Crime and Cyberspace

[Criminalitatea și cyberspațiul]

Diana GRUMEZA¹

¹ Ph.D. in Law, State University
of Republic of Moldova, Law
Faculty.

Abstract: The evolution of the Internet led to the birth of cyberspace. The analyze of cyberspace means an interdisciplinary approach: normative, cultural, sociological and psychological. The Internet is now a part of our lifestyle. The evolution of the legal system should follow the world technological development. But, the cyberspace is insufficiently regulated. In this article, we analyze the international, regional regulation, but also the law in Romania and the Republic of Moldova; the link between crime, digital crime and cyberspace; the killer and the victim from crime in cyberspace.

Keywords: cyberspace, law, digital crime, victim.

How to cite: Grumeza, D. (2017). Crime and Cyberspace. *Anuarul Universitatii “Petre Andrei” din Iasi, Fascicula: Drept, Stiinte Economice, Stiinte Politice*, 20, 5-20. <https://doi.org/10.18662/upalaw/01>

Introducere

Evoluția Internetului, a tehnologiei a condus la apariția cyberspațiului; acesta reclamă o analiză interdisciplinară: normativă, culturală, sociologică și psihologică.

Este important ca statele naționale să conștientizeze pericolul amenințărilor cyberspațiului și să înțeleagă importanța unor instrumente legale (convenții, tratate etc.) atât la nivel național, cât și regional, dar și pe plan internațional.

Aceasta deoarece Internetul și dezvoltarea tehnologică pe care o implică interconectivitatea au depășit stadiul evoluției *per se*, fiind astăzi un mod de viață. Sistemele computerizate nu există doar la nivelul unui desktop, a unui laptop, a unui telefon, dar stilul de viață *smart* a pătruns în construcția mașinilor, a clădirilor, în serviciile administrației locale/centrale/regionale/internaționale, logistică, utilități etc.

Ar fi ideal ca dezvoltarea legislației să urmeze îndeaproape evoluția tehnologică. În realitate însă, cadrul normativ privind infracționalitatea prin intermediul internetului este mult în urma dezvoltării tehnologice. În condițiile actuale ale promovării constante a societății cunoașterii, **avem un cyberspațiu insuficient reglementat**. Or, este imperativă luarea în considerare a construcției unui „model normativ care să guverneze spațiul cibernetic și care să fie suficient de suplu pentru a satisface ipotezele de lucru ale rețelelor web” (<https://ssrn.com/abstract=2242050>).

1. Reglementarea internațională și regională a cyberspațiului

Termenul „cyberspațiu” a apărut, pentru prima oară, într-o povestire de tip science-fiction - intitulată „Burning Chrome”, din anul 1982, aparținând autorului american William Gibson. Internetul și nanotehnologiile au creat cyberspațiul și împing societatea de astăzi într-o eră nouă. Din punct de vedere al dezvoltării tehnologice, este predictibil că acest secol va însemna pentru cyberspațiu mai mult decât o dezvoltare de o sută de ani.

Cyberspațiul a ajuns însă obiect al reglementărilor, acoperind domenii diverse: Internetul, cyber-crimele, protecția datelor personale, comerțul electronic.

Deși nu există o definiție unanim acceptată a cyberspațiului, acesta este ușor identificabil prin celebrul de acum „www” (World Wide Web). Cyberspațiul este un mod de viață, un obiect de reglementare, un mijloc de socializare, o modalitate de învățare, o formă de petrecere a timpului liber, o altă realitate - paralelă.

Reglementările privind cyberspațiul, respectiv criminalitatea informatică, sunt recente, având în vedere că apariția computerelor datează cu numai aproximativ 60 de ani în urmă. Este un domeniu de drept foarte nou, care necesită eforturi sporite pentru dezvoltarea sa. Dacă infracțiunile clasice (furt, omor etc.) le regăsim condamnate și în Biblie, nu același lucru putem spune despre domeniul nou al criminalității informatice.

Legislația privind cyberspațiul îmbină elemente de drept intern cu elemente de drept internațional.

Organizațiile internaționale au un rol important în dezvoltarea legislației în domeniul infracțiunilor informatice:

Grupul G8 a constituit o **Subcomisie privind criminalitatea high-tech**, al cărei prim rol - după cum rezultă și din titulatura sa - constă în lupta împotriva criminalității informatice. Principiile directoare vizează: investigarea infracționalității informatice internaționale trebuie realizată în mod coordonat, de toate statele implicate, nu doar de acel stat unde s-a produs prejudiciul; trebuie să existe investigatori, procurori și judecători specializați în criminalitate informatică, de aceea se impune alocarea de fonduri în acest sens.

