dacă voluntar previne folosirea în scopurile menționate în paragraful 118a, 119, 119a, 126a sau 126b a programului informatic menționat 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 acțiune 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 autorizație, produce, procură, vinde, deține ori pune la dispoziție altei persoane dispozitive speciale, echipamente, programe informatice sau date electronice create sau adaptate pentru săvârşirea infracțiunilor menționate în paragrafele 1, 2, 3 si 4 ale acestui articol …".

- Art. 615-quarter („Deținerea şi difuzarea abuzivă de coduri de acces la sistemele informatice sau de telecomunicații") alin. 1 din Codul penal italian incriminează pe „Oricine, în scopul obținerii 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 telecomunicații, protejate prin măsuri de siguranță, sau orice fel de indicații sau instrucțiuni adecvate acestui scop"; în art. 615-quinquies incriminează pe „Oricine, în scopul deteriorării ilicite a unui sistem informatic sau de telecomunicații, a informațiilor, datelor sau programelor conținute de acestea sau care le aparțin, sau în vederea întreruperii, totale sau parțiale, sau alterării funcționării acestuia, procură, produce, reproduce, importă, difuzează, comunică, livrează sau pune la dispoziție în orice fel altor persoane, echipamente, dispozitive sau programe informatice".

Este recomandabil ca toate țările să prevadă expres că dispozitivele trebuie să fie special create sau adaptate pentru comiterea infracțiunilor prevăzute de Convenție la art. 2-5, pentru evitarea unei supra-incriminări.

4. Analiza comparativă a modului în care au fost incriminate infracțiunile informatice

Articolele 7-10 se referă la infracțiunile obişnuite care sunt frecvent comise prin intermediul unui sistem informatic. Cele mai multe state au incriminat deja aceste infracțiuni obişnuite, iar legile lor existente pot/nu pot fi suficient de cuprinzătoare pentru a acoperi şi situațiile care implică rețele de calculatoare (de exemplu, legile existente care incriminează pornografia infantilă din unele state nu pot acoperi şi situațiile 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 situațiile în care sistemele informatice sau rețelele sunt implicate iar în cazul în care infracțiunile existente acoperă deja un astfel de comportament, nu există nicio obligație de a modifica infracțiunile existente sau de a adopta altele noi.[111]

4.1. Falsificarea informatică

Potrivit art. 7 din Convenție,

„Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, introducerea, alterarea, ştergerea sau suprimarea intenționată şi fără drept a datelor informatice, din care să rezulte date neautentice, cu intenția ca acestea să fie luate în considerare sau utilizate în scopuri legale ca şi cum ar fi autentice, chiar dacă sunt sau nu sunt în mod direct lizibile şi inteligibile. O parte va putea condiționa răspunderea penală de existența unei intenții frauduloase sau a unei alte intenții delictuale".

Scopul[112] acestei propuneri de incriminare este de a crea o infracțiune paralelă cu falsificarea de documente tangibile pentru acoperirea lacunelor în dreptul penal legate de falsificarea tradițională, 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 consecințe grave ca şi actele tradiționale de fals în cazul în care o terță 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 operațiunilor juridice care se bazează pe autenticitatea informațiilor conținute în date şi face obiectul unei înşelăciuni. Interesul legal protejat constă în securitatea şi fiabilitatea datelor informatice care pot avea consecințe pentru relațiile juridice.

Conceptul de falsificare informatică variază destul de frecvent în legislațiile naționale. Pot fi evidențiate două concepte diferite de falsificare informatică: primul se bazează pe autenticitatea autorului documentului, în timp ce al doilea se bazează pe veridicitatea conținutului documentului. Oricum, elementul de bază comun trebuie să fie legat de alterarea autenticității şi veridicității conținutului datelor.

Sunt câteva *țări* care au introdus în legislația internă *reglementări în concordanță* cu dispozițiile art. 7 din Convenție; spre exemplu: Austria[113], Croația[114], Cipru[115], Italia[116], Macedonia[117], Portugalia[118], Slovacia[119].

