REPERE ŞI PERSPECTIVE JURIDICE ÎN REGLEMENTAREA CRIMINALITĂȚII INFORMATICE

Radu Cristian*

ABSTRACT:

Cybercrime has to be prevented and fought by global, pertinent regulations, capable to handle both the technologic inefficiencies in terms of security and the legislative ones characterizing contemporary society. In this respect, the author believes there is need for a partitioned leadership at world level, capable to respond and adapt in due time to the major technologic changes of society. The solutions proposed for the regulation of cybercrime include establishment of an International Criminal Court judging cybercrimes and also a Global Treaty in the field of cyber security and cybercrime.
Keywords: **cybercrime, information society, cyber-attacks, Council of Europe, European Parliament, European Commission, ACTA.**

RÉSUMÉ

La cybercriminalité doit être prévenue et contrôlée par des règlements internationaux, pertinents, capables de gérer les inefficacités technologiques celles de sécurité et des inefficacités juridiques dans la société. À cet égard, ont est noté la nécessité d'un leadership partagé dans le monde entier à réagir et à s'adapter aux changements de temps technologiques de la société. Parmi les principales solutions proposées par la législation contre la cybercriminalité se de travailler et de lutter pour avoir une Cour pénale internationale de poursuivre les infractions dans le domaine des informations et de proposer une approche commun ainsi que l'existence d'un traité globale pour la cybercriminalité.
Mots-clés: **La cybercriminalité, société de l'information, les attaques, le Conseil de l'Europe, Parlement européen, Commission européenne, l'ACTA.**

În secolul XX, cel mai mare eveniment tehnologic şi social, în acelaşi timp, a fost apariția Internetului. În domeniul Ştiinței şi Tehnologiei Informației, marile evenimente tehnologice, cu importante consecințe sociale, au fost descoperirea tranzistorului, a circuitului integrat, a microprocesorului şi a calculatorului electronic. Internetul nu este numai un fenomen tehnologic, ci şi unul social, prin participarea utilizatorilor, din ce în ce mai numeroşi, la structurarea lui actuală.

Dezvoltarea Internetului a depins evident de tehnologie, dar în egală măsură şi de factorii sociali, care s-au îmbinat cu factorii tehnologici pentru ca Internetul să ajungă ceea ce a devenit astăzi[1]. Odată instaurat în fibrele societății, Internetul a produs şi produce consecințe noi pentru societate.

Simbolul convergenței dintre telecomunicații, calculatoare şi tehnologia de control, Internetul, reprezintă unul dintre vectorii Societății informaționale[2]. În prezent informația este omniprezentă în activitățile umane, tehnologia informației şi de comunicații, de la calculatorul personal la rețeaua Internet, de la telefonul mobil şi tablete până la rețelele globale de comunicații. Informația se dezvoltă continuu şi ne transformă şi ne influențează viața, relațiile şi organizarea societății.

* Dr., cercetător ştiinţific.

[1] A se vedea M. Drăgănescu, *Societatea informațională şi a cunoaşterii*. *Vectorii societății cunoaşterii*, Academia Română, Bucureşti, 2001, p. 6.

[2] A se vedea St. Iancu**,** *Unele probleme sociale, economice, juridice şi etice ale utilizării tehnologiei informației şi comunicațiilor,* Academia Română, Bucureşti, septembrie 2001.

Societatea Informațională este caracterizată, în principal, prin ubicuitatea tehnologiei informației şi prin dinamica dezvoltării infrastructurii rețelelor de calculatoare, care constituie coordonatele referențiale ale actualei etape de evoluție din domeniul Tehnologiei Informației şi Comunicațiilor (TIC). În acest context, nivelul cel mai înalt de evidențiere al convergenței dintre telecomunicații şi calculatoare este reprezentat de Internet, care reprezintă dimensiunea globală a acesteia.

Dezvoltările din domeniul TIC din ultima perioadă au transformat deja societatea sub multe aspecte. Cu toate acestea, se consideră că şi țările dezvoltate din punct de vedere industrial care beneficiază, comparativ cu celelalte țări, din plin de noile facilități, nu se află decât la prima etapă a exploatării unor tehnologii, care nu s-au maturizat şi care se află încă în plină dezvoltare.

Societatea Informațională – Societatea Cunoaşterii (SI-SC) este concepută ca un mediu foarte diferit, fără precedent, în care implementarea ultimelor realizări tehnice şi procedurale trebuie să meargă în paralel cu adoptarea de noi soluții juridice, care să monitorizeze efectele negative ale impactului utilizării TIC.

Potențialul Internetului de a informa, de a educa, de a distra şi de a se constitui ca suport pentru organizarea şi desfăşurarea afacerilor la scară globală este considerabil. Dar, ca orice tehnologie inovatoare, Internetul poartă şi un conținut potențial nociv, putând fi folosit şi pentru organizarea şi desfăşurarea de activități criminale.

Examinarea activităților cu caracter ilegal derulate prin intermediul mijloacelor electronice evidențiază evoluția ascendentă a fenomenului din domeniul cybercrime la nivel global, fiind relevate tendințe de manifestare sub forme organizate, din ce în ce mai complexe, generatoare de efecte directe asupra tuturor domeniilor economice şi sociale, aspect ce poate genera riscuri de concretizare a unor categorii de amenințări asimetrice la adresa sistemelor informatice.