Națiunile Unite și-au asumat în mod serios rolul luptei împotriva criminalității informatice. Astfel, **Convenția privind drepturile copilului**, adoptată în anul 1989, deși nu definește pornografia infantilă, conține în **art. 34** baza necesară prevenției exploatarei copilului prin orice mijloace: Statele părți se angajează să protejeze copilul contra oricărei forme de exploatare sexuală și de violență sexuală. În acest scop statele vor lua, în special, toate măsurile corespunzătoare pe plan național, bilateral și multilateral, pentru a împiedica: a) incitarea sau constrângerea copiilor să recurgă la activități sexuale ilegale; b) exploatarea copiilor în scopul prostituției sau al altor practici sexuale ilegale; c) exploatarea copiilor în scopul producției de spectacole sau de materiale cu caracter pornografic.

Pornografia infantilă este definită însă în **Protocolul facultativ la Convenția cu privire la drepturile copilului, referitor la vânzarea de copii, prostituția copiilor și pornografia infantilă**. Astfel, **art. 2 lit. c** definește pornografia infantilă ca „orice reprezentare, prin orice mijloace, a copiilor angajați într-o activitate sexuală explicită, reală ori simulată, sau orice altă expunere a organelor sexuale ale copiilor, în principal în scopuri sexuale” (<http://www.hotararicedo.ro/files/files/CONVENTIA%20CU%20PRIVIRE%20LA%20DREPTURILE%20COPILULUI%20-%20PROTOCOL%20FACULTATIV.pdf>).

De asemenea, Adunarea Generală a Națiunilor Unite a adoptat în anul 1990 **Rezoluția 45/121 privind legislația referitoare la criminalitatea informatică**; pe baza acesteia, în anul 1994, Națiunile Unite au elaborat un manual privind prevenirea și controlul criminalității informatice.

În cadrul Națiunilor Unite a fost constituită o Agenție specializată - **Uniunea Internațională a Telecomunicațiilor**, cu rol important în reglementarea securității informatice.

La nivel regional, un rol important revine Consiliului Europei. Încă din anul 1976 Consiliul Europei anunța pericolul internațional al criminalității informatice, iar nouă ani mai târziu se întrunea un comitet de experți pentru a dezbate problematica legală a criminalității informatice.

Importanța Consiliului Europei în acest domeniu rezidă în **Convenția privind criminalitatea informatică**, reprezentând primul tratat internațional conținând reglementări privind crime săvârșite prin intermediul Internetului, vizând cu predilecție încălcări ale drepturilor de autor, fraude, pornografie infantilă etc.

Semnata la **Budapesta la data de 23 noiembrie 2001**, Convenția privind criminalitatea informatică a fost semnată de state precum: Albania, Armenia, Austria, Belgia, Bosnia și Herțegovina, Canada, Croația, Cipru, Danemarca, Estonia, Finlanda, Franța, Germania, Grecia, Islanda, Italia, Letonia, Lichtenstein, Lituania, Luxemburg, Malta, Republica Moldova, Muntenegru, Olanda, Norvegia, Polonia, Portugalia, România, Serbia, Slovenia, Suedia, Elveția, Africa de Sud, Macedonia, Turcia, Ucraina. Procesul de ratificare a fost însă unul și mai greu. Semnatarele Convenției au avut nevoie de unu până la zece ani pentru ratificare. Astfel, dacă Albania a ratificat Convenția în jumătate de an de la semnare, Germania a avut nevoie de zece ani pentru a o ratifica. Și chiar odată ratificată, statele întâmpină greutăți în implementarea acesteia. Nici chiar marile state - S.U.A. sau Germania - nu aplică integral prevederile Convenției. Cu titlu de exemplu, Germania nu incriminează accesul fără drept la un computer, ci doar accesarea fără drept a datelor stocate într-un computer.

Dificultăți în implementarea Convenției apar din perspectiva implementării Titlului 3 al reglementării, respectiv „Rețeaua 24/7”; conform **art. 35** din Convenție, fiecare stat semnatar „va desemna un punct de contact disponibil 24 de ore din 24, 7 zile din 7, în scopul asigurării unei asistențe imediate pentru investigațiile referitoare la infracțiunile privind sisteme sau date informatice, sau pentru a strânge dovezile unei infracțiuni în format electronic”. Asistența imediată se referă

la: asistența tehnică, conservarea datelor și strângerea dovezilor, furnizarea datelor cu caracter juridic și localizarea suspecților.