Multe dintre legislațiile naționale ale unor state ca Albania[120], Armenia[121], Bulgaria[122], Estonia[123], Turcia[124], Ucraina[125] nu acoperă toate activitățile ilegale, aşa cum sunt descrise în art. 7 din Convenție; totuşi, majoritatea cazurilor de falsificare informatică pot intra sub incidența prevederilor tradiționale.

Unele țări incriminează nu numai modificarea sau alterarea datelor dar şi 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 „înşelării 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, ştergerea 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, şterge sau face inutilizabile date ori programe care sunt de însemnătate pentru relațiile juridice în scopul de a fi folosite ca autentice, sau oricine foloseşte 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, şterge 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 aceluiaşi articol este prevăzută o agravantă „Dacă infracțiunea stipulată la paragraful (1) este săvârşită asupra datelor sau programelor informatice care sunt folosite în activități ale autorităților statului, instituțiilor publice, întreprinderi sau alte persoane fizice sau juridice care desfăşoară 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 şi în cel privat, o creştere exponențială a documentelor electronice, majoritatea legislațiilor naționale recunoscând aceeaşi relevanță juridică ca cea a documentelor tradiționale.

Pentru a garanta o desfăşurare sigură şi corectă a relațiilor economice, sociale şi 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, aşa cum a reținut şi Curtea Supremă de Casație italiană, Camera a Cincea Penală, prin decizia nr. 11930 din 25 martie 1999[126], în lipsa unei reglementări speciale, instanțele italiene au extins dispozițiile de drept comun existente (care incriminau falsul) pentru a acoperi situațiile de falsificare a unor documente sau arhive electronice.

4.2. Frauda informatică

Potrivit art. 8 din Convenție,

„Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, fapta intenționată şi fără drept de a cauza un prejudiciu patrimonial unei alte persoane:

a) prin orice introducere, alterare, ştergere 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 însuşi sau pentru altă persoană".

Scopul[127] 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 şi 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[128], Cipru[129], Germania[130], Italia[131], Portugalia[132], SUA[133].

Unele țări ca Albania, Armenia[134], Bulgaria[135], Croația[136], Estonia[137], Lituania[138], Macedonia[139], Ucraina[140], Ungaria[141], 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.) şi (în parte) în prevederile altor infracțiuni de drept comun (cartea III, titlul I, cap. III, secț. 1 „Escrocheria" art. 313-1 şi 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 ştergerea 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 şi fără autoritate şi cu intenția de a înşela cauzează pierderea de proprietate altei persoane prin a. orice introducere, alterare, ştergere 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, utilizarea neautorizată a datelor sau altă influențare 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".

Și de această dată, de punctat faptul că, încă din anul 1999, aceiaşi Curte Supremă de Casație italiană, Camera a Șasea Penală, prin decizia nr. 3065 din 14 decembrie 1999[142], 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.

5. Analiza comparativă a modului în care au fost incriminate infracțiunile 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;

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-menționat, 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-menționat, termenul minor desemnează *orice persoană în vârstă de mai puțin de 18 ani*. Totuşi o parte poate solicita o limită de vârstă inferioară, care trebuie să fie de cel puțin 16 ani.

4. O parte îşi va putea rezerva dreptul de a nu aplica, în totalitate sau parțial, paragraful 1 subparagrafele d) şi e) şi paragraful 2 subparagrafele b) şi c)".

Propunerea de incriminare caută[143] să consolideze măsurile de protecție pentru copii, inclusiv protecția acestora împotriva exploatării sexuale, prin modernizarea dispozițiilor de drept penal pentru a circumscrie mai eficient utilizarea sistemelor informatice în comiterea infracțiunilor sexuale împotriva copiilor. Această dispoziție incriminează diferite aspecte ale producției, deținerea şi distribuirea de materiale de pornografie infantilă electronice. Majoritatea statelor incriminează deja producția tradițională şi distribuția fizică a pornografiei infantile, dar cu utilizarea tot mai mare a Internetului ca instrument principal de tranzacționare a unor astfel de materiale, s-a resimțit tot mai puternic că dispoziții specifice într-un instrument juridic internațional sunt esențiale 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 infracțiunilor sexuale împotriva copiilor.