Modificările tehnologice sau introducerea unei noi tehnologii, de regulă, impun modificări corespunzătoare în cadrul legislativ existent, în organizarea instituțiilor, în politica afacerilor, în schimbarea abilităților personale ale celor implicați şi chiar transformarea mentalităților. O nouă tehnologie poate să facă fezabile activități sau acțiuni care nu se puteau realiza anterior, când a fost elaborat cadrul legislativ şi, de aceea, asemenea acte şi activități nu pot fi ilegale sau criminale până ce nu se elaborează o lege care să le interzică.

Atacurile informatice asupra disponibilității serviciilor din mediu TIC prcum şi ritmul susținut de penetrare asupra comunicațiilor electronice determină dezvoltarea continuă a unui mediu virtual cu potențial infracțional, afectând în mod esențial modalitățile concrete prin care structurile decidente trebuie să reacționeze şi să intervină în mod proactiv, în scopul asigurării echilibrului social, respectiv a protecției, conform reglementărilor principale din domeniu, a drepturilor şi libertăților fundamentale ale omului. Astfel, noile tehnologii informatice au creat unele dintre cele mai importante provocări şi oportunități, fiind evidențiate de cei care susțin, promovează şi apără drepturile omului şi protecția vulnerabilităților sociale. Există un defazaj semnificativ între ritmul de dezvoltare din sfera tehnologiei informației şi modul în care mediul legislativ reacționează la aceste transformări, efectul constând în aceea că evoluțiile din acest domeniu pot scapa de sub controlul normelor juridice, putând fi încălcate drepturile omului.

Potențialul uriaş din domeniul TIC trebuie integrat şi valorificat eficient în toate direcțiile în care se regăseşte amprenta acestor tehnologii revoluționare, în respectul unor principii, valori şi norme comune, având în atenție şi posibilitatea de a contracara sau preveni posibilele consecințe nocive ale unei utilizări necontrolate a acestei resurse[3].

[3] A se vedea Irina Moroianu Zlătescu, *Drepturile omului şi noile tehnologii ale informației şi comunicării*,

Utilizările TIC în sfera activităților circumscrise drepturilor omului pot fi grupate în patru domenii principale din punct de vedere al angajării rețelelor de comunicații, astfel: guvernamentale, individuale, afectate ONG-urilor şi destinate instituțiilor supranaționale. Această ierarhizare a fost acreditată în măsura în care comunicarea s-a realizat efectiv în domeniul specific, cu relevanță în modul de rezolvare a problemelor prin consultarea, colaborarea şi sprijinul acordat de organismele internaționale acreditate în domeniul drepturilor omului. Astfel, tehnologia informației a devenit un suport catalizator pentru eficientizarea şi operaționalizarea activităților din domeniu, oferind o platformă globală pentru mişcarea de opoziție ce contestă regimurile totalitare şi dictatura militară, încercările guvernelor de a reduce libertățile şi drepturile cetățenilor. Stabilirea de noi relații între entitățile societății civile, intensificată şi susținută de dinamica TIC, a contribuit în multe direcții la dezvoltarea unei noi diplomații a drepturilor omului, care a evidențiat aşa-numita tensiune dintre putere şi moralitate şi care a schimbat predispoziția unor organizații, cum este O.N.U., de a aprecia selectiv anumite regiuni ale lumii față de altele.

Implementarea tehnologiilor informatice în aproape toate domeniile vieții, precum şi evoluția infrastructurilor de comunicații la dimensiuni globale, au făcut ca infracționalitatea comisă prin intermediul mijloacelor din sfera tehnologiei informației să fie mai elaborată, mai periculoasă şi mai acută la nivel mondial. Un studiu al factorilor generatori de activități criminale a arătat că rețelele de comunicații şi generațiile modern de echipamente din domeniul TIC prezintă caracteristici specifice, care sunt de mare utilitate pentru proliferarea activităților infracționale. Tehnologiilor sofisticate utilizate de făptuitori, lacunele în instruirea specifică a personalului din cadrul organelor de urmărire penală, lipsa unui plan eficient de reacție în caz de atacuri şi, nu în ultimul rând, carențele unei legislații specifice domeniului, precum şi deficiențele unor proceduri de aplicare, care să ofere posibilitatea unei intervenții operative cauzează mari dificultăți pentru potențialele victime de a contracara, de a se apăra şi de a pune în aplicare normativele legale.

Societatea a căutat căi şi modalități, care să-i asigure o cât mai bună adaptare la schimbările majore tehnologice. Pe măsură ce au apărut noi necesități, noi probleme şi s-au identificat noi mijloace tehnice de soluționare, de satisfacere a necesităților vieții, s-au creat noi instituții, care au urmărit să amortizeze şocurile noilor tehnologii şi să descurajeze abuzurile care ar fi putut duce la efecte necontrolabile. Cu toate acestea, aplicarea unor noi tehnologii, chiar şi în cazul soluționării unor probleme curente de producție, de creştere a bunăstării, de îmbunătățire a stării de sănătate, a dat naştere, uneori, la efecte secundare nedorite a căror soluționare a necesitat şi necesită noi eforturi.