Considerăm totuși că prin semnarea Convenției, statele semnatare au reușit crearea unui instrument real de interpretare unitară la nivel internațional a unor noțiuni de criminalitate informatică, oferind definiții larg acceptate ale criminalității informatice.

Tot în Consiliul Europei a fost adoptată **Convenția privind protecția copiilor împotriva abuzurilor și exploatării sexuale**, din anul 2007, semnată din chiar prima zi de 23 de state, iar până în anul 2012 de 42 de state, din care 18 au ratificat-o.

Scopul Convenției l-a reprezentat armonizarea prevederilor legale din domeniul penal pentru protecția copiilor împotriva abuzurilor și exploatării sexuale, definind abuzurile sexuale (art. 18), reglementând o serie de infracțiuni - referitoare la prostituția infantilă (art. 19), la pornografia infantilă (art. 20), privind participarea unui copil la spectacole pornografice (art. 21), coruperea copiilor (art. 22) și acostarea lor în scopuri sexuale (art. 23).

O.N.U. dezvoltă preocupări similare, prin adoptarea de către Adunarea Generală a **Rezoluției privind crearea unei culturi globale privind cybersecuritatea** la 21 decembrie 2009. Rezoluția vizează importanța cybersecurității, a dezvoltării de strategii integrate pentru a lupta eficient împotriva criminalității informatice.

La nivelul O.N.U. a fost creată **Agenția Uniunea Internațională a Telecomunicațiilor (I.T.U.)** care a stabilit în anul 2007 „Agenda Globală a Cybersecurității” (<http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>). Cei cinci piloni ai cybersecurității identificați de Națiunile Unite sunt:

- îmbunătățirea legislației;
- măsuri tehnice și procedurale;
- structuri organizaționale;
- capacitatea instituțională;
- cooperarea internațională.

Uniunea Europeană în anul 2000 a adoptat o Decizie privind pornografia infantilă prin intermediul Internetului, dar, din păcate, aceasta nu conține obligații specifice pentru statele membre U.E. Ulterior, Consiliul U.E. a adoptat o serie de decizii-cadru privind fraudă prin intermediul mediului on-line (2001), atacurile împotriva sistemelor de informații (2005), stocarea informațiilor, combaterea terorismului (2007), pornografia infantilă (2011).

Aceasta din urmă, **Directiva privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile**, grupează cele douăzeci infracțiuni la care face referire în patru categorii (<http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=LEGISSUM:jl0064&from=RO>):

- abuzul sexual: practicarea unor activități sexuale cu un copil care nu a împlinit vârsta consimțământului sexual sau forțarea unui copil pentru a se supune unor astfel de activități cu o altă persoană;
- exploatarea sexuală: constrângerea unui copil să practice prostituția sau să participe la spectacole pornografice;
- pornografia infantilă: deținerea, accesarea, distribuirea, furnizarea sau producerea de pornografie infantilă;
- ademenirea copiilor online în scopuri sexuale: propunerea pe internet a unei întâlniri cu un copil cu scopul săvârșirii unor abuzuri sexuale sau incitarea unui copil, tot online, să furnizeze materiale pornografice în care acesta este reprezentat.

Nici **O.C.D.E. (Organizația pentru Cooperare și Dezvoltare Economică)** nu este străină de acest domeniu. Aceasta a inițiat un studiu privind posibilitatea armonizării legislației penale la nivel internațional în vederea diminuării criminalității informatice. În acest sens, se recomandă întocmirea unei liste conținând infracțiuni informatice care să fie sancționate la nivel mondial, cum ar fi alterarea datelor și programelor computerelor, interceptarea fără drept a comunicațiilor, fraudele prin intermediul computerelor.

Cooperarea Economică Asia-Pacific (A.P.E.C.) a identificat criminalitatea informatică ca pe un domeniu extrem de important, liderii organizației fiind chemați să ia măsuri pentru combaterea acestei forme de criminalitate. În acest sens, în anul 2002 a fost semnată declarația privind lupta împotriva terorismului și promovarea creșterii, cu scopul de a dezvolta aptitudinile necesare investigării crimelor din domeniul informaticii. De asemenea, organizația a promovat organizarea a numeroase conferințe în domeniul criminalității informatice, a organizat grupuri de lucru (privind informația și telecomunicațiile, strategia securității informatice).

Uniunea Africană care în anul 2009, la reuniunea miniștrilor responsabili cu tehnologiile, informațiile și comunicarea, a atins subiecte importante legate de creșterea gradului de folosire a internetului și a computerelor la nivelul continentului african. S-a hotărât cu acest prilej adoptarea unui cadru legislativ unitar privind tranzacțiile electronice, securitatea informatică și protecția datelor. În anul 2011 se ajunsese deja la

o formă a Convenției privind stabilirea unui cadru legal credibil pentru securitatea informatică în Africa.