În literatura de specialitate sunt, de asemenea, exprimate păreri[144] conform cărora nu era necesară o asemenea propunere de incriminare întrucât distribuția şi posesia de materiale pornografice cu minori sunt deja infracțiuni în majoritatea țărilor iar definițiile utilizate în legătură cu pornografia infantilă sunt prea 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[145], Cipru[146], Franța[147] Italia[148], Spania[149], SUA[150].

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[151], Armenia[152], Croația[153], Franța[154], Lituania[155], Slovacia[156], Turcia[157] nu sunt definiți termenii „pornografie infantilă" şi „minor".

Unele state ca Estonia[158], Germania[159], Portugalia[160], 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, şi 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 şi „oferirea, punerea la dispoziție sau distribuirea unei astfel de imagini sau reprezentări, prin orice mijloace"; în alin. 3 şi 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" şi „atunci când sunt comise în bande organizate". Prin alin. 5, incriminarea depăşeşte scopul art. 9 din Convenție, sancționând chiar şi „consultarea obişnuită 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 şi deținerea de materiale pornografice implicând minori") din Codul penal german pedepseşte 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 şi 176b) (materiale pornografice implicând minori): 1. răspândeşte; 2. afişează 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 si 2 ori face posibilă o astfel de utilizare de către altcineva" şi 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 şi materiale pornografic implicând copii ce reproduc un eveniment real sau adevărat".

- Art. 600-ter („Pornografia infantilă") din Codul penal italian pedepseşte, în alin. 1 şi 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" şi pe „cei care comercializează materialele pornografice"; în următoarele două alineate (alin. 3 şi 4) sunt incriminate două forme atenuate „Oricine ... prin orice mijloace, chiar şi prin telecomunicații, distribuie,

divulgă, difuzează sau face publice materiale pornografice … distribuie sau difuzează ştiri sau informaţii finalizate cu ademenirea sau exploatarea sexuală de minori de optsprezece ani" şi „Oricine ... oferă sau cedează altora, chiar şi cu titlu gratuit, materiale pornografice". Prin art. 600-quater („Deținerea de materiale pornografice") din acelaşi cod, este pedepsit „Oricine ... conştient procură sau deține materiale pornografice realizate utilizând minori de optsprezece ani". Potrivit dispozițiilor art. 600-quater.1 („Pornografia virtuală") din acelaşi cod, dispozițiile mai sus citate (art. 600-ter şi 600-quater) „se aplică chiar şi 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 acelaşi cod, legislația italiană depăşeşte 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" şi „pornografie infantilă".

În plus, ar trebui luată în considerație şi 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".

6. Analiza comparativă a modului în care au fost incriminate infracțiunile referitoare la atingerile aduse proprietății intelectuale şi drepturilor conexe

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 revizuieşte 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".

Încălcări ale drepturilor de proprietate intelectuală, în special a dreptului de autor, sunt printre cele mai frecvente infracțiuni comise pe Internet, care produc îngrijorare atât pentru titularii drepturilor de autor şi celor care lucrează cu rețele de calculatoare. Reproducerea şi difuzarea pe internet a operelor protejate (literare, fotografice, muzicale, audio-vizuale, etc.), fără acordul deținătorului drepturilor de autor, sunt extrem de frecvente. Uşurința cu care pot fi făcute copii neautorizate datorită tehnologiei digitale şi amploarea reproducerii şi difuzării în cadrul rețelelor a făcut necesară includerea unor dispoziții în dreptul penal şi consolidarea cooperării internaționale în acest domeniu[161].

Cu toate acestea se susține[162] în literatura de specialitate că acest articol (art. 10 din Convenție) nu-şi are locul aici, întrucât protecția proprietății intelectuale este o problemă complicată care atinge ambele probleme, libera exprimare şi viața privată, şi în care legea este încă în curs de dezvoltare; în plus, există alte foruri internaționale, în care aceste aspecte sunt abordate într-un mod mai corespunzător.

Exemple de *țări* care au introdus în legislația internă *reglementări în concordanță* cu dispozițiile art. 10 din Convenție: Albania[163], Armenia[164], Cipru[165], Franța[166], Germania[167], Italia[168], SUA[169].