Polemicile asupra drepturilor omului şi a tehnologiilor informației s-au mutat dincolo de tema dreptului la intimitate şi al asigurării protecției informațiilor, cuprinzând probleme legate de modul în care trăim şi suntem guvernați, precum şi de criptografierea mesajelor vehiculate în cadrul rețelelor informatice, dreptul de accesare a oricăror baze de date de către autoritățile abilitate pentru activități ce vizează securitatea națională, contracararea terorismului, combaterea crimei organizate.

Statisticile şi prognozele efectuate la nivel mondial asupra fenomenului de cybercrime, a evoluției obiectivelor, formelor de manifestare, precum şi a metodelor şi mijloacelor utilizate în mediul cibernetic, ritmul accelerat de evoluție şi afectare a serviciilor şi rețelelor din domeniul TIC, precum şi a punctelor slabe asociate acestui proces dinamic, asigură condițiile favorabile pentru utilizarea capacităților agresionale distructive ce pot fi incluse în categoria atacurilor informatice de către organizații teroriste în scopuri şi acțiuni specific terorismului cybernetic. Nivelul de risc estimat pentru astfel de amenințări este corelat, pe termen scurt, mediu şi lung, cu mutațiile mediului de securitate internațional şi cu nivelul

„Drepturile Omului", nr. 4/2006, p. 3 şi urm.

general de risc estimat pentru ameninţarea teroristă. Pentru reducerea şi controlul riscurilor asociate în cadrul societăţii informaţionale, procesul de aplicare a legii trebuie susţinut la nivelul principalelor organisme cu rol şi atribuţii în domeniul de referinţă, prin asigurarea unei bune comunicări internaţionale, a unei abordări unitare şi coerente a activităţilor subsumate prevenirii şi combaterii criminalităţii informatice, în scopul furnizării către forumurile decizionale a acelor date şi informaţii analitico-sintetice, ce pot permite adoptarea şi stabilirea deciziilor executive optime, de natură să minimizeze cauzele şi sursele generatoare ale fenomenului, precum şi de diminuare a efectelor[4].

Convergenţa dintre telecomunicaţii, serviciile multimedia şi tehnologia informaţiei şi comunicaţii, ce orientează dezvoltarea Societăţii Informaţionale Globale (Global Information Society – GIS), este responsabilă pentru transformările economice şi politice dintr-o multitudine de sectoare de activitate. Beneficiile din domeniul TIC nu se regăsesc numai în diversitatea funcţionalităţilor, ci mai ales în varietatea şi versatilitatea aplicaţiilor oferite.

Una dintre soluţiile de a distinge complexitatea relaţionării dintre TIC şi schimbările sociale, în contextul drepturilor omului, se află în evaluarea gradului de interactivitate funcţională din cadrul uneia dintre tehnologiile implicate în procesul de amplificare a schimbului de informaţii.

Ideea că noile tehnologii de comunicare pot determina schimbări la nivel social, în sensul

stabilirii unei competenţe sporite a protecţiei drepturilor omului la nivel internaţional, relevă faptul că un factor important al susţinerii şi respectării drepturilor omului îl constituie modul în care puterea este administrată şi dirijată de cei ce controlează şi reglează sfera comunicaţiilor[5].

La dezvoltarea Societăţii Informaţionale trebuie să contribuie toate părţile interesate, prin adoptarea unei viziuni comune şi explicite asupra modului de implementare a noilor tehnologii informaţionale, în strânsă legătură cu drepturile omului, prin armonizarea politicilor de dezvoltare cu principiile de utilizare ale cyberspaţiului.

Extinderea utilizării tehnicii de calcul în aproape toate domeniile vieţii, precum şi conectarea calculatoarelor în reţele internaţionale a făcut ca infracţiunea comisă cu ajutorul sau prin intermediul calculatorului să fie mai diversă, mai periculoasă şi mai prezentă la nivel internaţional. O analiză a factorilor generatori de acţiuni criminale a arătat că reţelele de comunicare şi calculatorul modern prezintă caracteristici specifice, care sunt de mare utilitate pentru criminali şi implică mari dificultăţi pentru potenţialele victime şi pentru aplicarea legii (probleme complexe de securizarea sistemelor, multiplicitatea sistemelor hard şi soft, lipsa de experienţă a multor utilizatori, anonimatul comunicării, criptarea şi mobilitatea internaţională). Între ţintele grupurilor care activează în domeniul crimei organizate, ai profesioniştilor în spionajul economic şi al serviciilor secrete din întreaga lume, care exploatează aceste noi caracteristici ale acţiunilor criminale cibernetice se numără atât guverne, oameni de afaceri, cât şi utilizatori particulari.

