UNELE ASPECTE PRIVIND NOUL TRATAT GLOBAL ÎN DOMENIUL CYBERCRIMINALITĂŢII ŞI CYBERSECURITĂŢII

IOANA VASIU[*]
LUCIAN VASIU

Abstract *The evolution and revolution of information technology brought great advantages for all domains of our modern society; however, in parallel, an evolution and a revolution in high-tech crime was noted. Powerful digital technologies made the Internet not only the source of information, communication, entertainment and education, but also, the perfect world for crime, internet being now a real magnet for all sorts of common criminals. The consequences of high-tech crimes may have serious consequences. It is clear that effectively combating cybercrime will require global cooperation, involving a much broader group of countries than the current signatories of the Council of Europe's Convention on Cybercrime. In this study, we argue part of the solution to these problems is the adoption of a Global Treaty on Cybersecurity and Cybercrime. This Global Treaty would represent the required legal framework globally applicable and interoperable with the existing national and regional laws and regulations.*

Key words: *Cybersecurity, Cybercriminality, Cyber risk, Information infrastructure, Computer contaminants.*

[*] Conf. univ. dr. Ioana Vasiu, Facultatea de Drept, Universitatea „Babeş-Bolyai" şi Facultatea de Drept Cluj-Napoca, Universitatea Creştină „Dimitrie Cantemir"; Director al Institutului de Ştiinţe Administrative Paul Negulescu şi *Research Director* al proiectului FP7 CONSENT, finanţat de Comisia Europeană. E-mail: ioanav3@yahoo.com.

– Consideraţii introductive

Avansurile tehnologice aduc îmbunătăţiri pentru societate, dar, în acelaşi timp, creează noi oportunităţi infracţionale[1]. Vulnerabilităţile asociate sistemelor informatice, atacurile informatice complexe (formate din secvenţe de activitate infracţională, executată în mai multe etape, pe mai mulţi vectori de atac), posibilitatea de a acţiona de la mare distanţă şi de a elimina complet evidenţele privind momentul şi/sau modul de comitere a infracţiunilor informatice (nu vor exista martori, impresiuni digitale sau ADN), dificultăţile legate de detectarea infracţiunilor şi problemele jurisdicţionale şi de cooperare internaţională cresc serios pericolul acestor infracţiuni[2].

Criminalitatea în cyberspaţiu a crescut în sofisticare şi prevalenţă, implicând, din ce în ce mai mult, crima organizată, *hacking*-ul, utilizarea *botnet*-urilor, furtul de date din interior şi atacuri masive asupra infrastructurilor de informaţii critice, pagubele înregistrate datorită acestui tip de criminalitate fiind în continuă creştere[3]. Activitatea făptuitorilor nu poate fi rezolvată efectiv cu măsuri doar la nivel naţional, sau chiar la nivel de grup de state, ci este nevoie de un efort concertat al industriei în domeniu, al guvernelor, al organelor cu atribuţii de punere în aplicare a legislaţiei în domeniu şi al cetăţenilor tuturor ţărilor, chiar dacă, în trecut, au existat şi opinii potrivit cărora nu este necesară armonizarea legilor sau procedurilor privind criminalitatea informatică, cazurile de infracţionalitate informatică nefiind decât cazuri obişnuite, care au în

[1] Vezi U. S. Department of Justice, *The challenge of unlawful conduct involving the use of the Internet*, *A Report of the President's working group on unlawful conduct on the Internet,* 2000.

[2] Vezi, spre exemplu, E. S. Podgor, *International computer fraud: a paradigm for limiting national jurisdiction*, p. 35 în „U. C. Davis Law Review", 2002, P. 267-317; S. W. Brenner şi J. J. Schwerha, *Cybercrime: A Note on International Issues*, în „Information Systems Frontiers", 6 (2), 2004, p. 111-114; R. Skibell, *Cybercrimes & Misdemeanors: A reevaluation of the Computer Fraud and Abuse Act*, în „Berkeley Technology Law Journal", 2003, 18:3; N. K. Katyal, *Criminal Law in Cyberspace*, în „University of Pennsylvania Law Review", 1003, 2001, p. 149; M. A. Sussmann, *The critical challenges from international high-tech and computer-related crime at the millennium*, în „Duke Journal Of Comparative & International Law", 9, 1999.