Reglementările interne pentru protecția drepturilor de autor şi a drepturilor conexe nu fac trimitere la sistemul informatic, ca mijloc de comitere a infracțiunilor. Doar câteva țări, ca Armenia[170], Cipru[171], prevăd în legislația internă, în mod expres, ca aceste infracțiuni să fie comise prin intermediul unui sistem 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[172], Croația[173], Turcia[174], Ungaria[175], ar putea extinde aplicabilitatea prevederilor şi 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 şi 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[176], Estonia[177], Lituania[178], 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 şi 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 şi fără permisiunea deținătorului drepturilor" iar secț. 108 („Încălcarea drepturilor conexe") din aceiaşi lege, incriminează pe „(1) Oricine, într-o altă manieră permisă de lege şi fără permisiunea deținătorului drepturilor:

1. reproduce, distribuie ori comunică public o ediție ştiințifică (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 şi audio contrar secțiunii 94 sau secțiunii 95 coroborată cu secțiunea 94

8. foloseşte o bază de date contrar secțiunii 87b (1)".

Secț 108b („Interferența neautorizată cu măsurile tehnice de protecție şi informații necesare managementului drepturilor") din aceiaşi 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 ştiință 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 cu o comunicare publică a unei astfel de opere sau materii protejate, sau

b) diseminează, pregăteşte 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 şi 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 înfăptuieşte intenționat în scopuri comerciale orice act prin intermediul unui sistem informatic care potrivit Legii privind proprietatea intelectuală şi drepturile conexe din 1976 încalcă dreptul de proprietate intelectuală sau drepturile conexe".

- Art. 171-bis din Legea italiană nr. 633/1941 pedepseşte pe „1. Oricine în mod abuziv multiplică, pentru profit, programe sau în acelaşi scop importă, distribuie, vinde, deține în scop comercial sau de afaceri ori leasing programe conținute pe suporturi nemarcate de Societatea italiană a autorilor şi editorilor (SIAE) … prin orice mijloace urmăreşte 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 şi 64-sexies, sau efectuează extragerea ori reutilizarea bazei de date încălcând dispozițiile articolelor 102-bis şi 102-ter, sau distribuie, vinde sau închiriază o bancă de date". Art. 171-ter din aceiaşi 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 conțin înregistrări audio sau video a operelor muzicale, cinematografice ori audiovizuale asimilate sau secvențe de imagini în mişcare

b) în mod abuziv reproduce transmite sau difuzează în public, prin orice mijloc, opere ori părți din opere literare, dramatice, ştiințifice 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 țării, deține 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 menționate la literele a) şi b)

d) deține 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 conține înregistrări audio ori video ale operelor muzicale, cinematografice ori audiovizuale sau secvențe de imagini în mişcare, sau alte suporturi pentru care este prevăzută, în sensul prezentei legi, aplicarea marcajului Societății 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 recepționat prin intermediul aparatelor sau părților din aparatele pentru decodarea transmisiunilor cu acces condiționat

f) introduce pe teritoriul țării, deține 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 deține 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 informațiile electronice prevăzute la articolul 102-quinquies, sau distribuie, importă pentru distribuire, difuzează prin radio ori televiziune, comunică sau pune la dispoziția publicului opere ori alte materiale protejate de la care au fost eliminate sau modificate aceleaşi informații electronice

2. … oricine

a) reproduce, multiplică, transmite ori difuzează abuziv, vinde sau introduce în alt mod în comerț, 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 rețele 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 activitățile ilicite menționate la alineatul 1".

Este de dorit incriminarea penală a încălcării drepturilor de autor prin intermediul sistemelor informatice în maniera propusă de art. 10 din Convenție deoarece s-ar putea evita incriminarea reproducerii fişierelor făcută de utilizatorii

privați de Internet. În aceste cazuri ar putea fi aplicate sancțiuni mai uşoare – cum ar fi sancțiunile 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.

7. Concluzii

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 infracțiuni, şi, pe de altă parte, permite organizarea unui sistem internațional de cooperare rapid şi eficient.

