PREVENIREA ȘI COMBATEREA CRIMINALITĂȚII INFORMATICE PRIN COOPERARE LA NIVEL NAȚIONAL ȘI INTERNAȚIONAL

PREVENTING AND COMBATING CYBERCRIME THROUGH NATIONAL AND INTERNATIONAL COOPERATION

Igor SPÎNU, dr.în drept, conf.univ. USEM

ORCID 0000-0001-7512-6546

Oleg SPÎNU,doctorand

Școala Doctorală Stiințe Juridice și Relații Internaționale, USEM

ORCID 0000-0002-6824-1981

Summary

The evolution of technologies and the increase of cybercrime, requires the development of new tools in combating this criminal phenomenon, as it is necessary for responsible authorities at both national and international level to involve new tools, acquire new skills and develop effective investigative methods and techniques to combat cybercrime through international collaboration of states. It is necessary to specify that the responsible authorities must secure, identify and collaborate with other organizations and institutions at international level in order to combat and prevent cybercrime, as well as for the use of evidence obtained through collaboration, in a criminal trial by case and in the court.

The authors consider that the approach to this topic is essential from the perspective of both theorists and practitioners, given that cybercrime is increasing at the national and international level, especially lately there is a major increase in cybercrime in the Republic of Moldova. Thus, we have a particular interest in addressing this topic, analyzing aspects and strategies that could prevent cybercrime in the future, such as: combating illegal online content, protection against communications in relation to the retention or disclosure of personal data, deception and other computer crimes that seriously violate human rights and obviously lead to moral damage and material damage.

Keywords: cybercrime, fighting, crime, prevention, technologies, security.

Calculatorul și sistemele informatice actualmente au devenit indispensabile în dezvoltarea mai multor ramuri de activitatea a societății la nivel național și internațional. Impactul și dezvoltarea avansată a domeniului informatic este evidentă atât în sectorul public cât și privat, având o influență majoră asupra vieții cotidiene și avansării informaționale la nivel național.

Actualmente, tehnologiile și sistemele informatice au ajuns a fi baza oricărei activități cotidiene a fiecărui om, fiind sursa la care recurg cetățenii zi de zi, pentru satisfacerea rapidă, eficintă și simplificată a necesităților sale, precum domeniile profesionale de: agricultură, construcții, comerț, sănătate și asistență socială, industria-extractivă, invățământ, administrație publică, justiție, activități extrateritoriale, activități profesionale, științifice și tehnice etc.

În funcție de rolul său social, domeniul informatic este folosit în diverse instituții ale statului precum informatica parlamentară, jurisdicțională, administrativă, fiind un factor considerabil pentru optimizarea activității juridice moderne și activității sociale.

Evoluția progresivă in domeniul informatic determină aspecte problematice de natură social-economică, juridică și în domeniul activității criminale la nivel național și internațional.

Din perspectiva infarcționalității spațiul informațional reprezintă o formă pentru pregătirea și comiterea crimelor informatice, prin prisma cărora se produc acte de terorism cibernetic, sau alte acțiuni directe sau indirecte care prejudiciază securitatea națională. Astfel, penetrarea sistemelor informatice și comunicațiilor electronice, a bazelor de date ale autorităților în cadrul cărora se gestionează informaţie sensibilă, poate duce la compromiterea confidenţialităţii, integrităţii sau disponibilităţii acestei informaţii, şi, prin urmare, la cauzarea prejudiciilor financiare sau de altă natură, inclusiv la afectarea securităţii statului.

La nivel național, penetrarea sistemelor informatice poate duce la obținerea controlului neautorizat asupra acestor sisteme și prejudicia procesele sociale, econimice, politice, juridice, informaționale etc.

Noțiunea de criminalitatea informatică, pe plan international (Comitetul European pentru Problemele Criminale) se foloseste exprimarea "criminalitatea legată de calculator” – ”computer related crime" [1].