[3] A se vedea Ioana Vasiu şi Lucian Vasiu, *Criminalitatea în cyberspaţiu*, Editura Universul Juridic, Bucureşti, 2012; *2012 Data Breach Investigations Report*, Studiu realizat de Verizon RISK Team, US Secret Service, Police Central e-Crime Unit etc.

comun folosirea de tehnologii ale informaţiei şi comunicaţiei[4].

Cyberspaţiul pune în discuţie noţiunile tradiţionale de jurisdicţie[5] şi suveranitate, impunând un răspuns coordonat la nivel internaţional. Dificultăţile actuale se datorează lipsei unui acord la nivel global în ceea ce priveşte procedurile şi practicile în domeniul investigaţiei în comunicaţiile digitale, precum şi lipsei de sisteme efective, adecvate de schimb de date, legilor inadecvate[6], disparităţilor existente în ceea ce priveşte prevederile legale şi lipsei de expertiză la nivelul organelor de investigare şi judecată[7]. Natura criminalităţii informatice este una globală, prin urmare şi natura problemelor cadrului legal în domeniu, necesitatea unui consens global, pentru armonizarea legislaţiei şi a procedurilor de investigare şi acuzare, noi forme de drept multilateral sau globalizat[8].

Nici un stat nu poate de unul singur să elimine sau măcar să reducă problema infracţionalităţii în Cyberspaţiu. Este nevoie de leadership partajat şi determinare, un demers în acest sens este reprezentat de Convenţia europeană (ETS No. 185), considerată un început pozitiv, dar care trebuie continuat şi îmbunătăţit în ceea ce priveşte detalierea elementelor necesare în cazul fiecărei infracţiuni, specificarea unor proceduri consistente pentru investigarea şi urmărirea în justiţie a

---

[4] Vezi F. H. Easterbrook, *Cyberspace and the Law of the Horse*, în „University of Chicago Legal Forum", 207, 1996.

[5] Vezi S. W. Brenner şi B.-J. Koops, *Approaches to Cybercrime Jurisdiction*, „4 Journal of High Technology Law", 1, 2004.

[6] Vezi consideraţiile lui D. B. Hollis, *An e-SOS for Cyberspace*, „Harvard International Law Journal", Vol. 52, No. 2, Summer, 2011.

[7] Vezi Raportul grupului de experţi ITO pentru elaborarea Tratatului la nivel global în domeniul cybersecurităţii şi criminalităţii informatice.

[8] Vezi M. Goodman, *International Dimensions of Cybercrime*, în S. Ghosh şi E. Turrini (eds.), *Cybercrimes: A Multidisciplinary Analysis* , 2010; S. Schjolberg, *The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva*, 2008; A. I. Cerezo, J. Lopez şi A. Patel, *International Cooperation to Fight Transnational Cybercrime*, Second International Workshop on Digital Forensics and Incident Analysis, 2007; M. Gercke, *The Slow Wake of a Global Approach Against Cybercrime*, „Computer Law Review International", 2006 141; M. L. Rustad şi T. H. Koenig, *Harmonizing Cybertort Law for Europe and America*, „5 Journal of High Technology Law", 13, 2005; S. Brenner, *Toward a Criminal Law for Cyberspace: Distributed security*, „Boston University Journal of Science & Technology Law", Vol. 10, 2004; M. L. Rustad, *Private enforcement of cybercrime on the electronic frontier*, „Southern California Interdisciplinary Law Journal", Vol. 11, 2001.

infractorilor ş.a.[9]. În plus, după cum observă Comisia Europeană, norme minime comune în anumite domenii ale infracţionalităţii sunt necesare pentru a consolida încrederea reciprocă între statele membre şi autorităţile judiciare naţionale şi a permite o bună cooperare[10].

O abordare de succes trebuie să aibă în vedere următoarele: crearea de legi eficiente în domeniu, o bună rezolvare a problemelor privind jurisdicţia, cooperarea în investigaţiile internaţionale[11], elaborarea de bune practici în ceea ce priveşte percheziţia în mediul informatic şi confiscarea şi stabilirea unei interacţiuni efective între mediul public şi cel privat[12].

– **Drumul spre un tratat global**

Propunerea unui Tratat Global în Domeniul Cybersecurităţii şi Cyberinfracţionalităţii şi constituirea unei Curţi Penale Internaţionale pentru judecarea infracţiunilor informatice a fost făcută[13]. Un astfel de Tratat, sau un set de tratate ale Naţiunilor Unite, incluzând tratate în domeniul cybersecurităţii, cybercriminalităţii şi alte cybertratate, ar fi un cadru legal pentru pace, justiţie şi securitate în cyberspaţiu şi ar reprezenta un punct de cotitură în reglementarea acestui domeniu. Multe dintre marile state ale lumii, reticente în ceea ce priveşte semnarea şi ratificarea Convenţiei europene privind criminalitatea informatică, susţin puternic adoptarea acestui Tratat al Naţiunilor Unite[14].

