CZU: 343.3:004

RISCURILE ASOCIATE EVOLUȚIILOR DIN DOMENIUL TEHNOLOGIILOR INFORMAȚIONALE ȘI DE COMUNICAȚII

Nicolae VASILIȘIN,
doctorand, asistent universitar,
Catedra „Activitate specială de investigații și anticorupție”
a Academiei „Ștefan cel Mare” a MAI
ORCID: 0000-0002-8840-8750

Rezumat

Secolul XXI se confruntă cu un nou element al criminalității - infracțiunile informatice care au luat turații tot mai mari la nivel global, iar pentru a învinge aceste amenințări la securitatea cibernetică, care afectează inclusiv drepturile și libertățile fundamentale ale omului, fiecare stat urmează să-și elaboreze și implementeze un sistem de garanții solide pentru așsi consolida securitatea și a respinge atacurile cibernetice externe și interne, iar utilizarea securizată a tehnologiilor informaționale și de comunicații trebuie să devină o prioritate.

Cuvinte-cheie: drepturi și libertăți fundamentale ale omului, securitate cibernetică, infracțiuni informatice, tehnologii informaționale și de comunicații, riscuri, activitate specială de investigații, măsuri speciale de investigații.

Summary

The 21st century is faced with a new element of crime - computer that have increased at a global level, and in order to defeat these threats to cyber security, which also affect fundamental human rights and freedoms, each state is going to develop and implement a system of solid guarantees to strengthen its security and repel external and internal cyber-attacks, and the secure use of information and communication technologies must become a priority.

Keywords: fundamental human rights and freedoms, cyber security, computer crimes, information and communication technologies, risks, special investigative activity, special investigative measures.

Tehnologiile informaționale și de comunicații continuă să se dezvolte intensiv, iar pe măsură ce această tehnologie devine tot mai integrată în mai multe aspecte ale vieții umane, se extind și riscurile asociate evoluției acestui sector.

Evoluția rapidă a tehnologiilor informaționale și de comunicații (în

continuare – TIC) a impulsionat și dezvoltarea legislației în acest domeniu. În acest sens, fiecare țară își asigură în mod independent elaborarea cadrului normativ și aplică mecanisme, inclusiv ajustate la normele internaționale, orientate la opunerea de rezistență și de înlăturare a eventualelor riscuri privind securitatea cibernetică care poate afecta dur securitatea țării, drepturile și libertățile fundamentale ale omului.

Astfel, legea penală a Republicii Moldova stabilește categoriile de pedepse penale pentru șirul de infracțiuni comise prin utilizarea tehnologiilor informaționale și de comunicații, iar infracțiunilor informatice și în domeniul comunicațiilor electronice îi dedică un capitol separat [1]. De asemenea, pentru șirul de contravenții comise prin utilizarea tehnologiilor informaționale și de comunicații, legea contravențională stabilește sancțiuni contravenționale, iar contravențiilor în domeniul comunicațiilor electronice și al comunicațiilor poștale îi consacră la fel un capitol separat [2].

De rând cu reprimarea și pedepsirea acțiunilor ilegale prin utilizarea TIC, statul încurajează dezvoltarea domeniului tehnologiilor informaționale și de comunicații, iar în acest sens, acordă unele facilități fiscale prin aplicarea normelor speciale rezidenților parcurilor pentru tehnologia informației și angajaților acestora, adică reduce sau exclude unele taxe [3].

Dezvoltarea industriei tehnologiei informației, cercetării și inovării, bazată pe tehnologia informației în diverse domenii, activității didactice în domeniul tehnologiei informației, precum și crearea locurilor de muncă cu valoarea adăugată înaltă, atragerea investițiilor autohtone și străine pentru dezvoltarea TIC este încurajată prin Legea nr. 77 din 21.04.2016 cu privire la parcurile pentru tehnologia informației, iar în baza acestei legi, sunt acordate facilități și stimulente la crearea și funcționarea parcurilor pentru tehnologia informației [4].

Cadrul normativ național privind reglementarea domeniului TIC este variat, iar în baza bunelor practici europene și internaționale, poate fi îmbunătățit și dezvoltat.