Aşa cum se poate observa din analiza prezentată, unele dintre reglementările naționale sunt în concordanță cu dispozițiile Convenției, în timp ce altele sunt încă departe de acest deziderat.

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 țări, ar permite o armonizarea globală efectivă (nu la nivel declarativ) a legislației cu privire la infracțiunile din sfera criminalității informatice.

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

---

* **Gheorghe-Iulian IONIȚĂ**, Lector, Universitatea Româno-Americană, Avocat, Baroul Bucureşti; ionita.gheorghe.iulian@profesor.rau.ro

[1] Council of Europe, *Convention on Cybercrime* (CETS no: 185), disponibilă la: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (ultima dată accesat la 24.08.2010)

[2] A se vedea şi Galdieri, P., *Crimini informatici: un passo avanti con la ratifica della Convenzione*, disponibil la: http://www.interlex.it/regole/galdieri2.htm#* (ultima dată accesat la 28.08.2010)

[3] A se vedea şi Akdeniz, Y., Cyber-Rights & Cyber-Liberties, *An Advocacy Handbook for the Non Governmental Organisations: The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems* (updated and revised in May 2008), p. 7-9 disponibil la: www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf (ultima dată accesat la 30.08.2010)

[4] Ioniță, G.I., 2009, *Criminalitatea informatică*, teză de doctorat (nepublicată), Bucureşti, Academia de Poliție „Alexandru Ioan Cuza".

[5] Aceste profiluri legislative au fost elaborate în cadrul de lucru al Proiectului Consiliului Europei asupra criminalității informatice, având în vedere schimbul de informații cu privire la legislația criminalității informatice şi evaluarea stadiului actual de implementare a Convenției privind criminalitatea infor-

matică în legislația națională; sunt disponibile la: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp (ultima dată accesat la 24.08.2010)

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

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

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

[9] 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 la: http://www.police.gov.cy/police/police.nsf/All/F68C2910055AE565C22574C9002FA68B?OpenDocument (ultima dată accesat la 29.08.2010)

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

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

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

[13] Secț. 202a(2) Cod penal german (Strafgesetzbuch) disponibil la: http://bundesrecht.juris.de/stgb/index.html (ultima dată accesat la 24.08.2010)

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

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

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

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

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

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

[20] Idem, pct. 44

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

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

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

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

[25] Art. 323-1 Cod penal francez (Code pénal) disponibil la: http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719

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

[27] Art. 198 şi 198-1 Cod penal lituanian (Kriminăllikums) disponibil la: http://www.ttc.lv/export/sites/default/docs/LRTA/Likumi/The_Criminal_Law.doc

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

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

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

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

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

[33] Alabama, Arkansas, Conneticut, Delaware, Iowa, Kansas, New Hampshire

[34] Secț. 118a Cod penal austriac

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

[36] Art. 217 Cod penal eston

[37] Secț. 202a Cod penal german

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

[39] Art. 211 bis1 Cod penal federal mexican

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

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

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

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

[44] Art. 323-1 Cod penal francez

[45] Art. 615-ter Cod penal italian

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

[47] Secț. 118a Cod penal austriac

[48] Art. 251 Cod penal armean

[49] Art. 319a Cod penal bulgar

[50] Art. 223(1) OG croată 105/04

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

[52] 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 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)

