INTERNETUL UN NOU UNIVERS AL CRIMINALITĂȚII

Angelica PETROV, Facultatea de Drept

Even though cybercrime seems to be a relatively new phenomenon, it is in fact an extension of the ordinary criminal world. Therefore, this paper serves as a comprehensive study of cybercrime, aiming to highlight the particularities and the amplitude of the phenomenon through an in depth analysis of the typology of cybercrime; and the international, regional, and national legal framework as to identify the most efficient solutions for preventing and fighting cybercrime.

Existența calculatoarelor, a telefoanelor și altor dispozitive conectate la Internet au redefinit societatea în care trăim. Internetul, actual a trecut printr-un proces complex de evoluție, fiind un instrument inevitabil vieții cotidiene. Multitudinea de avantaje pe care le oferă spațiul virtual reprezintă raționamentul tendinței de digitalizare a societății, susținută pe larg de comunitatea internațională, regăsindu-se ca o prioritate strategică într-o multitudine de strategii internaționale, regionale și naționale.

În continuare, viteza accelerată de dezvoltare a tehnologiilor informaţionale, creează o adevărată provocare pentru conceptele juridice existente. Progresul tehnologiilor informaţionale a dus la „remodelarea" unor infracţiuni tradiţionale, în prezent săvârşite şi prin intermediul Internetului. Ori, apariția Internetului nu a făcut decât să faciliteze migrarea infracțiunilor tradiționale în spațiul virtual [1, p.5], acestea fiind calificate ca infracțiuni cibernetice. În contextul supra, organele de urmărire penală se confruntă cu o adevărată provocare de asigurare a unui spațiu sigur, în această eră digitală.

Internetul nu este un element static ci unul dinamic [2, p.7], acesta înglobând în sine un șir de practici sociale, forma căruia este reliefată de multitudinea de informații pe care noi, utilizatorii, le facem disponibile, existența unui cadru normativ eficient este o condiție *sine qua non* pentru asigurarea unui spațiu virtual sigur.

Toate premisele enumerate impun necesitatea stringentă de a analiza fenomenul criminalității cibernetice, în vederea identificării măsurilor de prevenire și combatere, atât de ordin legislativ, tehnic, cât și practic aplicabile la nivel național. Totodată, spre deosebire de alte categorii de infracțiuni, în cazul criminalității cibernetice, datorită caracterului transfrontalier, pe lângă reglementările naționale de o egală importanță este și cadrul legal internațional și regional. Din aceste considerente, o atenție sporită, în cadrul lucrării, este destinată aspectelor globale. Analiza aspectelor teoretico-practice ale fenomenu lui criminalității cibernetice a permis a identifica un șir de probleme.

În momentul actual, la nivel internațional, identificăm lipsa unui consens asupra definirii fenomenului criminalității cibernetice, care drept consecință generează un șir de impedimente pentru state în procesul de adoptare a legislației și incriminării acțiunilor. În accepțiunea noastră, criminali tatea cibernetică poate fi definită:

stricto sensu şi *lato sensu*. În sens îngust, prin criminalitate cibernetică se înţelege orice activitate ilegală care este săvârşită sau a cărei săvârşire este facilitată de Internet, de către o persoană ce deţine cunoştinţe speciale în domeniul ciberspaţiului. În sens larg, criminalitatea cibernetică constituie activitatea ilegală săvârşită prin intermediul computerelor, telefoanelor mobile sau altor dispozitive, indiferent dacă sunt sau nu conectate la Internet, cu scopul de a provoca prejudicii sau daune altor persoane.Un al doilea aspect ce necesită o atenţie sporită reprezintă cele şapte „blocuri" de instrumente internaţionale de combatere a criminalităţii cibernetice, instrumentele: Consiliului Europei; Uniunii Europene; Comunităţii Statelor Independente (CSI); Organizaţiei de Cooperare de la Shanghai; Uniunii Africane; statelor Arabe; şi instrumentele elaborate sub auspiciul sau de către Organizaţia Naţiunilor Unite şi Agenţiile ei [3, p.63]. În timp ce unele state au aderat la mai mult de un singur instrument, altele nu au aderat la niciunul. Mai mult, în momentul actual nu există nicio convenţie sau document unic, care să aibă atingere globală în domeniul criminalităţii cibernetice. Lipsa unui cadru de reglementare uniform la nivel internaţional duce la apariţia „paradisurilor digitale" [4, p.46], care oferă infractorilor posibilitatea de a perturba securitatea spaţiului virtual, fără a fi atraşi la răspundere penală. Deşi Convenţia de la Budapesta [5], rămâne unica cu cea mai vastă expansiune în materie, considerăm că aceasta nu corespunde actualităţii, prevederile ei fiind lacunare, dat fiind faptul că reglementările acesteia sunt bazate pe practicile infracţionale ale anilor `90. La nivel naţional, analiza fenomenului criminalităţii cibernetice a permis a formula următoarele recomandări şi propuneri *de lege ferenda:*