Uniunea Europeană (în continuare – UE) promovează tranziția digitală modelată la valorile europene, dorind să ofere cetățenilor mijloace necesare pentru a se bucura pe deplin de oportunitățile pe care le oferă această tranziție. În decembrie 2022 a fost semnată Declarația europeană privind drepturile și principiile digitale pentru deceniul digital [5], care prezintă viziunea UE pentru un deceniu de transformare digitală. Declarația oferă un cadru de referință pentru cetățeni, pentru factorii de decizie, pentru companii și instituții atunci când interacționează cu tehnologiile digitale sau când implementează noi tehnologii, inclusiv ghidează UE și statele membre spre o transformare digitală, asigurând respectarea drepturilor și libertăților omului în conformitate cu valorile și drepturile fundamentale ale UE. Aceas-

tă Declarație include referințe privind suveranitatea digitală într-o manieră deschisă, privind respectarea drepturilor fundamentale, privind statul de drept și democrația, incluziunea, accesibilitatea, egalitatea, durabilitatea, reziliența, securitatea, precum și îmbunătățirea calității vieții, disponibilitatea serviciilor, respectul pentru drepturile și aspirațiile fiecăruia.

Capitolul V al Declarației prenotate este dedicat siguranței, securității și capacității de acțiune pentru crearea unui mediu digital protejat, sigur și securizat, iar pentru realizarea acestui scop UE și-a asumat un șir de angajamente orientate la asigurarea mediului digital protejat, sigur și securizat, la asigurarea vieții private și a controlului individual asupra datelor și la asigurarea protecției și capacitării copiilor și tinerilor în mediul digital.

Asumarea angajamentelor menționate urmăresc scopuri determinate de a include oamenii în centrul transformării digitale, asigurând pentru fiecare persoană accesul la tehnologii, produse și servicii digitale care, din momentul conceperii lor, trebuie să fie sigure și securizate pentru a proteja viața privată și de a oferi la un nivel ridicat confidențialitatea, integritatea, disponibilitatea și autenticitatea informațiilor prelucrate.

Totodată, nivelul scăzut de securitate cibernetică a produselor cu elemente digitale, cuprins de vulnerabilități larg răspândite, constituie nu doar provocări cheie pentru Republica Moldova, dar se află în atenția Uniunii Europene cât și în preocuparea altor state. Atacurile cibernetice, care iau tot mai mare amploare, au un impact critic nu numai asupra securității economice a țărilor țintă, dar și asupra democrației, siguranței și sănătății consumătorilor.

Instrumentele legislative elaborate și puse în aplicare de către UE, inclusiv Regulamentul Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale de securitate cibernetică pentru produsele cu elemente digitale, stabilesc condițiile limită pentru dezvoltarea securității produselor cu elemente digitale [6].

Republica Moldova, țară candidată la aderare la UE, și-a asumat angajamente de aducere a actelor legislative naționale în concordanță cu legislația europeană, iar acest fapt vizează și domeniul tehnologiilor informaționale și de comunicații.

La 16.03.2023, Parlamentul Republicii Moldova a adoptat Legea nr. 48 privind securitatea cibernetică [7], care stabilește competența autorităților și instituțiilor publice în materie de securitate cibernetică, determină cadrul național general de gestionare a crizelor în domeniul securității cibernetice, instituie cerințe, măsuri și mecanisme în scopul asigurării securității rețelelor și sistemelor informatice, care sunt esențiale pentru funcționarea societății și pentru gestionarea incidentelor cibernetice.

Sectoarele de comunicații electronice, tehnologiei informației și co-

municaţiei poştale se află în domeniul de competenţă a Agenţiei Naţionale pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei a Republicii Moldova (în continuare – ANRCETI). Agenţia menţionată asigură implementarea strategiilor de dezvoltare a sectoarelor nominalizate şi supraveghează respectarea de către furnizorii de pe pieţele de comunicaţii electronice şi de servicii poştale a legislaţiei în acest domeniu, precum şi conform competenţei, constată şi examinează contravenţiile prevăzute în art. 410 al Codului contravenţional al Republicii Moldova.

Domeniile de competenţă privind administrarea infrastructurii de tehnologie a informaţiei şi a Sistemului de telecomunicaţii al autorităţilor administraţiei publice ca parte a reţelei de comunicaţii speciale, administrarea şi menţinerea sistemelor informaţionale de stat, securitate cibernetică, gestionarea infrastructurii unice a cheii publice a Guvernului, implementarea tehnologiilor informaţionale în sectorul public, îi revin Instituţiei Publice „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" (STISC).