[53] Council of Europe, *Explanatory Report*, op. cit., pct. 51

[54] Secț. 119 şi 119a Cod penal austriac

[55] Art. 223 par. 4 OG croată 105/04
[56] Art. 5 Legea cipriotă nr. 22(III)/2004
[57] Sect. 202b Cod penal german
[58] Art. 617-quater, 617-quinquies, 617-sexies, 623-bis Cod penal italian
[59] Art. 8 Legea portugheză nr. 109/1991
[60] Art. 247(2) Cod penal slovac
[61] Art. 8 Legea sri lankeză nr. 24/2007
[62] Art. 171(1) Cod penal bulgar
[63] Art. 8 Legea portugheză nr. 109/1991
[64] Titlul 18, partea I, cap. 119, § 2511 Cod penal federal american
[65] Art. 254(1) Cod penal armean
[66] Art. 223(4) OG croată 105/04
[67] Art. 5 Legea cipriotă nr. 22(III)/2004
[68] Art. 137 Cod penal eston
[69] Art. 198 Cod penal lituanian
[70] Secț. 119a Cod penal austriac
[71] Council of Europe, *Explanatory Report*, op. cit., pct. 60
[72] Idem, pct. 64
[73] Secț. 126a Cod penal austriac
[74] Art. 223 par. 3 OG croată 105/04
[75] Art. 6 Legea cipriotă nr. 22(III)/2004
[76] Secț. 303 a Cod penal german
[77] Art. 635-bis şi 635-ter Cod penal italian
[78] Art. 247(1)b Cod penal slovac
[79] Art. 5(a) Legea sri lankeză nr. 24/2007
[80] Art. 319b Cod penal bulgar
[81] Art. 206 Cod penal eston
[82] Art. 196 Cod penal lituanian
[83] Art. 223(3), OG croată 105/04
[84] Art. 247(1)b Cod penal slovac
[85] Art. 244(2) Cod penal turc (Türk Ceza Kanunu) disponibil la: http://www.tbmm.gov.tr/kanunlar/k5237.html (ultima dată accesat la 26.08.2010)
[86] Art. 253 Cod penal armean
[87] Art. 192/b Cod penal albanez (Kodi Penal I Republikës Së Shqipërisë) disponibil la: http://www.mpcs.gov.al/dpshb/images/stories/files/kodet/3.3.5._Kodi_Penal.pdf (ultima dată accesat la 26.08.2010)
[88] Art. 253 Cod penal armean
[89] Art. 477.1 şi art. 477.2 Cod penal australian
[90] Art. 362 alin.1. Cod penal ucrainean
[91] Art. 247(1) b Cod penal slovac

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

[93] Council of Europe, *Explanatory Report*, op. cit., pct. 65

[94] Secț. 126b Cod penal austriac

[95] Art. 7 Legea cipriotă nr. 22(III)/2004

[96] Art. 323-2 Cod penal francez

[97] Secț. 303b Cod penal german

[98] Art. 635-quater şi 635-quinquies Cod penal italian

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

[100] Art. 5a Legea sri lankeză nr. 24/2007

[101] Secț. 126b Cod penal austriac

[102] Art. 223(3) OG croată 105/04

[103] Art. 5 şi 6 Legea portugheză nr. 109/91

[104] Explanatory Report, op. cit., pct. 71

[105] A se vedea şi Baron, R., *op .cit.*, p. 269

[106] A se vedea şi Global Internet Liberty Campaign, *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime*, disponibil la: http://gilc.org/privacy/coe-letter-1000.html (ultima dată accesat la 30.08.2010)

[107] Secț. 126c Cod penal austriac

[108] Art. 223 alin. 6-7 OG croată 105/04

[109] Art. 615-quater şi 615-quinquies Cod penal italian

[110] Art. 9 Legea sri lankeză nr. 24/2007

[111] Council of Europe, *Explanatory Report*, op. cit., pct. 79

[112] Idem, pct. 81

[113] Secț. 225a Cod penal austriac

[114] Art. 223a OG croată 105/04

[115] Art. 9 Legea cipriotă nr. 22(III)/2004

[116] Art. 491-bis Cod penal italian

[117] Art. 379-a Cod penal macedonean (Кривичниот законик) disponibil la: http://www.mlrc.org.mk/zakoni/Z1996033.htm (ultima dată accesat la 26.08.2010)

[118] Art. 4 Legea portugheză nr. 109/91

[119] Art. 247(1)d Cod penal slovac

[120] Art. 186-189 Cod penal albanez

[121] Art. 252 Cod penal armean

[122] Art. 319b şi 319c Cod penal bulgar

[123] Art. 344 Cod penal eston

[124] Art. 244 par. 2 Cod penal turc

[125] Art. 362(1) Cod penal ucrainean

[126] A se vedea şi Sarzana C**.,** *op. cit.*, p. 10

[127] Council of Europe, *Explanatory Report*, *op. cit.*, pct. 86

[128] Sect. 148a Cod penal austriac

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

[130] Secț. 263a Cod penal german

[131] Art. 640-ter Cod penal italian

[132] Art. 221 Cod penal portughez (Código Penal) disponibil la: http://www.aacs.pt/legislacao/codigo_penal.htm (ultima dată accesat la 26.08.2010)