---

[9] Vezi J. Vogel, *Towards a Global Convention against Cybercrime*, *First World Conference of Penal Law. Penal Law in the XXIst Century. Guadalajara* (Mexico), 18-23 November 2007; S. L. Hopkins, *Cybercrime Convention: A Positive Beginning to a Long Road Ahead*, „Journal Of High Technology Law", Vol. II, No. 1, 2003.

[10] Vezi Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul economic şi social şi Comitetul regiunilor, *Către o politică a UE în materie penală: asigurarea punerii în aplicare eficace a politicilor UE prin intermediul dreptului penal*, COM(2011) 573 final.

[11] Vezi A. Ehuan, *Cybercrime and Law Enforcement Cooperation*, în J. Bayuk (ed.), *CyberForensics*, Springer's Forensic Laboratory Science Series, 2010.

[12] A se vedea pentru recomandări în domeniu, American Bar Association, *International Guide to Combating Cybercrime* , 2003.

[13] A se vedea, S. Schjolberg şi S. Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime*, Second edition, 2011; S. Schjolberg, *An International Criminal Court or Tribunal for Cyberspace (ICTC)*, A paper for the EastWest Institute (EWI) Cybercrime Legal Working Group, 2011.

[14] A se vedea http://www.cybercrimelaw.net/Cybercrimelaw.html.

Eforturile recente par a indica susţinerea unui asemenea demers. Astfel, organisme şi instituţii internaţionale, cum ar fi Naţiunile Unite[15], Consiliul Europei, Grupul celor 8 State (G8 - SUA, Italia, Canada, Franţa, Germania, Japonia, Regatul Unit şi Federaţia Rusă), ITU, Oficiul Naţiunilor Unite pe Probleme de Droguri şi Crime (UNODC, singurul organism interguvernamental global pe probleme de prevenire a criminalităţii), Organizaţia Statelor Americane (OAS), Organizaţia de cooperare în zona Asia-Pacific, Comunitatea Economică a Statelor West Africane (ECOWAS[16]), Commonwealth of Nations sau OECD au depus şi depun eforturi pentru armonizarea legislaţiei în domeniu.

Naţiunile Unite, la al doisprezecelea Congres pe probleme de prevenire a criminalităţii (desfăşurat în Salvador, Brazilia, 12-19 April 2010), au relevat importanţa găsirii de soluţii la provocările puse de infracţionalitatea informatică. Rezoluţia 64/179, numită *Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity*, atrage atenţia asupra problemelor identificate de Secretarul General (A/64/123), printre acestea infracţionalitatea informatică, şi invită UNODC să exploreze modalităţile de adresare ale acestora. Rezoluţia Resolution 20/7, numită *Promotion of activities relating to combating cybercrime, including technical assistance and capacity-building*, observă necesitatea obţinerii de date asupra noilor forme de infracţionalitate informatică, pentru a elabora răspunsuri adecvate şi subliniază că un răspuns comprehensiv la problema infracţionalităţii în cyberspaţiu trebuie să includă un număr de elemente, incluzând drept penal, posibilitatea dezvoltării unei convenţii internaţionale universale, asistenţă tehnică şi alte măsuri.

G8 a adoptat următoarele *Principii* şi încurajează ţările să le considere în dezvoltarea unei strategii pentru reducerea riscurilor la adresa infrastructurilor informaţionale critice[17]:

---

[15] Vezi întâlnirea grupului de experţi pe probleme de cybercriminalitate, Viena, 17-21 ianuarie 2011; discutarea subiectului criminalităţii în cyberspaţiu la al 12-lea Congres Crime Prevention and Criminal Justice în 2010. În martie 2010, Adunarea Generală a adoptat o nouă Rezoluţie 64/211 - *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*.

[16] Aceasta a adoptat o *Directivă on Fighting Cybercrime* în anul 2009.

[17] Vezi *Principles for Protecting Critical Information Infrastructures*, adoptate de Miniştrii de Justiţie şi Afaceri Interne a G8, mai 2003. A se vedea şi *Ten Principles to*

I. Ţările trebuie să aibă reţele de avertizare privind vulnerabilităţile, ameninţările şi incidentele din cyberspaţiu.

II. Ţările trebuie să mărească nivelul conştientizării pentru a facilita părţilor interesate înţelegerea naturii şi măsurii infrastructurilor informaţionale critice şi a rolului pe care fiecare trebuie să îl joace în protejarea acestora.