Modelul organizaţional de securitate cibernetică în Republica Moldova este reprezentat de autorităţi şi instituţii publice, aflate în structura administrativă a Guvernului sau în afara acesteia, investite cu drepturi şi responsabilităţi în vederea realizării politicii de stat în domeniul securităţii cibernetice. Autorităţile şi instituţiile publice care asigură supravegherea şi controlul în domeniul tehnologiilor informaţionale şi de comunicaţii, au menirea să aplice toate mecanismele existente naţionale şi internaţionale orientate la identificarea oportună a potenţialelor riscuri de securitate cibernetică, inclusiv a vulnerabilităţilor persoanelor faţă de manipularea lor online. Prin urmare, progresul legislativ este interdependent de progresul tehnologic, iar eventualele riscuri care pot afecta drepturile şi libertăţile omului pot fi anticipate şi/sau înlăturate prin stabilirea şi aplicarea unor mecanisme sigure şi eficace.

Sistemul tehnologiilor informaţionale se confruntă şi la nivel global cu multiple riscuri *software* şi *hardware*, iar aceste pericole se manifestă prin breşe de date (informaţii) şi întreruperi operaţionale, pierderi de date, ori capacităţi operaţionale reduse, care în rezultat produc defecţiuni al întregului sistem. Erorile *software* şi eşecurile *hardware* pot aduce la imposibilitatea funcţionării tehnicii utilizate, iar unii viruşi de infectare a programelor operaţionale, utilizaţi de hackeri şi infractori cibernetici, contribuie la delapidarea datelor şi informaţiilor despre persoane fizice şi juridice care pot fi utilizate pentru comiterea de infracţiuni, ori pot servi ca obiect de răscumpărare.

Securitatea cibernetică se află în atenţia permanentă a agenţiilor specializate ale statelor supuse unor astfel de riscuri, iar cea mai veche agenţie din familia Organizaţiei Naţiunilor Unite (în continuare - ONU), specializată pentru tehnologiile informaţiei şi comunicaţiilor, este Uniunea Internaţională a Telecomunicaţiilor (în continuare - ITU). Această agenţie (ITU) îşi

are sediul la Geneva, Elveţia, iar birourile ei regionale sunt active pe fiecare continent. ITU a fost înființată în 1865 și are o istorie a inovației de la gestionarea primelor rețele telegrafice internaționale la invenția telefoniei vocale, dezvoltarea radiocomunicațiilor, lansarea primilor sateliți de comunicații până la recenta inteligență artificială și metaversul. Obiectivul de bază al ITU rămâne a fi valorificarea inovațiilor în sectorul TIC și conectarea la acest sector a întregii lumi pentru a le asigura un viitor mai bun. La nivel global, ITU este unul din cele mai reprezentative organizații, având reprezentanți a 194 de state membre și un suport de la peste 1000 de companii, universități și organizații internaționale și regionale [8].

Deci, la nivel mondial, există mecanisme de evaluare a incidentelor informatice, iar riscurile asociate tehnologiilor informaționale și de comunicații, pot fi relevate și înlăturate, inclusiv cu suportul specialiștilor în domeniu din cadrul Uniunii Internaționale a Telecomunicațiilor.

Experții ITU au evaluat Republica Moldova la compartimentul etapelor parcurse de transformare digitală și au identificat riscurile asociate tehnologiilor informaționale și de comunicații, iar în decembrie 2022 a fost publicat Raportul de evaluare a Moldovei „Incidentul informatic național. Echipa de răspuns (CIRT-MD)" [9].

Potrivit raportului menționat, Republica Moldova are un peisaj al amenințărilor cibernetice similar altor țări, care vizează nu numai entitățile guvernamentale, dar și sectorul privat și populația în general. Deși, autoritățile urmăresc și monitorizează peisajul amenințărilor cibernetice legate de entitățile guvernamentale, potrivit experților ITU, lipsește înțelegerea holistică a atacurilor cibernetice care au loc în țară. Cu toate acestea, ITU și-a propus să realizeze un proiect care vizează implementarea CIRT-MD (echipa de răspuns la incidentele computerizate) folosind metodologia programului ITU CIRT. Prin urmare, CIRT-MD devine punctul focal pentru coordonarea fluxului de informații atunci când va răspunde la atacurile cibernetice pentru a oferi remedierea incidentelor de securitate cibernetică în Moldova [10].