De asemenea, **Liga Arabă și Consiliul de Cooperare al Golfului** s-au arătat interesate de dezvoltarea legală a acestui domeniu, de noile tendințe la nivel internațional.

Organizația Statelor Americane abordează problematica criminalității informatice la nivelul statelor membre. Alte preocupări în același domeniu întâlnim în Insulele Caraibe și Pacific.

Așadar, constatăm că la nivel internațional există o preocupare majoră pentru acest domeniu, pentru definirea criminalității informatice și în vederea luării de măsuri pentru prevenirea și sancționarea comportamentelor antisociale în domeniu.

2. Criminalitatea și cyberspațiul

Anterior analizei tandemului criminalitate - cyberspațiu, considerăm necesară prezentarea definiției „criminalității”. Conform *Dicționarului explicativ al limbii române* criminalitatea reprezintă *totalitatea infracțiunilor săvârșite pe un anumit teritoriu într-o anumită perioadă* (***, 1975).

Legătura dintre crimă - crima digitală - crima din cyberspațiu este ca de la întreg la parte. Astfel, explicăm această afirmație folosindu-ne de un exemplu: dacă o persoană păstrează o colecție de fotografii conținând pornografie infantilă pe un computer, atunci aceasta este atât o crimă, cât și o crimă digitală. Dacă însă computerul este conectat la alte computere, acestea toate fiind interconectate, toți având acces la fotografiile sau materialele în cauză, atunci vorbim despre o crimă în cyberspațiu (Earl, 2010).

La nivel național, regional și internațional sunt utilizați termeni/sintagme diferite pentru a defini același fenomen: criminalitatea electronică, criminalitatea informatică (*computer crime*), criminalitatea de

întălnă tehnologie (*high-tech crime*), criminalitatea în legătură cu utilizarea calculatorului (*computer-related crime*), cyber-criminalitatea (*cyber-crime*). Folosirea noțiunilor anterior menționate, ca noțiuni sinonime, nu face decât să îngreuneze însăși definirea acestui tip de criminalitate.

Astfel, criminalitatea informatică este definită ca:

- Activitatea care implică folosirea computerelor sau a rețelelor de comunicații ca fiind instrumentul, ținta sau locul unde are loc activitatea infracțională (Gercke);

- Actul criminal este îndreptat către un computer sau către o rețea de computere ori sisteme cu caracter informatic și/sau orice crimă care este facilitată sau comisă prin utilizarea unui computer, rețele sau dispozitiv informatic (Ruiu, 2014).

Criminalitatea informatică poate fi definită atât în sens restrâns, cât și în sens larg (<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>):

- În **sens restrâns**, criminalitatea informatică înseamnă orice comportament ilegal săvârșit prin mijlocirea echipamentelor electronice îndreptat împotriva securității sistemelor informatice, respectiv a datelor prelucrate de acestea;

- În **sens larg**, criminalitatea informatică înseamnă orice comportament ilegal săvârșit prin intermediul unui sistem informatic sau în legătură cu acesta, inclusiv infracțiuni ca posesia ilegală și oferirea și/sau distribuirea de informații prin intermediul unui sistem informatic sau a unei rețele informatice.

Criminalitatea prin intermediul cyberspațiului sau criminalitatea informatică reprezintă „totalitatea faptelor comise în zona tehnologiilor informaționale, într-o anumită perioadă de timp bine-determinată și pe un anumit teritoriu” (<http://drept-md.com/wp-content/uploads/2014/02/Raport-Criminalitatea-informatica.pdf>).

În Republica Moldova, legiuitorul nu reglementează o definiție a sistemului informatic, deși Codul penal al Republicii Moldova incriminează o serie largă de fapte antisociale săvârșite prin intermediul sistemelor informatice. Titlul IX din Codul penal reglementează „Infracțiunile informatice și infracțiuni în sistemul telecomunicațiilor”.

Noul Cod Penal al României definește „sistemul informatic”, respectiv „datele informatice” în capitolul dedicat explicitării unor noțiuni de drept penal. Astfel, **art. 181 alin. 1** din Codul penal al României prevede că *prin sistem informatic se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic, iar*

art. 181 alin. 2 definește datele informatice prin care *se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic.*

Modalitatea în care legiuitorul român a ales să reglementeze cyber-criminalitatea este diferită decât în cazul celorlate fapte antisociale și remarcăm diferența și raportat la modalitatea în care legiuitorul din Republica Moldova reglementează aceleași infracțiuni. Ca atare, criminalitatea în cyberspațiu nu ocupă doar un singur titlu/capitol din Codul penal (astfel cum este regula și astfel cum este reglementarea și în Republica Moldova), ci infracțiunile săvârșite prin utilizarea calculatorului se regăsesc în titluri diferite ale legii organice penale românești, respectiv în categoria infracțiunilor contra patrimoniului, a infracțiunilor contra siguranței publice, a infracțiunilor de fals.