Impactul negativ al utilizării TIC a fost remarcat în următoarele tipuri de infracţiuni: încălcarea caracterului privat al datelor personale, violarea drepturilor de proprietate intelectuală, infracţiuni economice, infracţiuni bancare, diseminarea de materiale cu conţinut ilegal sau nociv. Analiza situaţiei a evidenţiat că infracţiunile comise prin intermediul calculatorului s-au focalizat în domeniul crimei economice, în special prin comiterea de fraude cu ajutorul calculatorului, spargeri de coduri, spionaj economic, furt de secrete tehnologice.

Folosirea TIC în domeniile tradiţionale ale crimei organizate (de ex. comerţul cu arme

[4]A se vedea E. Bîsceanu, *Fenomenul criminalităţii informatice în România*, Revista Intelligence, nr. 15, 2009.

[5]A se vedea A. Selian, *ICTs in Support of Human Rights, Democracy and Good Governance*, www.itu.int/osg/spu/wsis-themes/humanrights.

şi droguri) capătă o importanţă tot mai mare. Studiul celor patru direcţii de acţiune infracţională prin utilizarea TIC ilustrează faptul că internetul a devenit ţara celor patru cavaleri ai Apocalipsei: crima organizată, terorismul, traficul de arme şi droguri, pedofilia[6].

Datorită conţinutului variat, infracţiunile informatice cuprind pe lângă actele infracţionale clasice şi acţiuni specifice mediului cibernetic (virusarea infrastructurilor informaţionale, falsificarea instrumentelor electronice bancare, spam-ingul, terorim cybernetic, etc.).

Ca urmare a dezvoltărilor din domeniul TIC, infracţionalitatea informatică a crescut în complexitate şi importanţă, implicând, din ce în ce mai mult, crima organizată, hacking-ul, utilizarea botnet-urilor, furtul de date din interior şi atacuri masive asupra infrastructurilor informatice critice, fiind prolifice şi activităţi din domeniul cyberterorismului.

Activităţile făptuitorilor nu pot fi contracarate efectiv cu măsuri doar la nivel naţional, fiind nevoie de un efort concertat al industriei din domeniul TIC, al guvernelor, al organelor cu atribuţii de punere în aplicare a legislaţiei din domeniu şi al cetăţenilor tuturor ţărilor, chiar dacă, în trecut, au existat şi opinii conform cărora nu este necesară armonizarea legilor sau procedurilor privind criminalitatea informatică, cazurile de infracţionalitate informatică nefiind considerate decât cazuri obişnuite, care au în comun folosirea de tehnologii informatice şi de comunicaţii[7].

Cyberspaţiul pune în discuţie noţiunile tradiţionale de jurisdicţie[8] 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 de date, a lipsei de sisteme corespunzătoare pentru comunicaţiile digitale, existenţa unor legi inadecvate[9], disparităţilor existente în ceea ce priveşte prevederile legale şi lipsei de expertiză la nivelul organelor judiciare[10] şi de investigare. Natura criminalităţii informatice este una globală, prin urmare şi natura problemelor cadrului legal în domeniu, impune necesitatea unui consens pentru armonizarea legislaţiei şi a procedurilor de investigare şi incriminare, noi forme de drept multilateral sau globalizat[11].

Niciun stat nu poate de unul singur să elimine sau măcar să reducă problema înfracţionalităţii în Cyberspaţiu. Este nevoie de leadership partajat şi determinare la nivel mondial. Un demers în acest sens a fost iniţiat de Convenţia Europeană privind criminalitatea informatică (ETS No. 185)[12], care introduce noi canale de comunicare în lupta împotriva acestui tip de infracţionalitate şi defineşte un set comun de standarde pentru incriminarea faptelor ilicite legate de tehnologia informaţiei. Considerăm că prevederile Convenţiei sunt de bun augur, însă acestea trebuie continuate şi îmbunătăţite în ceea ce priveşte detalierea elementelor necesare în cazul fiecărei infracţiuni, specificarea unor proceduri consistente pentru investigarea şi urmărirea în justiţie a infractorilor ş.a.[13]. În plus, după cum observă Comisia Europeană, sunt necesare norme minime comune în anumite domenii ale infracţionalităţii, pentru a consolida încrederea reciprocă între statele membre şi autorităţile judiciare naţionale şi pentru a

[6] *Ibidem,* pp. 2-5.

[7] A se vedea F. H. Easterbrook, *Cyberspace and the Law of the Horse*, University Of Chicago Legal Forum, 207.

[8] A se vedea S. W. Brenner şi B. J. Koops, *Approaches to Cybercrime Jurisdiction*, 4 Journal of High Technology Law.

[9] A se vedea D. B. Hollis, An e-SOS for Cyberspace, Harvard International Law Journal, Vol. 52, No. 2, Summer (2011).

[10] A se vedea Raportul grupului de experţi ITU pentru elaborarea Tratatului la nivel global în domeniul cybersecurităţii şi criminalităţii informatice

[11] A se vedea M. Goodman, *International Dimensions of Cybercrime*, în S. Ghosh şi E. Turrini (eds.), *Cybercrimes: A Multidisciplinary Analysis*, 2010.