Caracteristica privind criminalitatea informatică produsă în Republica Moldova rezultă din evaluările grupărilor criminale care acţionează în domeniu:

- caracter predominant financiar, se urmărește obţinerea unui produs financiar substanţial şi sunt vizate sisteme de plată, produse de credit şi plăți oferite de instituţii financiare;
- organizarea grupărilor care acţionează, structurarea şi specializarea membrilor acestora;
- folosirea unor tineri cu abilităţi în a utiliza computerele şi noile tehnologii, care sunt organizaţi şi coordonaţi de către lideri ai grupărilor infracţionale;
- trecerea de la fraudele informatice, în care încrederea era elementul primordial în realizarea tranzacţiilor, la fraudarea cu folosirea anumitor programe informatice speciale;
- caracterul transnaţional al acestor fapte, alienarea victimilor din alte ţări, fiind anumite activităţi care sunt derulate de pe teritoriul altor state sau sunt folosite sisteme informatice din alte state;
- permanenta preocupare pentru identificarea a noilor modalități de operare, de identificarea a produselor ce pot fi fraudate, precum şi sisteme informatice ce pot fi compromise;

- reorientarea grupărilor infracţionale către fraudarea mijloacelor de plată electronică oferite de instituţiile financiare din Republica Moldova;
- reorientarea grupărilor infracţionale care comit fraude informatice, de la fraudele mărunte (prejudicii mici) îndreptate împotriva persoanelor, către fraudele mari (prejudicii mari a sute de mii/milioane de euro) împotriva companiilor;
- zonarea infractorilor pe tipuri de infracţiuni şi ţări de destinaţie, datorate specificului zonei (zone turistice, zone cu număr ridicat de grupări infracţionale bine organizate etc) [2].

La nivel internațional criminalitatea informatică se atribuie, în deosebi unei din celei mai răspândite forme particulare a criminalității gulerelor albe, având o serie de factori decisivi cu un rol deosebit și anume: concentrarea de informații, ușor de modificat în sistemele informatizate si legate între ele, ce face mai vulnerabil acest mediu în ceea ce privește calitățile sale de disponibilitate, de integrare și de exclusivitate; stocarea datelor sensibile sau strategice privind dezvoltarea de produse noi, de informații financiare sau despre vizibilitatea securizată a clienților în organizații. Calculatorul central, liniile de comunicații sunt puncte în care se pot produce cu ușurință acțiuni infracționale, fiind o problematică ce capătă dimensiuni speciale, printr-o sursă inginerată, atunci când fluxurile de date trec între calculatoarele conectate într-o rețea sau pot prezenta un caracter transfrontalier, și anume:

- **Frauda-salam** presupune manipularea unui număr însemnat de mici sume de bani. În programul care calculează și bonifică dobanzile se fac anumite modificări pentru a "rotunji în jos" sumele bonificate ale clienților și transferarea, în contul infractorului, a sumei astfel obtinute.
- **Frauda-Zap** este numele unei comenzi (program) care realizează ștergerea de date de pe hard-discul unui calculator, desigur ca o activitate ileglă.
- **Necurățirea** dacă memoria internă a calculatorului nu este curățată după rularea fiecarui program, în diverse locații rămân date reziduale.Tehnic, este posibil ca un utilizator cu acces la calculatorul respectiv să poată citi aceste date reziduale, care pot fi confidențiale, dar foarte rar din aceste date se pot obține date comprehensibile.
- **Programe-aspirator** sunt acele programe care înregistrează neautorizat parolele folosite de utilizatori.
- **Substituirea Piggy** apare când o persoană neautorizată pretinde că este un utilizator autorizat, pentru a obtine acces la un calculator sau la o rețea de calculatoare.

- **Capcana** reprezintă acele instrucțiuni care permit utilizarea frauduloasă a calculatoarelor prin înlăturarea barierelor de securitate [3 p.199].