[133] Titlul 18 partea I cap. 47 § 1030(a)(4) şi § 1343 Cod penal federal american

[134] Art. 252 Cod penal armean

[135] Art. 212a şi 319b(2) Cod penal bulgar

[136] Art. 224a Cod penal croat

[137] Art. 213 Cod penal eston

[138] Art. 182, 196 şi 197 Cod penal lituanian

[139] Art. 251(4-5) Cod penal macedonean

[140] Art. 190(3) Cod penal ucrainean

[141] Art. 300/C şi 300/E Cod penal ungar

[142] A se vedea şi Sarzana C**.,** *op. cit.*, p. 12

[143] Council of Europe, *Explanatory Report*, *op. cit.*, pct. 91 şi 93

[144] A se vedea Taylor, G., *The Council of Europe Cybercrime Convention A civil liberties perspective*, disponibil la: http://www.crime-research.org/library/CoE_Cybercrime.html (ultima dată accesat la 28.08.2010)

[145] Secț. 207a Cod penal austriac

[146] Art. 12(1) Legea cipriotă nr. 22(III)/2004

[147] Art. 227-23 Cod penal francez

[148] Art. 600-ter, 600-quater, 600-quinquies Cod penal italian

[149] Art. 189 Cod penal spaniol (Código Penal) disponibil la: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html (ultima dată accesat la 26.08.2010)

[150] Titlul 18, partea I, cap. 110, § 2252 Cod penal federal american

[151] Art. 117 Cod penal albanez

[152] Art. 263 Cod penal armean

[153] Art. 197 OG croată 105/04

[154] Art. 227-23 şi 227-24 Cod penal francez

[155] Art. 162 şi 309 Cod penal lituanian

[156] Secț. 368-370 Cod penal slovac

[157] Art. 226 Cod penal turc

[158] Art. 177 Cod penal eston

[159] Secț. 184b Cod penal german

[160] Art. 172 Cod penal portughez

[161] Council of Europe, *Explanatory Report*, *op. cit.*, pct. 107

[162] A se vedea Taylor, G., op. cit.

[163] 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 la: http://www.zshda.gov.al/kuadriligjor/ligji.doc (ultima dată accesat la 26.08.2010)

[164] Art. 158 Cod penal armean

[165] Art. 12 Legea cipriotă nr. 22(III)/2004

[166] Art. L112-1 şi L112-1 Cod proprietate intelectuală francez (Code de la propriété intellectuelle) disponibil la: http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006069414 (ultima dată accesat la 26.08.2010)

[167] Secț. 106 Legea germană cu privire la drepturile de autor şi drepturile conexe (Gesetz über Urheberrecht und verwandte Schutzrechte) disponibil la: http://www.gesetze-im-internet.de/urhg/index.html (ultima dată accesat la 26.08.2010)

[168] Art. 171-bis, 171-ter, 171-octies, 174-ter Legea nr. 633/1941 (Legge 22 aprile 1941, n. 633, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio) disponibil la: http://www.altalex.com/index.php?idstr=12&idnot=34610 (ultima dată accesat la 28.08.2010)

[169] Titlul 17, cap. 5, § 506 şi titlul 18, partea I, cap. 47, § 2319 Cod penal federal american

[170] Art. 158 Cod penal armean

[171] Art. 12 Legea cipriotă nr. 22(III)/2004

[172] Art. 172a Cod penal bulgar

[173] Art. 230 OG croată 110/97

[174] Art. 72-73 Legea nr. 5846/1951 (Fikir Ve Sanat Eserleri Kanunu) disponibil la: http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=1.3.5846&MevzuatIliski=0&sourceXmlSearch= (ultima dată accesat la 28.08.2010)

[175] Art. 329/A şi 329/C Cod penal ungar

[176] Art. 12 Legea cipriotă nr. 22(III)/2004

[177] Art. 223 şi 225 Cod penal eston

[178] Art. 192 Cod penal lituanian