[12] A se vedea *Convenţia privind Criminalitatea Informatică*, ETS 185, Consiliul Europei, din 23 noiembrie 2001, Budapesta. Convenţia a fost semnată de 46 de ţări dintre care 4 nu sunt membre ale Consiliului. Dintre acestea, 24 de ţări (inclusiv România) au ratificat Convenţia, Statele Unite fiind singura ţară non-membră care a ratificat-o.

[13] A se vedea I. Vasiu şi L. Vasiu, *Criminalitatea în Cyberspaţiu*, Ed. Universul Juridic, Bucureşti, 2011, p. 124

permite o bună cooperare între acestea[14].

Considerăm că ar fi oportun să se creeze legi eficiente în domeniu, care să ducă la o bună rezolvare a problemelor privind jurisdicția, cooperarea în investigațiile internaționale[15], la elaborarea de bune practici în ceea ce priveşte percheziția şi confiscarea în mediul informatic şi la stabilirea unei interacțiuni efective între mediul public şi cel privat[16].

Propunerea unui Tratat Global în Domeniul Cybersecurității şi Cyberinfracționalității şi constituirea unei Curți Penale Internaționale pentru judecarea infracțiunilor informatice a fost făcută[17]. Un astfel de Tratat, sau un set de tratate ale Națiunilor Unite, incluzând tratate în domeniul cybersecurității, cybercriminalității şi alte cybertratate, ar fi un cadru legal pentru pace, justiție şi securitate în cyberspațiu 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 Convenției Europene privind criminalitatea informatică, susțin puternic adoptarea acestui Tratat al Națiunilor Unite[18].

Eforturile recente par a indica susținerea unui asemenea demers. Astfel, organismele şi instituțiile internaționale, cum ar fi Națiunile Unite, Consiliul Europei, Grupul celor 8 state, ITU, Oficiul Națiunilor Unite pe Probleme de Droguri şi Crime (UNODC), Organizația Statelor Americane (OAS), Organizația de cooperare în zona Asia-Pacific, Comunitatea Economică a Statelor Vest-Africane (ECOWAS), Commonwealth of Nations sau OECD, îşi conjugă eforturile pentru armonizarea legislației în domeniu.

Națiunile Unite, la al doisprezecelea Congres pe probleme de prevenire a criminalității (desfăşurat în Salvador, Brazilia, 12-19 April 2010), au relevant importanța găsirii de soluții la provocările puse de infracționalitatea informatică.

Rezoluția 64/179, numită Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity, atrage atenția asupra problemelor identificate de Secretarul General (A/64/123), printe acestea infracționalitatea informatică, şi invită UNODC să exploreze modalitățile de adresare ale acestora. Rezoluția Resolution 20/7, numită Promotion of activities relating to combating cybercrime, including technical assistance and capacitz-building, observă necesitatea obținerii de date asupra noilor forme de infracționalitate informatică, pentru a elabora contramăsuri adecvate, şi subliniază că un răspuns comprehensive la problema infracționalității în cyberspațiu trebuie să includă un număr de elemente, incluzând drept penal, posibilitatea dezvoltării unei convenții internaționale universal, asistență tehnică şi alte măsuri.

G8 a adoptat un set de unsprezece Principii şi încurajează țările să le ia în considerare în dezvoltarea unei strategii pentru reducerea riscurilor la adresa infrastructurilor informatice critice[19].

În mai 2007, secretarul general al Uniunii Internaționale a Telecomunicațiilor (ITU) a lansat Agenda Globală a Cybersecurității (Global Cybersecurity Agenda), cadru al cooperării internaționale în domeniu, având ca obiectiv central sinergia eforturilor tuturor factorilor-cheie la nivel global

[14] A se vedea 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 pena l"*, COM , 2011, p. 573 şi urm.

[15] A se vedea A. Ehuan, *Cybercrime and Law Ennforcement Cooperation*, în J. Bayuk(ed.), *Cyber Forensics*, Springer's Forensic Laboratory Science Series,2010.

[16] A se vedea American Bar Association, *International Guide to Combating Cybercrime*, 2003.

[17] 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.

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

[19] A se vedea *Priciples for Protecting Critical Information Infrastructures,* adoptate de Miniştrii de Justiție şi Afaceri Interne ai G8.

în realizarea unei societăți informaționale mai sigure pentru toți. Un grup de experți la nivel înalt, de peste o sută de persoane, a fost creat pentru a asista ITU în dezvoltarea propunerilor de strategie. Acest grup a realizat un raport, care a fost făcut public în noiembrie 2008 şi care include cinci piloni strategici – măsuri legale, măsuri de ordin etnic şi procedural, măsuri de ordin organizațional, construcția capacității şi cooperare internațională – şi şapte obiective esențiale:

1. elaborarea unei legislații în domeniu aplicabile global, interoperabile cu măsurile naționale sau regionale existente;
2. elaborarea de strategii pentru crearea de structuri organizaționale şi politici naționale şi regionale pe problema criminalității în cyberspațiu;
3. dezvoltarea unei strategii pentru stabilirea de criterii de securitate minime şi scheme de acreditare pentru programele şi sistemele informatice global acceptate;
4. dezvoltarea de strategii pentru crearea unui cadru global pentru monitorizare, avertizare şi răspuns la incidente, pentru a asigura coordonarea transfrontalieră între inițiativele noi şi cele existente;
5. dezvoltarea de strategii pentru crearea şi susținerea unui sistem de identitate generic şi universal şi a structurilor organizaționale necesare pentru asigurarea recunoaşterii credențialelor digitale pentru indivizi peste granițe geografice;
6. dezvoltarea unei strategii globale pentru facilitarea creării de capacitate umană şi instituțională pentru îmbunătățirea cunoaşterii şi a know-how-ului transsectorial şi în domeniile mai sus menționate;
7. un cadru potențial pentru o strategie globală pentru cooperare internațională, dialog şi coordonare în domeniile mai sus menționate[20].