2.1. Criminalul din cyberspațiu

În principiu, criminalul din lumea obișnuită și cel din spatele calculatorului sunt similari, au o psihologie apropiată unul de altul. Dar, spre deosebire de criminalul din lumea reală, cel din cyberspațiu este chiar mai periculos, deoarece comportamentul său infracțional este premeditat, plănuit intenționat anterior, nefiind un act impulsiv, astfel cum se întâmplă de multe ori în faptele criminale din lumea offline.

Criminalul digital folosește computerul și Internetul ori ca mijloc de săvârșire a faptelor penale, ori în legătură cu acestea.

Astfel, unii cyber-criminali folosesc Internetul pentru a-și selecta și cunoaște victimele; alții pentru a-și ține evidențele faptelor penale; alții pentru a ține legătura cu alți eventuali participanți la săvârșirea infracțiunilor.

Criminalul digital se caracterizează prin specializarea în tehnologia calculatoarelor. Din punct de vedere al vârstei sau al categoriei sociale, al ocupației sunt similari cu infractorii obișnuiți.

Dat fiind faptul că grupa de vârstă care utilizează cel mai des internetul în România, dar și în Republica Moldova, este cuprinsă între 16-34 ani, (<http://www.insse.ro/cms/sites/default/files/compresa/compdf/ticr2016.pdf>), rezultă că vorbim despre un segment demografic care, teoretic și practic, prezintă un potențial criminogen ridicat.

Optimismul criminalului din mediul on-line este alimentat de faptul că este mult mai probabil să nu fie prins, spre deosebire de infractorul clasic.

Internetul este un mediu unde competiția este în permanență actuală, iar lucrurile evoluează foarte rapid. Pe cale de consecință, și infractorul din mediul virtual evoluează cu fiecare click. Gradul de anonimat pe care îl furnizează spațiul on-line sporește numărul potențialilor infractori. Psihologic vorbind, simpla impresie că ești privit te poate face să te comporți în concordanță cu normele morale și sociale.

Digitizarea criminalității presupune o transformare a avantajelor mijloacelor electronice într-o veritabilă sursă a răului. Securitatea și încrederea pe care ar trebui să o inspire mijloacele electronice, care derivă din atribuirea unei identități electronice, folosirea semnăturii digitale, securizarea informațiilor prin criptare, asigurarea confidențialității sunt speculate de criminalul informatic și transformate din mijloace destinate să deservească un interes public în mijloace de acoperire a criminalului digital.

Criminalii digitali sunt împărțiți în următoarele categorii:

1. Hacker-ul este un explorator al profunzimii lumii digitale, programator, care se specializează în spargerea sistemelor informatice, profitând de slăbiciunile sistemului și, de multe ori, revoluționându-l și făcându-l să evolueze, săvârșind uneori acte de spionaj corporatist ori guvernamental.

De multe ori, hackerii vizează „spargerea” parolilor, a site-urilor protejate de parole. Atacurile hackerilor au, de cele mai multe ori, ținte importante: Pentagonul, Forțele Aeriene Americane, site-uri arhicunoscute (Google, Yahoo etc.).

2. Phreaker-ul (etimologic vorbind, provine din combinația termenilor *phone* și *breaker*) este hackerul sistemelor de telefonie, intrând în mod neautorizat în convorbirile interne ale unei companii.

3. Cracker-ul este infractorul care pătrunde în sistemul informatic al unei organizații, instituții sau companii prin violarea sistemelor de securitate (<http://e-crime.ro/ecrime/site/files/93361241097364> [Infractiuniindomeniulinformatic.pdf](#)).

3. Traficanții de informații și mercenarii sunt acei infractori care realizează profituri materiale însemnate din infracțiuni de spionaj economic, prin prejudicierea persoanelor fizice și/sau juridice. Prezența unor secrete comerciale în computerele firmelor sau a unor informații privind conturile bancare ale persoanelor fizice sunt scopuri în sine pentru criminalii informatici.

4. Teroriștii și devianții folosesc sistemele de comunicare în scopuri politice, pentru a propaga idei, a instiga la un comportament antisocial, săvârșind infracțiuni pentru presupusa atingere a scopului urmărit.