Programele anti-virus, firewall-uri și alte sisteme de monitorizare a amenințărilor se regăsesc printre mecanismele adecvate de a respinge un atac cibernetic, iar aceste mecanisme vor avea o eficiență sustenabilă când fiecare persoană care utilizează tehnologia digitală va avea și o instruire adecvată privind tehnologiile necesare de protecție contra riscurilor asociate tehnologiei digitale.

Manipularea online este un alt risc asociat domeniului tehnologiilor informaționale și de comunicații, iar potrivit academicienilor de la Universitatea din Cambridge [11], manipularea online este definită ca fiind utilizarea deficienților psihologice umane pentru a redirecționa comportamentul. Or, impactul social al tehnologiilor noi și emergente, precum modul în care

noile tehnologii ne afectează procesele de luare a deciziilor sunt comparate cu efectul Dunning-Kruger, care apare atunci când lipsa de cunoştinţe şi abilităţi a unei persoane într-un anumit domeniu îi determină să-şi supraestimeze propria competenţă, iar cei care excelează într-o anumită zonă de competenţă cred că sarcina ce stă în faţa lor este simplă pentru toată lumea, determinându-i să-şi subestimeze abilităţile.

Deci, manipularea online este un fenomen social ce a luat amploare globală şi a devenit un instrument tot mai eficient şi mai puternic, fiind comparat cu o „armă", care poate fi utilizată împotriva oricărei persoane sau unui grup de persoane, unui stat ori unui grup de state, alte ţinte, pentru obţinerea de către factorii interesaţi a unor scopuri determinate. Aceste riscuri însă nu înseamnă necesitatea impunerii unor interdicţii sau restricţionări a accesului liber la reţelele de informare, inclusiv online, dar dimpotrivă statul urmează să informeze şi să asigure toţi cetăţenii cu informaţii şi cu instruiri utile în vederea cultivării în societate a culturii digitale în spiritul respectării legii şi eticii tehnologiei informaţiei.

Criminalitatea informatică este la moment cel mai mare risc asociat tehnologiilor informaţionale şi de comunicaţii, iar spaţiul cibernetic a ajuns să fie utilizat pentru pregătirea şi comiterea diferitor infracţiuni, cu preponderenţă informatice şi de ciberterorism (*terorism electronic*), iar acţiunile malițioase (*răutăcioase*) sunt cel mai frecvent întâlnite în acest spaţiu. Penetrarea sistemelor informatice şi de comunicaţii electronice poate compromite confidenţialitatea şi integritatea informaţiilor sensibile, inclusiv a celor cu caracter personal, iar printre consecinţele acestor acţiuni se vor enumera cauzarea de prejudicii financiare şi morale, ori cauzarea prejudiciilor de altă natură. La fel, penetrarea sistemelor informatice pentru obţinerea controlului neautorizat asupra sistemelor aferente infrastructurii critice ale statului pot aduce daune colosale proceselor informaţionale, sociale, economice, militare, politice, etc.

Este dificil de a avea o predictibilitate privind totalitatea eventualelor riscuri asociate tehnologiilor informaţionale şi de comunicaţii, fiindcă acestea apar pe măsura tentativei şi/sau realizării acţiunilor de destabilizare a securităţii spaţiului cibernetic la general, iar în special a acţiunilor ilegale întreprinse împotriva unei persoane fizice sau juridice, or împotriva unei societăţi umane sau împotriva securităţii unui stat. De aceea, în scopul combaterii criminalităţii cibernetice, identificării riscurilor şi factorilor ce condiţionează acest fenomen, reieşind din natura globală a sistemelor informaţionale şi a reţelelor de comunicaţii electronice, este necesară o colaborare viabilă între toate instituţiile responsabile la nivel naţional, cât şi la nivel transnaţional.

Subiectul riscurilor asociate evoluţiei din domeniul tehnologiilor in-

formaţionale şi de comunicaţii este multidimensional şi poate fi dezvoltat încontinuu, însă cert este că pe măsura dezvoltării tehnologiei informaţiei o deosebită atenţie trebuie de acordat eticii tehnologiei informaţiei, care este o disciplină a eticii aplicate ce studiază problemele de ordin moral [12]. Noile progrese în mai multe tipuri de tehnologii cu siguranţă vor aduce provocări etice, iar inteligenţa artificială, biotehnologia, tehnologia de decarbonizare, etc. tehnologii ce vor apărea, vor fi însoţite de riscuri potenţiale printre care se va regăsi securitatea cibernetică a infrastructurilor critice ale statului, ori securitatea datelor personale şi vulnerabilitatea persoanelor la manipularea online. Aşadar, în următorul deceniu, vătămarea digitală, dezinformarea, interferenţa străină, etc. provocări, vor fi printre preocupările instituţiilor responsabile ale statului, care urmează să întreprindă măsuri de anticipare, atenuare şi combatere a riscurilor din domeniu tehnologiilor informaţionale şi de comunicaţii.