1. Atât în literatura de specialitate, cât şi în legislaţia internaţională, sunt utilizaţi termenii: *„computer crime"* şi „*cybercrime"*. În limba română, legiuitorul a tradus ambele sintagme *„criminalitate informatică"*, acestea fiind percepute ca sinonime, deşi conţinutul lor este distinct. Lipsa unor termeni potriviţi în legislaţia Republicii Moldova impune necesitatea revizuirii din punct de vedere terminologic a noţiunilor utilizate, în vederea evitării confuziilor. În acest sens, propunem definirea şi utilizarea termenilor după cum urmează: *‚computer crime* - criminalitate informatică şi *cybercrime* -

criminalitate cibernetică.

2. Subsecvent, din punct de vedere criminologic, conceptele existente privind criminalitatea tradiţională sunt de o valoare limitată în tentativa explicaţiei genezei criminalităţii cibernetice. Dat fiind specificul infracţiunilor săvârşite prin intermediul Internetului se constată necesitatea mai degrabă a creării unor inovaţii teoretice [6, p.90-95] decât transpunerea conceptelor criminologice deja existente privind criminalitatea tradiţională. În acest sens, propunem implicarea specialiştilor ce posedă cunoştinţe în domeniul TI în procesul de analiză a fenomenului criminalităţii cibernetice, din punct de vedere criminologic, în scopul eficientizării activităţii de identificare şi formulare a noilor concepte criminologice ce au ca scop explicarea genezei comportamentului criminal.

3. În continuare pe măsură ce tehnologiile informaţionale se dezvoltă, cercul infracţiunilor posibile de a fi săvârşite pe Internet şi prin intermediul acestora va creşte. Din practica internaţională, putem extrage un şir de infracţiuni a căror transpunere în legislaţia Republicii Moldova este oportună. În acest sens ca propunere *de lege ferenda* recomandăm suplimentarea listei existente a infracţiunilor cibernetice a Codului Penal [7], cu următoarele tipuri: spionajul informatic, pirateria informatică, defăimarea pe Internet şi hărţuirea online.

4. Într-o eră digitală, în care practic toate infracţiunile pot fi transpuse în lumea virtuală, nu există necesitatea de a dubla infracţiunile spre exemplu hărţuire sexuală vs. hărţuire online sau determinarea la sinucidere vs. determinarea la sinucidere prin Internet, or acestea reprezintă în esenţă aceleaşi infracţiuni, unica distincţie fiind modalitatea în care este săvârşită. Cu toate acestea, faptele ilicite săvârşite prin intermediul Internetului trebuie să îşi găsească reglementarea în Codul Penal. În acest context, o a doua propunere alternativă *de lege ferenda* este suplimentarea listei circumstanţelor agravante a art. 77 CP [8], după cum urmează; „săvârşirea infracţiunii pe Internet sau prin intermediul Internetului” şi adăugarea prezentei circumstanţe în componenţele infracţiunilor relevante din Codul Penal. Fenomenul criminalităţii cibernetice este unul de o amploare şi actualitate deosebită, studiul căruia poate fi cu greu redat într-un volum restrâns. Din aceste considerente, prezentul articol reprezintă o trecere în revistă a doar câteva aspecte esenţiale. În vederea cercetării

în detaliu a fenomenului criminalității din punct de vedere crimino logic propunem a se studia textul integral al tezei.

Referințe:

1. BRENNER, S. W. *Cybercrime and the Law: Challenges, Issues and Outcomes.* Lebanon, US: Northeastern, 2012. p.272.
2. YAR, M. *Cybercrime and Society.* London: SAGE Publications Ltd, 2006. p.200.
3. United Nations Office on Drugs and Crime. Comprehensive study on cybercrime. New York, 2013, p.320. https://www.unodc.org/documents /organized-crime/UNODC_CCPCJEG.4_2013/CYBERCRIME _STUDY _210213.pdf (vizitat 09.03.2017)
4. GHERNAOUTI, S. *Cyber Power: Crime, Conflict and Security in Cyberspace.* Switzerland: EPFL Press, 2013. p.220.
5. Convenția Consiliului Europei privind criminalitatea informatică https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 /signatures?p_auth=VHZ47Ovt (vizitat pe 11.04.2017)
6. HOLT, T. J., BOSSLER, A. M. *Cybercrime in progress: theory and prevention of technology-enabled offenses.* New York: Routledge, 2016. p.226.
7. Codul Penal nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 72-74.
8. Convenția Uniunii Africane privind securitatea cibernetică și protecția datelor personale semnată la Malabo, la 27 iunie 2014, este unicul instrument din lume care în cadrul art. 30 prevede agravarea infracțiunilor tradiționale a căror săvârșire a fost facilitată de Internet.