Reglementarea infracțiunilor informatice în legislația națională și anume, în Codul penal al Republicii Moldova, adoptat prin Legea nr. 985 din 18.04.2002, în vigoare din 12.06.2003 fost introdus capitolul ”Infracțiuni informatice și Infracțiuni în domeniul telecomunicațiilor”, care cuprindea inițial trei articole:

- art. 259 – Accesul ilegal la informația computerizată;
- art. 260 – Producerea, importul, comercializarea sau punerea ilegală la dispoziție a mijloacelor tehnice sau produselor program;
- art. 261 – Încălcarea regulilor de securitate a sistemului informatic.

După ratificarea Convenției Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23.11.2001, prin Legea nr. 6 din 02.02.2009, Codul penal al R.Moldova, a fost armonizat în conformitate cu prevederile Convenției prin Legea nr 278 din 18.12.2008, fiind suplinit cu articole noi 260/1-260/6, care prevedeau noi tipuri de infracțiuni cum ar fi interceptarea ilegală a unei transmisii de date, perturbarea funcționării sistemului informatic, falsul informatic, frauda informatică, etc [4].

Convenția Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23.11.2001, are ca scop principal armonizarea dispozițiilor de drept cu caracter penal în domeniul infacționalității informatice și implimentarea a dispozițiilor procedurale care sunt în deosebi importante și necesare pentru investigarea și urmărirea a asemnea infracțiuni, la fel și elaborarea unui mecanism privind preveirea și combaterea acestora printr-un sistem de cooperare internațională [5]. Totodată, este important de specificat tipologia infracțiunilor din domeniul informatic stipulate în Convenţia Consiliului Europei privind criminalitatea informatică, și anume:

- Infracțiuni împotriva confidențialității, integrității și disponibilității unui sistem computerizat sau datelor în format electronic: accesul ilegal; interceptarea ilegală; modificarea datelor; accesul neautorizat într-un sistem computerizat; utilizarea metodelor ilicite.
- Infracțiuni în domeniul sistemelor computerizate: falsuri în domeniul sistemelor computerizate; Fraude în domeniul sistemelor computerizate.
- Infracțiuni legate de conținutul datelor în format electronic: infracțiuni legate de pornografia infantilă.

- Infracțiuni legate de încălcarea drepturilor de proprietate intelectuală și a drepturilor conexe.

Astfel, în sens generalizat fraudele informatice prezintă a fi *"orice infracțiune comisă prin intremediul calculatorului sau o rețea de calculatoare fiind obiectul unei infacțiuni sau instrumentul și mediul de înfăptuire a unei infracțiuni informatice"* sau *„orice acțiune ilegală în care un calculator constituie instrumentul sau obiectul delictului, sau, altfel spus, orice infracțiune al cărei mijloc sau scop este influențarea funcționării normale a calculatorului".*

Potrivit, Raportului Comitetului European pentru problemele criminale, infracțiunile informatice sunt clasificate în următoarele categorii: infracțiunea de fraudă informatică; infracțiunea de fals în informatică; infracțiunea de prejudiciere a datelor sau programelor informatice; infracțiunea de sabotaj informatic; infracțiunea de acces neautorizat la un calculator; infracțiunea de interceptare neautorizată; infracțiuna de reproducere neautorizată a unui program informatic protejat de lege; infracțiunea de reproducere neautorizată a unei topografii; infracțiunea de alterare fară drept a datelor sau programelor informatice; infracțiunea de spionaj informatic; etc [6 p.51].