În data de 19 mai 2011, ITU şi UNODC au semnat un acord de colaborare pentru a acționa în combaterea amenințării criminalității informatice. Cele două organizații au afirmat că acest parteneriat are ca scop constituirea unui Internet mai sigur pentru utilizatori şi afaceri, prin coroborarea expertizei şi a resurselor în a ajuta națiunile lumii să creeze o legislație adecvată, care să facă față provocărilor din domeniu. Intenția este de a acorda asistență guvernelor pentru stabilirea unui cadru legal corespunzător şi standarde de securitate, pentru a face față atacurilor din mediul informatic[21]. Adițional a fost creat IMPACT (International Multilateral Partnership Against Cyber Threats), agent exclusiv al ITU pe problem de infracționalitate în Cyberspațiu, parteneriat public-privat care cuprinde 137 națiuni[22].

În legătură cu infracțiunile ce ar trebui incluse într-un Tratat global au existat discuții şi controverse. Astfel, s-a avut în vedere faptul că încălcările în domeniul dreptului de autor nu sunt considerate infracțiuni în toate țările şi, din acest motiv, au existat membri, care nu au fost de acord cu înscrierea lor ca infracțiuni în Tratatul global. Totodată, infracțiunile de rasism, xenofobie şi pornografie infantilă sunt considerate de unii membri infracțiuni tradiționale, nu specific cyberspațiului, deşi incidența lor în mediul online şi uşurința cu care sunt comise au făcut ca experții, care au elaborat Convenția Europeană să le prevadă şi să le propună şi pentru Tratatul global. Datorită frecvenței şi gravității, au fost propuse pentru includere furtul de identitate, spam-ul, phishing-ul, actele preparatorii în comiterea infracțiunilor, atacurile masive asupra infrastructurilor informatice critice şi actele de terorism prin utilizarea tehnologiilor informatice.

Convenția privind criminalitatea informatică adoptată în cadrul Consiliului Europei cuprinde nouă categorii de infracțiuni informatice, clasificate în patru titluri:

[20] A se vedea ITU, Understanding Cybercrime: A guide for developing countries, 2011.

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

[22] A se vedea http://www.impact-alliance.org/home/index.html

1. Infracțiuni împotriva confidențialității, integrității şi disponibilității datelor şi sistemelor informatice:
   - accesarea ilegală;
   - interceptarea ilegală;
   - afectarea integrității datelor;
   - afectarea integrității sistemului;
   - abuzurile asupra dispozitivelor.
2. Infracțiuni informatice:
   - falsificarea informatică;
   - frauda informatică.
3. Infracțiuni referitoare la conținut:
   - pornografia infantilă
4. Infracțiuni referitoare la atingerile aduse proprietății intelectuale şi drepturilor conexe:
   - infracțiuni referitoare la atingerile aduse proprietății intelectuale şi drepturilor conexe

Convenția Europeană în domeniul criminalității informatice din anul 2001 este considerată un moment istoric de referință, piatra de temelie a cadrului global în domeniu, multe din prevederile acesteia fiind preluate şi în Tratatului global.

Convenția Europeană este singurul cadru legislativ deschis tuturor statelor lumii, unele dintre acestea preferând să utilizeze Convenția ca pe un ghid de elaborare a propriei legislații sau ca o referință în dezvoltarea acesteia, prin implementarea principiilor şi normelor pe care aceasta le conține, în concordanță cu propriul cadru legislativ şi jurisprudența caracteristică. Cu toate acestea, Convenția Consiliului Europei privind criminalitatea informatică nu pare să mai aibă forța necesară pentru a ține pasul cu provocările ridicate de un domeniu cu o dinamică de dezvoltare accentuată.

În prezent, Convenția este criticată pentru că are în vedere manifestări criminale în mediul informatic de la sfârşitul anilor 1990, în timp ce infractorii folosesc metode din ce în ce mai sofisticate, iar infrastructura, aflată într-o dezvoltare continuă, le oferă numeroase ținte de atac. Totodată, terminologia utilizată în cadrul Convenției nu mai este considerată capabilă să exprime cu acuratețe realitățile din mediul informatic actual. O altă piedică în îndeplinirea obiectivelor declarate în Preambulul Convenției este aceea că aceasta nu s-a bucurat de un nivel de admitere global, deşi în articolele referitoare la aderare şi acceptare, Convenția este deschisă tuturor statelor lumii.

Concluzionând, putem afirma că în momentul actual este nevoie de un nou Tratat al Națiunilor Unite, ca rezultat al acordului global, cu acceptul tuturor părților.