Printre mijloace utile şi eficiente în combaterea acţiunilor infracţionale din domeniu tehnologiilor informaţionale şi de comunicaţii se regăsesc măsurile speciale de investigaţii şi metodele activităţii speciale de investigaţii, prevăzute în legislaţia naţională [13], care constituie un instrument legal de a combate infracţiunile informatice.

Omenirea parcurge o eră în care inteligenţa artificială a devenit o necesitate indispensabilă în dezvoltarea tuturor ramurilor economiei, iar informarea şi comunicarea a devenit accelerată şi variată.

Multitudinea de riscuri asociate tehnologiilor informaţionale şi de comunicaţii, identificate şi care, pe parcursul dezvoltării acestui sector, vor apărea în noua sa formă de manifestare, urmează a fi cunoscute de către omenire, iar rezistenţa care urmează a fi opusă eventualelor provocări în domeniul tehnologiilor informaţionale şi de comunicaţii nu trebuie să îngrădească sau să încalce drepturile şi libertăţile fundamentale ale omului.

Referinţe bibliografice

1. Codul penal al Republicii Moldova nr. 985 din 18.04.2002, publicat la 14.04.2009 în Monitorul Oficial nr. 72-74 art.195, redacţia actualizată, noiembrie 2024, (art. 62, art.150, art. 175^1, art.177, art. 220^1, capitolul XI art.259-261^1).

2. Codul contravenţional al Republicii Moldova nr. 218 din 24.10.2008, publicat la 17.03.2017 în Monitorul Oficial nr.78-84 art. 100, redacţia actualizată noiembrie 2024 (art.32, capitolul XIV art. 246-262).

3. Codul fiscal al Republicii Moldova nr. 1163 din 24.04.1997, publicat la 18.09.1997 în Monitorul Oficial nr. 62 art. 522, redacţia actualizată, noiembrie 2024, (art.14^1, art. 27^1, art. 51^4, art.282^1, art. 294^1, art. 342^1, art. 367–379).

4. Legea Republicii Moldova nr. 77 din 21.04.2016 cu privire la parcurile pentru tehnologia informației, publicat la 10.06.2016 în Monitorul Oficial nr. 157-162 art.318, redacţia actualizată, noiembrie 2024, (art. 2, art. 15).

5. Declarația europeană privind drepturile și principiile digitale pentru deceniul digital, semnată la 15 decembrie 2022 de către președinții Consiliului UE, Parlamentului European și a Comisiei „Busola digitală 2030 o cale europeană de urmat pentru deceniul digital", publicată 2023/C 23/01.

6. Regulamentul Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerinţele orizontale de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) nr. 168/2013 și (UE) 2019/2020 și Directiva (UE) 2020/1828 (Legea privind rezistența energetică).

7. Legea Republicii Moldova nr. 48 din 16.03.2023 privind securitatea cibernetică, în vigoare din 01.01.2025, publicată la 28.04.20223 în Monitorul Oficial nr. 151-153 art. 225, redacţia actualizată, noiembrie 2024;

8. International Telecommunication Union (ITU). https://www.itu.int/en/Pages/accessibility.aspx

9. https://moldova.un.org/sites/default/files/2023-01/CIRT-Assessment -Moldova-final.pdf

10. Assessment report of Moldova National Computer Incident Response Team (CIRT-MD). https://moldova.un.org/ro/node/216556

11. What is online manipulation and how do we regulate it? 12 March 2019, © 2024 Centre for Science and Policy.

12. Etica tehnologiei informației. https://ro.wikipedia.org/wiki/Etica_tehnologiei_informației

13. Codul de procedură penală al Republicii Moldova nr. 122 din 14.03.2003, publicat la 05.11.2013 în Monitorul Oficial nr. 248-251 art. 699, redacţia actualizată, noiembrie 2024, (secţiune a V-a).

14. Legea privind activitatea specială de investigații nr. 59 din 29.03.2012, publicat la 08.06.2012 în Monitorul Oficial nr. 113-118 art. 373, redacţia actualizată, noiembrie 2024.