Manualul Națiunilor Unite pentru prevenirea și controlul infacționalității sistematizează următoarele categorii de infracțiuni informatice, și anume: fraude prin manipularea calcultoarelor electronice; fraude prin falsificare de documente; alterarea sau modificarea datelor sau a programelor pentru calculator; accesul neautorizat la sistemele și serviciile informatice și reproducerea neautorizată a programelor pentru calculator protejate de lege [7 p.57]. Totodată, potrivit studiului COMCRIM, realizat pentru Comisia Europeană de către prof. dr. Ulrich Sieber, de la Universitatea din Wurzburg, Germania, sunt prezentate următoarele categorii și sub-categorii de infracțiuni informatice: atingeri aduse dreptului la viaţa private și infracţiuni cu caracter economic, precum: penetrarea sistemelor informatice in scopul depăşirii dificultăţilor tehnice de securitate ("HACKING"); spionajul informatic; pirateria programelor pentru calculator; sabotajul informatic; frauda informatică; distribuirea de informaţii cu caracter ilegal sau prejudiciabil (propagandă rasistă,difuzare de materiale pornografice, etc.); și alte infracţiuni: infracţiuni contra vieţii; infracţiuni legate de crima organizată și război electronic.

Cu prilejul Summitului G8 de la Denver, miniştrii de interne şi de justiţie ai statelor prezente la reuniune au luat act de intensificarea fără precedent a acţiunilor criminale în domeniul informaticii, la care a fost adopoptat un document final. Astfel, reprezentanţii G8 au discutat despre pericolul acestui tip de infracţionalitate fiind clasificat în două mari domenii:

- criminalitatea informatică care are ca scop distrugerea reţelelor de calculatoare şi sistemul de telecomunicaţii, fapt care produce pagube importante atât autorităţilor oficiale, cât şi persoanelor private;
- organizaţiile teroriste sau de crimă organizată care utilizează facilităţile noilor tehnologii pentru săvârşirea de infracţiuni deosebit de grave.

Comunicarea prezentată la sfârşitul Summitului G8 din anul 1997 cuprinde 10 principii şi direcţii de acţiune pentru combaterea criminalităţii informatice, idei care au fost citate în foarte multe Recomandări şi Directive care au fost adoptate din 1998 până în prezent [8]. Conform comunicării pezentate au fost specificate următoarele *principii*: nu trebuie să existe nici un loc sigur pentru cei care comit abuzuri prin intermediul tehnologiei informatice; investigaţiile şi pedepsele aplicate acestor infracţiuni trebuie coordonate cu sprijinul tuturor statelor, chiar dacă nu se produce nici un fel de pagubă; legea trebuie să combată explicit fiecare infracţiune de acest tip; legea trebuie să protejeze confidenţialitatea, integritatea şi utilitatea bazelor de date informatice, precum şi să sancţioneze pătrunderea neautorizată în sistemele informatice; legea trebuie să permită apărarea şi conservarea bazelor de date cu acces rapid, cele mai expuse din punct de vedere al atacurilor exterioare; regimul de asistenţă mutuală al statelor trebuie să permită informarea periodică şi în caz de necesitate, în situaţiile unor infracţiuni trans-continentale; accesul la baze de date electronice deschise trebuie să se poată realiza liber, fără acordul statului pe teritoriul căruia se află acestea; regimul juridic privind trimiterea şi autentificarea datelor electronice utilizate în cazul investigaţiilor informatice trebuie dezvoltat; extinderea unui sistem de telecomunicaţii practic şi sigur trebuie cumulată cu implementarea unor mijloace de detecţie şi prevenire a abuzurilor; activitatea în acest domeniu trebuie coordonată de instituţii şi foruri internaţionale specializate în domeniul informatic.