Comisia, care a elaborat Convenția, a avut în vedere continua dezvoltare a mediului informatic şi necesitatea aducerii în timp de modificări sau amendamente. Astfel, în art. 44 se prevede că vor putea fi propuse amendamente de către fiecare parte, iar acestea vor fi communicate de către secretarul general al Consiliului Europei statelor membre ale Consiliului Europei, statelor member, care au participat la elaborarea Convenției, precum şi a oricărui stat, care a aderat sau care a fost invitat să adere, în conformitate cu art. 37.

O strategie pentru o societate a informației mai sigură a fost adoptată în anul 2006[23]. Elementele principale ale acestei strategii au fost cuprinse în Rezoluția Consiliului 2007/068/01, incluzând securitatea şi reziliența infrastructurilor din domeniul TIC. Această strategie întăreşte rolul la nivel tactic şi operațional al Agenției Europene pentru Securitatea Rețelelor Informatice şi a Datelor (ENISA), creată în anul 2004 pentru a contribui la asigurarea unui nivel înalt al securității informatice în Uniunea Europeană şi dezvoltarea unei culturi a securității informatice, pentru beneficiul cetățenilor, consumatorilor, organizațiilor şi administratorilor.

Un pas important în asigurarea unei platforme tehnice şi legale, COM(2009) se focalizează pe prevenția, pregătirea şi creşterea conştientizării prin elaborarea unui plan de acțiuni imediate de întărire a securității şi rezilienței infrastructurilor informatice critice. În COM(2011)[24] se subliniază că încrederea şi

[23] A se vedea Additional Protocol to the Convention of Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, 2003 (ETS No.189).

[24] A se vedea Comunicarea Comisiei către Parlamentul

securitatea sunt condiţii prealabile fundamentale pentru utilizarea la scară largă a TIC şi se consideră că o abordare doar la nivel European nu este suficientă pentru rezolvarea problemelor viitoare, ci trebuie să se înscrie într-o strategie de coordonare globală, care să includă partenerii-cheie, fie că este vorba de naţiuni sau organizaţii internaţionale[25].

Referitor la partea de reglementare, propunerea Comisiei de a reforma Cadrul de reglementare pentru comunicaţii şi servicii (Regulatory Framework for electronic communications, networks and services)[26]conţine noi prevederi în domeniul securităţii şi integrităţii, care întăresc obligaţiile operatorilor de a asigura măsuri corespunzătoare pentru a identifica riscurile, a garanta continuitatea furnizării de servicii şi notificare promptă a problemelor de securitate[27]. Aceste măsuri şi acţiuni completează prevederile existente în domeniul cooperării judiciare, care urmăresc prevenirea, combaterea şi pedepsirea infracţiunilor de terorism.

Propunerea de Directivă a Parlamentului European şi a Consiliului privind atacurile împotriva sistemelor informatice şi de abrogare a Deciziei-Cadru 2005/222/JAI a Consiliului consideră că răspunsul insuficient al mecanismelor de punere în aplicare a legii contribuie la răspândirea acestor fenomene, iar dificultăţile iau amploare, deoarece anumite forme de fapte penale transcend frontierele naţionale.

Propunerea de Directivă preia dispoziţiile Deciziei-Cadru şi include elemente noi în ceea ce priveşte dreptul penal material, incriminând producerea, vânzarea, achiziţionarea în vederea utilizării, importului, distribuirii sau punerii la dispoziţie, în alt mod, a dispozitivelor/instrumentelor utilizate pentru comiterea faptelor penale. Propunerea prevede circumstanţe agravante pentru crearea unui botnet sau a unui instrument similar şi în cazurile în care atacurile sunt comise prin disimularea identităţii reale a autorului şi provocarea de prejudicii deţinătorului de drept al identităţii; introduce „interceptarea ilegală" ca infracţiune penală; măsuri de îmbunătăţire a cooperării europene în materie de justiţie penală prin consolidarea structurii existente, care constă în puncte de contact disponibile 24 de ore din 24 şi 7 zile.

În pas cu dezvoltările tehnologice, Uniunea Europeană plănuieşte, de asemenea, introducerea unei actualizări a Directivei de Protecţie a Datelor (Binding Safe Processor Rules), care va face furnizorii de servicii de tip cloud responsabili pentru incidentele de securitate a datelor[28].

În anul 2011 Senatul SUA a elaborat proiectul legislativ intitulat PIPA (Senate Bill S. 968 – Protect IP Act), iar Camera Reprezentanţilor a SUA a întocmit proiectul legislativ SOPA (House Bill HR. 3261-Stop Online Piracy Act), ambele combătând pirateria şi focalizându-se pe măsurile împotriva site-urilor ce nu respectă legislaţia SUA din domeniu infracţionalităţii informatice.