III. Ţările trebuie să examineze infrastructurile lor şi să identifice interdependenţe, astfel mărind protecţia unor asemenea infrastructuri.

IV. Ţările trebuie să promoveze parteneriate între cei implicaţi, public şi privat, să partajeze şi să analizeze informaţiile privind infrastructurile critice pentru a preveni, investiga şi răspunde daunelor sau atacurilor produse unor astfel de infrastructuri.

V. Ţările trebuie să creeze şi să menţină reţele de comunicare în situaţii de criză şi să le testeze pentru a asigura siguranţa şi stabilitatea acestora în situaţii de urgenţă.

VI. Ţările trebuie să asigure că politicile privind disponibilitatea datelor i-au în considerare necesitatea protejării infrastructurilor informaţionale critice.

VII. Ţările trebuie să faciliteze facilitate analiza atacurilor asupra infrastructurilor informaţionale critice şi, unde este cazul, să furnizeze aceste informaţii altor ţări.

VIII. Ţările trebuie să realizeze pregătire şi exersare pentru a îmbunătăţi capacităţile de răspuns şi să testeze planurile de continuitate şi urgenţă în cazul unui atac asupra infrastructurilor informaţionale critice şi trebuie să îi încurajeze pe cei implicaţi să realizeze activităţi similare.

IX. Ţările trebuie să asigure că au legi de fond şi procedurale adecvate, cum ar fi cele din Convenţia Consiliului Europei din 23 noiembrie 2001 şi personal pregătit pentru a permite investigarea şi urmărirea în justiţie a atacurilor infrastructurilor informaţionale critice şi să coordoneze asemenea investigaţii cu alte ţări, după cum este adecvat.

X. Ţările trebuie să se implice în cooperare internaţională, când este cazul, pentru a asigura infrastructurile informaţionale critice, incluzând dezvoltarea şi coordonarea sistemelor de avertizare de urgenţă, partajarea şi analizarea informaţiilor privind vulnerabilităţi, ameninţări şi incidente şi coordonarea investigaţiilor atacurilor asupra unor asemenea infrastructuri în acord cu legile naţionale.

XI. Ţările trebuie să promoveze cercetarea şi dezvoltarea naţională

Combat High-Tech Crime, Action Plan to Combat High-Tech Crime. A se vedea şi Recomandarea OECD din anul 2008, [C(2008)35].

şi internaţional şi să încurajeze aplicarea tehnologiilor de securitate certificate conform standardelor internaţionale.

În mai 2007, secretarul general al Uniunii Internaţionale a Telecomunicaţiilor a lansat Agenda Globală a Cybersecurităţii (*Global Cybersecurity Agenda*), cadru al cooperării internaţionale în domeniu, având ca obiectiv central sinergia eforturilor tuturor factorilor cheie la nivel global în realizarea unei societăţii a informaţiei mai sigură pentru toţi. Un grup de experţi la nivel înalt de peste 100 persoane a fost creat pentru a asista Uniunea Internaţională a Telecomunicaţiilor în dezvoltarea propunerilor de strategie. Acest grup a realizat un raport care a fost făcut public în noiembrie 2008 şi include cinci piloni strategici - măsuri legale, măsuri de ordin tehnic şi procedural, măsuri de ordin organizaţional, construcţia capacităţii şi cooperare internaţională şi şapte obiective esenţiale:

Elaborarea unei legislaţii în domeniu aplicabile global, interoperabile cu măsurile naţionale sau regionale existente;

Elaborarea de strategii pentru crearea de structuri organizaţionale şi politici naţionale şi regionale pe problema criminalităţii în cyberspaţiu;

Dezvoltarea unei strategii pentru stabilirea de criterii de securitate minime şi scheme de acreditare pentru programele şi sistemele informatice global acceptate;

Dezvoltarea de strategii pentru crearea unui cadru global pentru monitorizare, avertizare şi răspuns la incidente pentru a asigura coordonare transfrontalieră între iniţiativele noi şi cele existente;

Dezvoltarea de strategii pentru crearea şi susţinerea unui sistem de identitate generic şi universal şi a structurilor organizaţionale necesare pentru asigurarea recunoaşterii credenţialelor digitale pentru indivizi peste graniţe geografice;

Dezvoltarea unei strategii globale pentru facilitarea creării de capacitate umană şi instituţională pentru îmbunătăţirea cunoaşterii şi a know-how-ului trans-sectorial şi în domeniile mai sus menţionate;

Un cadru potenţial pentru o strategie globală pentru cooperare internaţională, dialog şi coordonare în domeniile

mai sus menţionate)[18].