În literatura de specialitate (http://www.mpublic.ro/sites/default/files/PDF/PUBLICATII/rccp_4_2015.pdf), găsim și alte clasificări, chiar mai generale, ale infractorilor din cyberspațiu:

- 1. Utilizatorii neglijenți** - care se fac vinovați de nerespectarea politicilor de securitate;
- 2. Infractorii tradiționali** - care săvârșesc infracțiuni comune, folosindu-se de noile tehnologii;
- 3. Șarlatanii și hoții** - care transmit mesaje comerciale nesolicitate de tip „phishing”, „spoofing”, „spimming”;
- 4. Hacker-ii, computer trespassers (intrușii informatici) și password crackers (spărgătorii de parole)** - exploratorii, cei care cercetează spațiul virtual, îi caută vulnerabilitățile și îl perfecționează;
- 5. Creatorii și distribuitorii de cod cu intenții criminale (malicious code writers and distributors)** - care lansează viruși informatici;
- 6. Pirații de muzică, de filme, și de software** - vizează încălcarea drepturilor de autor, copiind, distribuind, vânzând fișiere, date etc. Dacă în trecut copierea fișierelor însemna pentru fișierul copiat o pierdere de calitate, astăzi acest dezavantaj a fost depășit;
- 7. Hărțuitorii** - care amenință folosind tehnologiile informaționale;
- 8. Hărțuitorii, pedofilii sau alți infractori cyber sex** - cei care doresc să obțină controlul ori să obțină plăceri sexuale în afara legii. Materialele cu conținut sexual au fost printre primele comercializate prin intermediul Internetului., profitându-se de avantaje ca: accesul larg, fără a suporta costuri; considerarea mediului virtual ca asigurând anonimatul. Cercetările efectuate (<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>) evidențiază că sunt disponibile nu mai puțin de 4,2 milioane website-uri pornografice.

În ceea ce privește materialele pornografice care îi au ca protagoniști pe minori, dezvoltarea lor a fost posibilă ca urmare a accesului larg la mijloace de fotografiere și filmare, lipsa intermedierei dezvoltării fotografiilor ori prelucrării filmelor de firme specializate. Riscul acestei categorii de infractori de a fi prinși a devenit foarte mic din această perspectivă; se adaugă și reducerea numărului de materiale pornografice analogice și înlocuirea acestora cu cele digitale.

Din cercetările realizate, a rezultat o statistică privind pe infractorii arestați sau aflați în stare de deținere, care folosesc internetul și care dețin și/sau distribuie materiale pornografice cu copii: 15% dintre ei dețineau mai mult de 1.000 fotografii pornografice; 80% aveau în computere materiale pornografice cu copii având vârste cuprinse între șase și doisprezece ani; 19% cu copii sub vârsta de trei ani.

<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>.

1. **Trișorii academici** - plagiază lucrări, fură examene etc.
2. **Spionii industriali, guvernamentali și independenți** - care spionează în scopuri profesionale ori personale. De multe ori, informații importante sunt stocate în computere. Conexiunea la Internet a acestora le face vulnerabile, informații deosebit de importante sau delicate ajungând la îndemâna unor persoane care le pot comercializa.
3. **Teroriștii** - promovează scopuri diverse (sociale, religioase, politice) prin inducerea fricii.

Portretul criminalului din cyberspațiu:

1. Fuga de responsabilitate personală, fiind adeptul crezului: „Nu e treaba mea, dacă pot să iau, iau”;
2. Refuzul de a accepta că face rău unei alte persoane;
3. Condamnarea celor care sunt împotriva practicilor sale, pornind de la următoarea idee: „Ce au cu mine, eu nu fac niciun rău”;
4. Posibilitatea alegerii locului unde se va afla la momentul săvârșirii infracțiunii, având astfel senzația securității sale;
5. Săvârșirea infracțiunii într-un timp mult mai scurt decât în cazul săvârșirii infracțiunilor off-line;
6. Orientarea către culegerea de informații amănunțite despre viața victimei;
7. Petrece timp îndelungat pentru a cunoaște victima;
8. În ceea ce privește respectul de sine, acesta este diferențiat, în funcție de nivelul de calificare;
9. Manifestă apetență pentru singurătate;
10. La rândul său este posibilă victimă a abuzurilor fizice ori psihice;
11. Își creează o dublă personalitate, una pentru lumea reală și alta, dorită, în lumea virtuală.