Totodată, *planul de acţiune* cuprindea următoarele direcţii: utilizarea reţelei proprii de calculatoare şi a cunoştinţelor acumulate în domeniu pentru a asigura o comunicare exactă şi eficientă privind cazurile de criminalitate care apar în reţele mondiale; realizarea paşilor necesari creării unui sistem legislativ modern şi eficace pentru combaterea fenomenului care să fie pus la dispoziţia statelor membre; revizuirea legislaţiei naţionale a ţărilor membre şi armonizarea acestora cu legislaţia penală necesară combaterii criminalităţii informatice; negocierea unor noi acorduri de asistenţă şi cooperare; dezvoltarea soluţiilor tehnologice care să permită căutarea transfrontalieră şi efectuarea unor investigaţii de la distanţă; dezvoltarea procedurilor prin care pot obţine date de interes de la responsabilii sistemelor de telecomunicaţii; concertarea eforturilor cu ramurile industriale pentru obţinerea celor mai noi tehnologii utilizabile în combaterea criminalităţii

informatice; asigurarea de asistenţă în cazul unor solicitări urgente prin întregul sistem tehnologic propriu; încurajarea organizaţiilor internaţionale din sistemul informatic şi cele din telecomunicaţii pentru creşterea standardelor şi măsurilor de protecţie oferite sectorului privat; realizarea unor standarde unice privind transmiterea datelor electronice utilizate în cazul investigaţiilor oficiale sau private.

Concluzii și recomadări

Analizând cele menționate supra, este evident faptul că fenomenul criminalității informatice este în continuă creștere, fiind generat de dezvoltarea avansată a tehnologiilor, acest fapt la rândul său determină facilitarea și crearea noilor oportunități pentru săvârșirea infracțiunilor informatice.

Avansarea și dezvoltarea noilor programe, aplicații, tehnologii și sisteme informatice, sub viziunea utilității sociale are un impact pozitiv, dar tot odată impactul negativ acestor sisteme poate aduce la recrutarea asupra securității statului, securității cetățenilor, protecției datelor cu caracter personal, confidențialității și a libertăților fundamentale al acestora, atât a persoanelor fizice cât și juridice.

Reeșind din analiza situațiilor practice pe teritoriul RM, avansează fenomenul criminalității informatice, din anumite aspecte persoanele care au fost prejudiciate în multe cazuri nu declară că sunt victime a infacțiunilor informatice, sau la declararea acestora instituțiile de stat nu sunt eficient atrenate în investigarea crimelor informatice fapt ce generează nedescoperirea acestora. Considerăm că în deosebi este important ca la nivel național cu privire la investigarea crimelor informatice să se recurgă și să se aplice procedeile probării prevăzute de CPP și la rândul său formarea unui grup sau subinstituții specializate în tactica criminalistică și cercetare a infracțiunilor informatice.

Totodată, considerăm că insituțiile de stat responsabile de investigarea și cercetarea criminalistică a infracțiunlor informatice ar trebui să colaboreze cu organizațiile internaționale responsabile în prevenirea și combaterea infracționalității informatice, prin cerearea structurilor, acordurilor de colaborarea internațională mai eficientă, cu scopul desoperii rapide a infracțiunilor informatice comise pe teritoriul Republicii Molodva, cât și în afara acesteia.

Bibliografie

1. https://www.coe.int/en/web/cdpc (accesat la 15.01.2023)

2. http://www.academia.edu/9204220/CRIMINALITATEA_INFORMATIC (accesat la 15.01.2013)

3. Pavleanu V., Drept penal european : Ediția Lumen, Iași, România, 2018, p.199.

4.Codul penal al Republicii Moldova, nr. 985-XV din 18.04.2002. În: Monitorul Oficial l Republicii Moldova nr.128-129/1012 din 13.09.2002. Republicat în: Monitorul Oficial al Republicii Moldova nr.72-74/195 din 14.04.2009.

5. https://eur-lex.europa.eu/legal-content/RO (accesat la 17.01.2023).

6. Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică / Ministerul Comunicațiilor și Tehnologiilor Informaționale. București, 2004, p.51-52

7. Sfetcu N. Manualul investigatorului în criminalitatea informatică. Ministerul Comunicației și Tehnologiiloc Informaționale, p.57 http://uploads.worldlibrary.net (accesat la 17.01.2023).

8. https://1997.2001.state.gov/issues/economic/summit/g8.html (accesat la 18.01.2023).