PIPA şi SOPA sunt proiecte de legi pentru oprirea pirateriei pe Internet, ce vizează în principal următoarele aspecte:

- impun providerilor de Internet să modifice configurarea serverelor DNS astfel încât să nu permită propagarea domeniilor de internet din ţările străine, care găzduiesc copii ilegale ale fişierelor multimedia;
- motoarele de căutare vor fi obligate să modifice rezultatele căutării pentru a exclude site-urile străine care găzduiesc fişiere piratate;
- operatorii de plăţi online vor fi obligaţi să închidă conturile site-urilor străine care găzduiesc materiale copiate ilegal;
- serverele de publicitate online vor fi obligate să refuze orice reclamă, către

European, Consiliu, Comitetul Economic şi Social European şi Comitetul Regiunilor privind protecţia infrastructurilor informatice critice, din 2009, p. 149 şi urm şi din 2011 p. 163 şi urm.

[25] A se vedea Council of the European Union, Council conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime, Luxembourg, 26 April 2010.

[26] A se vedea COM(2007) p. 697 şi urm.

[27] A se vedea art. 13, Framework Directive.

[28] A se vedea SANS, NewsBites, Vol. XIII, Iss. 78, 2011.

site-urile care piratează materiale şi nu se vor mai face plăţi pentru publicitatea postată pe aceste site-uri.

Contoversele în jurul celor două proiecte legislative, mai ales cele de ordin tehnologic, induc temeri cu privire la faptul că acestea vor duce la inhibarea inovaţiei, vor determina înflorirea cenzurii şi vor afecta afacerile din Internet.

Tot în 2012 a fost promovat Acordul Comercial Anti-Contrafacere (ACTA – Anti-Counterfeiting Trade Agreement), care, potrivit Parlamentului European, are ca scop consolidarea respectării drepturilor de proprietate intelectuală, inclusiv online, şi de a combate contrafacerea şi pirateria. ACTA nu se referă exclusiv la protejarea proprietăţii intelectuale pe Internet, ci şi la protejarea acesteia în cadrul contrafacerilor fizice de bunuri de consum şi la reglementări în privinţa medicamentelor generice. Acestea din urmă sunt medicamente care copiază întocmai reţeta unui medicament de pe piaţă, dar sunt vândute sub un alt nume.

În urma dezbaterilor asupra ACTA, mai mulţi experţi au atras atenţia că, prin prevederile sale, acesta duce la îngrădirea libertăţii de exprimare pe Internet, arătând că proprietatea intelectuală poate fi protejată şi prin măsuri mai blânde, fără a se recurge la abuzuri. Controversele în jurul Acordului Comercial Anti-Contrafacere pot fi grupate astfel:

- felul în care s-a realizat negocierea Acordului îl privează de credibilitate democratică şi de claritate juridică. Daca va fi ratificat, ACTA va avea implicaţii majore pentru libertatea de exprimare, accesul la cultură şi viaţă privată, va afecta comerţul internaţional şi va reprezenta un obstacol în calea inovării;

- acordul a fost negociat în spatele uşilor închise, excluzând majoritatea ţărilor în curs de dezvoltare şi fără transparenţă democratică la nivelul ONU, UE sau la nivel naţional;

- acordul îşi propune să creeze o nouă instituţie, „Comisia ACTA", fără să definească însa obligaţiile sau garanţiile necesare pentru ca acest organism să funcţioneze într-o manieră deschisă, transparentă şi inclusivă, care să permită exercitarea unui control public asupra acţiunilor sale;

- privilegiile deţinătorilor de drepturi de proprietate intelectuală sunt puse mai presus de libertatea de exprimare, viaţă privată şi alte drepturi fundamentale;

- acordul va lăsa reglementarea libertăţii de exprimare în mâinile companiilor private, întrucât impune obligaţii referitoare la monitorizarea conţinutului online de către terţe părţi, cum ar fi intermediarii Internet, care nu sunt însă în măsură să reglementeze formele de exprimare în mediul online.

- acordul poate împiedica utilizarea patrimoniului cultural al societăţii, întrucât sporeşte sancţiunile şi riscurile de natură penală pentru utilizarea operelor ai căror proprietari sau deţinători de drepturi de autor sunt dificil sau imposibil de identificat sau localizat;

- precizările din versiunea finală a acordului, al căror înţeles nu va fi clarificat înainte de ratificarea ACTA, sunt vagi şi riscă să fie interpretate în moduri care ar putea permite incriminarea unui număr mare de cetăţeni, pentru delicte trivial;

- extinderea răspunderii intermediarilor îi va determina pe furnizorii de Internet să desfăşoare activităţi de supraveghere la nivelul reţelelor proprii şi să implementeze mecanisme intruzive de identificare a presupuşilor infractori, cum ar fi monitorizarea la scară largă a comunicaţiilor prin utilizarea procedurii de „deep packet inspection", permiţând astfel încălcarea gravă a vieţii private a utilizatorilor.

Putem concluziona că cyberspaţiul are nevoie de o reglementare globală, pertinentă, care să reflecte atât ineficienţele tehnologice în materie de securitate, cât şi cele de natură juridică datorate dinamicii dezvoltărilor din domeniul TIC, întrucât în cadrul societăţii, în cea mai mare parte a lor, acţiunile nu se produc ca o desfăşurare haotică de fapte, ci, dimpotrivă, ele se derulează într-un mod organizat, după reguli sociale precise, având un caracter normat.