Cauzele determinante pentru comportamentul infracțional în cyberspațiu sunt dintre cele mai diverse. Astfel, infractorul din cyberspațiu poate doar să se amuze prin săvârșirea infracțiunilor on-line, sau ar putea avea motive religioase, sociale ori politice, afecțiuni psihice, profituri material ori este posibil să urmărească satisfacerea unor impulsuri sexuale sau motive de ordin emoțional ori numai să își dovedească abilitățile deosebite în domeniul informatic.

Criminalii informatici săvârșesc infracțiunile informatice profitând de insuficienta protecție a computerelor.

2.2. Victima din cyberspațiu

Statisticile arată că este mult mai posibil ca o persoană să devină victima unei infracțiuni informatice decât a unei infracțiuni clasice îndreptate împotriva patrimoniului unei persoane (furt, tâlhărie etc.).

Creșterea criminalității prin utilizarea cyberspațiului se datorează și comportamentului victimei, care manifestă reținere în a raporta organelor de cercetare penală săvârșirea unei astfel de infracțiuni. Motivația unui astfel de comportament, descrisă în literatura de specialitate (Olteanu G., Iacob A., Gorunescu N., & Voicu A. 2008), se poate datora:

1. Dorinței victimei de a-și proteja imaginea în societate, fiind posibilă prejudicierea dreptului său la imagine, ca urmare a publicității realizată prin mediatizarea infracțiunii;
2. Recuperarea minoră a prejudiciului cauzat prin săvârșirea infracțiunii, chiar în situația identificării infractorului și a tragerii acestuia la răspundere penală.

De aceea, cooperarea victimei este un element important în combaterea criminalității informatice, pentru că de cele mai multe ori numai informațiile pe care le poate furniza victima vor permite cercetarea și tragerea la răspundere penală a infractorului informatic.

De cealaltă parte a infracțiunilor săvârșite în cyberspațiu sunt victimele din mediul on-line. Literatura de specialitate (Olteanu G., Iacob A., Gorunescu N., & Voicu A. 2008) le clasifica astfel:

1. Persoane care utilizează de scurt timp Internetul, care nu sunt familiarizate cu pericolele potențiale (virusi etc.)
2. Persoane naive care utilizează Internetul, care prin credulitatea lor sunt ținte ușoare. Se încadrează în această categorie ori persoanele foarte tinere, ori persoanele vârstnice. Tot aici avem în vedere și minorul/copilul, definit în Convenția privind criminalitatea informatică drept persoana care nu a împlinit vârsta de 18 ani, cu excepția situațiilor în care legislația statului în cauză stabilește că vârsta majoratului este atinsă mai devreme de 18 ani.
3. Persoanele cu nevoi speciale, care găsesc în Internet o modalitate facilă de socializare.
4. Persoanele singure, depresive, care caută întemeierea unei familii prin intermediul site-urilor matrimoniale sau care au alte nevoi emoționale ori fizice.
5. Pseudo-victimele - pericolul pseudo-victimizării în cyberspațiu este mai mare decât în mediul off-line. Există persoane care, din diverse motive

(pecuniare, emoționale etc), se consideră victime ale infracțiunii și sesizează organele de cercetare penală.

Crimele convenționale îndreptate împotriva persoanei sunt cele care implică, în mod tradițional, folosirea violenței, a coerciției, de către criminal împotriva victimei sale și un contact direct între agresor și victimă (infracțiuni de răpire, viol, omor etc). În ceea ce privește crimele din cyberspațiu, acestea se caracterizează prin excelență prin absența contactului direct dintre victimă și agresor, dată fiind mijlocirea calculatorului. În acest context, a vorbi despre crime îndreptate împotriva persoanei în cyberspațiu este oarecum impropriu (Jeri, Jaeckle, Thomas, & Jarvis, 2010).

Numărul infracțiunilor îndreptate împotriva persoanei în cyberspațiu este însă în creștere și se așteaptă o mărire a acestui număr, pe măsură ce tot mai multe persoane vor avea acces la computer.

Concluzii

Sistemele informatice fac parte integrantă din viața cotidiană: totul în jurul nostru se bazează pe computere - servicii aeriene, rutiere, domeniul construcțiilor, furnizarea de energie electrică, gaz, apă. Dependența de sistemul informatic ne face însă extrem de vulnerabili, căderea sistemului putând conduce la pierderi financiare uriașe și chiar la pierderi de vieți omenești (cum este în cazul sistemului de sănătate).

Creșterea popularității sistemelor informatice, pe de o parte, și a Internetului, pe de altă parte, au ca efect creșterea exponențială a criminalității informatice, prin sporirea numărului de agresori și, implicit, de victime.

Conceptele cu care operează cyber-criminalitatea nu sunt suficient de clare, nici chiar conceptul central de *cyber-criminalitate* nu este stabil.