În 19 mai 2011, ITU şi UNODC au semnat un acord de colaborare pentru a acţiona împreună în combaterea ameninţării în continuă creştere a criminalităţii informatice. Cele două organizaţii au afirmat că acest parteneriat are ca scop construirea unui Internet mai sigur pentru consumatori şi afaceri, prin punerea laolaltă a expertizei şi resurselor în a ajuta naţiunile lumii să creeze o legislaţie adecvată care să facă faţă provocărilor în domeniu. Intenţia este de a acorda asistenţă guvernelor pentru stabilirea unui cadrul legal corespunzător şi standarde de securitate, pentru a face atacurilor electronice[19]. Adiţional, a fost creat IMPACT (International Multilateral Partnership Against Cyber Threats), agent executiv al ITU pe probleme de infracţionalitate în Cyberspaţiu, parteneriat public-privat care cuprinde 137 de naţiuni, inclusiv România[20].

– **Conţinutul noului tratat global**

În legătură cu infracţiunile care ar trebui incluse într-un Tratat Global au existat discuţii şi controverse. Astfel, s-a avut în vedere faptul că nu în toate ţările încălcările în domeniul dreptului de autor sunt considerate infracţiuni şi, din acest motiv, au existat membrii care nu au fost de acord cu înscrierea lor ca infracţiuni în Tratatul global. De asemenea, infracţiunile de rasism, xenofobie şi pornografie infantilă sunt considerate de unii membrii infracţiuni tradiţionale, nu specifice cyberspaţiului, deşi incidenţa lor în mediul online şi uşurinţa cu care sunt comise au făcut experţii care au elaborat Convenţia Europeană să le prevadă şi să le propună şi pentru Tratatul global. Datorită frecvenţei şi gravităţii, au fost propuse pentru includere furtul de identitate, spam-ul, *phishing*-ul, actele preparatorii în comiterea infracţiunilor, atacurile masive asupra infrastructurilor de informaţii critice şi actele de terorism prin utilizarea tehnologiile informatice.

Multe dintre prevederile acestui Tratat Global sunt cele care compun Convenţia Europeană în domeniul criminalităţii informatice din anul 2001 (intrată în vigoare la 1 iulie 2004), considerată încă o un moment istoric de referinţă, piatra de temelie a cadrului legal global în

[18] Vezi ITU, *Understanding cybercrime: A guide for developing countries*, 2011.

[19] Vezi http://www.unodc.org/unodc/en/frontpage/2011/May/unodc-and-itu-to-cooperate-more-closely-to-make-the-internet-safer.html.

[20] Vezi http://www.impact-alliance.org/home/index.html.

domeniu. Numărul total de state care au ratificat Convenţia este 32, iar 15 state au semnat Convenţia, dar nu au ratificat-o[21]. Unele state au preferat să utilizeze Convenţia ca pe un ghid de elaborarea a propriei legislaţii sau ca o referinţă în dezvoltarea acesteia, prin implementarea standardelor şi principiilor pe care aceasta le conţine, în concordanţă cu propriul sistem legal şi propriile practici. Deşi importantă, Convenţia Consiliului Europei privind criminalitatea informatică nu pare să mai aibă forţa necesară (există state membre ale Uniunii Europene care nu au semnat-o sau ratificat-o, deşi recent li s-a recomandat puternic să o facă[22]) pentru a ţine pasul cu provocările ridicate de un domeniu într-o continuă dezvoltare[23].