Criminalitatea informatică este mobilă, se adaptează noilor tehnologii; legislația privind criminalitatea informatică trebuie văzută ca parte integrantă a unui întreg - strategia securității cyberspațiului, a politicii guvernamentale a statelor, a unui cadru global pentru dialog și cooperare internațională. În acest sens, se impune armonizarea legislației statelor, cu respectarea specificităților naționale și regionale, după caz.

Tendența de armonizare legislativă este evidentă la nivel internațional și regional. Pornind din S.U.A. și ajungând până în statele africane, omenirea a înțeles importanța în creștere a cunoștințelor, a tehnologiei informatice, a avantajelor și a dezavantajelor pe care le presupun. De aceea, O.N.U., Consiliul Europei, Uniunea Europeană,

Organizația pentru Cooperare și Dezvoltare Economică (O.C.D.E.), Cooperarea Economică Asia-Pacific (A.P.E.C.), Uniunea Africană, Liga Arabă și Consiliul de Cooperare al Golfului, Organizația Statelor Americane abordează problematica criminalității informatice în mod responsabil, prin încercări de armonizare legislativă.

Interferența mediului on-line cu societatea off-line înseamnă intervenția legiuitorului în reglementarea noului domeniu pentru a garanta respectarea drepturilor inerente persoanei, cum ar fi concilierea dreptului la viață privată cu protecția datelor cu caracter personal.

Bibliografie

Tratate, cursuri, monografii

Agenda Globală a Cybersecurității, disponibilă la

<http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>.

Articole publicate în reviste de specialitate

Begu, V., „Criminalitatea informatică”, disponibil la http://drept-md.com/wp-content/uploads/2014/02/Raport_-Criminalitatea-informatica.pdf.

Borges Fortes, Vinicius, *Privacy and Personal Data Protection in Cyberspace: The Brazilian Case* (March 30, 2013). TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy. Available at SSRN: <https://ssrn.com/abstract=2242050> (accesat la 10.05.2017).

Dicționarul Explicativ al Limbii Române, Editura Academiei, București, (1975).

Directiva privind combaterea abuzului sexual asupra copiilor, a exploataării sexuale a copiilor și a pornografiai infantile, disponibilă la <http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=LEGISSUM:jl0064&from=RO>.

Dobrinioiu, M., *Infracțiuni în domeniul informatic*, București, (2006), disponibil la http://e-crime.ro/ecrime/site/files/93361241097364Infracțiuni_indomeniulinformatic.pdf.

Gercke, M. *Understanding cybercrime – A Guide For developing countries*, ITU – International Telecommunication Union (ITU), ICT Applications and Cybersecurity Division - Policies and Strategies Departament – Bureau for Telecommunications Union, Place des Nations, 1211 Geneva 20, Elveția.

- Institutul Național de Statistică, Comunicat nr. 305/2016, disponibil la http://www.insse.ro/cms/sites/default/files/com_presa/com_pdf/tic_r2016.pdf.
- Moise Cristian Adrian, „Infractorii și victimele în cyberspațiu”, în *Revista de Criminologie, Criminalistică și Penologie* nr. 4/2015, disponibilă la http://www.mpublic.ro/sites/default/files/PDF/PUBLICATII/rc_cp_4_2015.pdf.
- Moulton Earl, „The future of cybercrime”, (2010) în *Future Challenges of Cybercrime*, Volume 5 Proceedings of the Futures Working Group. Federal Bureau of Investigation: Quantico, Virginia.
- Olteanu G., Iacob A., Gorunescu N., & Voicu A. (2008). Metodologie criminalistică. Structurile infracționale și activitățile ilicite desfășurate de către acestea, Editura AIT Laboratories, București.
- Protocolul facultativ la Convenția cu privire la drepturile copilului, referitor la vânzarea de copii, prostituția copiilor și pornografia infantilă, disponibil la <http://www.hotararicedo.ro/files/files/CONVENTIA%20CU%20PRIVIRE%20LA%20DREPTURILE%20COPILULUI%20-%20PROTOCOL%20FACULTATIV.pdf>.
- Roberts, J., Jaeckle, T., Thomas, P., & Jarvis, J., „Cybervictimization” (2010) în *Future Challenges of Cybercrime*, Volume 5 Proceedings of the Futures Working Group. Federal Bureau of Investigation: Quantico, Virginia.

Documente oficiale

- Ruiu, M. (2014). *Metodologia investigării criminalistice a unor genuri de infracțiuni*, Editura Universul Juridic, București.
- Telecommunication Developing Center, Understanding cybercrime: phenomena, challenges and legal response, p. 11, disponibil la <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>