Convenţia Europeană încă este singurul cadru legislativ deschis tuturor statelor lumii. Faptul că nu toate ţările la nivel global au semnat această Convenţie nu a fost şi nu este singura piedică în îndeplinirea obiectivelor de asigurare a securităţii în cyberspace. Sigur, semnarea şi ratificarea acesteia nu înseamnă neapărat reducerea, cu atât mai puţin eradicarea, acestui tip de criminalitate, ci un întreg set de măsuri complexe, tehnice şi legale. Un exemplu poate fi găsit în România, care a fost printre primele ţări care au semnat şi ratificat Convenţia, dar unde atacurilor informatice creează probleme; în plus, în anul 2008, după cum s-a semnalat şi în studii internaţionale, a refuzat să îl extrădeze pe un infractor informatic (V. Duiculescu), arestat cu ajutorul FBI pentru că a atacat servere NASA, a realizat fraude însemnate pe eBay, deşi ratificase Convenţia şi articolele referitoare la extrădare sunt foarte clare[24] (de remarcat cazul în care doi români au fost extrădaţi în SUA pentru acuze că ar fi folosite scheme de tip *phishing* împotriva clienţilor PayPal,

---

[21] La data de 5 octombrie 2011 - a se vedea detalii la locaţia http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG. România a ratificat Convenţia prin Legea nr. 64/2004, publicată în Monitorul Oficial Nr. 343 din 20 aprilie 2004.

[22] A se vedea Concluziile Consiliului Uniunii Europene privitoare la Planul de Acţiune pentru a implementa o strategie coerentă în combaterea criminalităţii informatice din 26 aprilie 2010.

[23] Vezi o critică a acesteia în N. E. Marion, *The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation*, „International Journal of Cyber Criminology", Vol 4 (1&2), Jan – July şi July - December (Combined Issue), 2010, p. 699–712.

[24] Vezi „România liberă", 19 aprilie 2008, care îl citează pe şeful Serviciului de Combatere a Criminalităţii Informatice al Inspectoratului General al Poliţiei Române.

Citibank şi a altor instituţii financiare[25]).

În primul rând, Convenţia este criticată pentru că are în vedere comportamentele criminale în mediul digital de la sfârşitul anilor '90, în timp ce infractorii au devenit din ce în ce mai sofisticaţi, iar mediul digital, într-o dezvoltare continuă, le oferă numeroşi vectori de atac. În al doilea rând, terminologia utilizată de Convenţie nu mai este considerată una care să exprime precis şi complet realităţile din noul mediu digital curent. O altă piedică în îndeplinirea obiectivelor declarate în Preambul Convenţiei este aceea că aceasta nu s-a bucurat de un nivel de acceptare similar în toate regiunile (puţine ţări din afara Europei au semnat şi ratificat Convenția, SUA fiind cea mai importantă dintre acestea[26]), deşi în articolele referitoare la aderare şi semnare Convenţia este una deschisă tuturor statelor lumii. Chiar dacă principiile şi standardele Convenţiei sunt acceptate, discuţiile care au avut loc în cadrul întâlnirilor grupului de experţi la nivel înalt au arătat că această Convenţie este în continuare percepută de state din alte regiuni ca o lege europeană şi aşa va rămâne, orgoliile existând, din păcate, şi la nivel înalt. În concluzie, este nevoie de acest tratat al Naţiunilor Unite, ca rezultat al acordului global, cu acceptul tuturor regiunilor (grupul de experţi a ţinut să precizeze că s-a ţinut seama de prevederile Convenției ca un exemplu de inițiativă regională şi a fost inclusă în recomandare[27]).

– Concluzie

Până la intrarea în vigoare a acestui unui Tratat global, considerăm important ca prevederile din cadrul acestuia să fie analizate şi dezbătute la toate nivelele implicate. Acest lucru ar elimina una dintre problemele pe care Convenţia Europeană în domeniul criminalităţii informatice le-a întâmpinat la semnare şi ratificare: la realizarea ei consultarea largă nu s-a realizat. Mai mult, statele ar trebui să-şi revizuiască legislaţia în domeniu, adaptând-o după acest Tratat, care are în vedere, pe de o parte, tendinţele recente ale criminalităţii informatice şi, pe de cealaltă parte, cele mai moderne şi complexe mecanisme de luptă împotriva acestei forme de

[25] Vezi SANS, *NewsBites*, oct., 2, Vol. 11, nr. 78, 2009.

[26] SUA au semnat Convenţia în 23/11/2001, au ratificat-o în 29/9/2006 şi a intrat în vigoare la 1/1/2007.

[27] Un model de elaborare a legislației in domeniu este *ITU Toolkit for Cybercrime Legislation*, publicat în mai 2009; acesta a fost elaborat de Comitetul Privacy & Computer Crime al American Bar Association (primul fiind elaborat în anul 2003).

criminalitate. România este una dintre ţările care trebuie să-şi adapteze normativul juridic, sursa legislaţiei româneşti în materie, atât în ceea ce priveşte Legea nr. 161/2003, cât şi noul Cod Penal fiind Convenţia Europeană în domeniul criminalităţii informatice.