PROVOCĂRI CONTEMPORANE DE SECURITATE ÎN ERA DIGITALĂ

CONTEMPORARY SECURITY CHALLENGES IN THE DIGITAL ERA

CZU: 342.34(478):004.056.5:007 https://doi.org/10.5281/zenodo.7885413

Angela BURLEA[1]

ABSTRACT. *This article focuses on the analysis of the subject of contemporary security challenges in the digital age in the context of the democratization process of the Republic of Moldova, a complex and multidimensional process, which requires the involvement of political actors, but also of society in all segments, mainly in the implementation of political and economic reforms, of citizens' security, with respect for fundamental human rights, free and fair elections and the achievement of the proposed European objectives.*

The sharp advancement of digital technologies in strategic fields such as the energy sector, health, education or transport, open up various opportunities and offer a range of solutions for efficient activity, simultaneously increasing the degree of cyber threats including the multiple security challenges facing the Republic of Moldova, accentuated against the backdrop of the COVID-19 pandemic crisis, but not least the war in Ukraine, requiring actions dedicated to security to focus on concrete directions that reduce security risks and threats on a national and international level.

Keywords: *security challenges, democratization, European Union, risks, digital technologies, human rights, globalization, cyber threats.*

REZUMAT. *Prezentul articol se axează pe analiza subiectului provocărilor contemporane de securitate în era digitală în contextul procesului de democtatizare a Republicii Moldova, proces complex și multidimensional, care necesită implicarea actorilor politici, dar și a societății pe toate segmentele, preponderent în implementarea reformelor politice și economice, a securității cetățenilor, cu respectarea drepturilor fundamentale ale omului, alegeri libere și corecte și atingerea obiectivelor europene propuse.*

Avansarea accentuată a tehnologiilor digitale în domenii strategice precum sectorul energetic, sănătate, educație sau transport, deschid varii oportunități și oferă o gamă de soluții pentru activitatea eficientă, concomitent sporind gradul de amenințări cibernetice inclusiv multiplele provocări de securitate cu care se confruntă Republica Moldova, acentuate pe fundalul crizei pandemice COVID-19,dar nu și în ultimul rând a războiului din Ucraina, necesitând ca acțiunile dedicate securității, să se axeze pe direcții concrete care să reducă riscurile și amenințările de securitate pe plan național și internațional.

Cuvinte-cheie: *provocări de securitate, democratizare, Uniunea Europeană, riscuri, tehnologii digitale, drepturile omului, globalizare, amenințări cibernetice.*

[1] Angela BURLEA, Doctorandă, Școala Doctorală Științe Sociale și ale Educației, Universitatea de Stat din Moldova, Chișinău, Republica Moldova, ORCID: https://orcid.org/0000-0001-8973-274X , email: pefrispaburlea.angela@gmail.com

Introducere

Problema riscurilor și a provocărilor contemporane de securitate în contextul procesului de democratizare a Republicii Moldova a accedat semnificativ în ultimii ani și rămâne a fi a o preocupare prioritară a structurilor de stat.

În cadrul studiului ne propunem ca scop cercetarea provocărilor contemporane de securitate generate de avansarea procesului de democratizare în RM, a diverselor aspecte ale provocărilor contemporane de securitate corelate cu problematica democratizării statului în era digitală.

Liberalizarea regimului vizelor, intrat în vigoare la 28 aprilie 2014; Acordul de asociere UE-Republica Moldova cu zona sa de liber schimb,din 01.07.2016; angajamentul de a consolida asocierea politică și integrarea economică dintre UE și Republica Moldova, inițiat în anul 2016; măsurile temporare de liberalizare a comerțului, operațiune de asistență macrofinanciară sub formă de împrumuturi și granturi în beneficiul Republicii Moldova, pe fundalul războiului din Ucraina - constituie acțiuni concrete ce reflectă voința politică a guvernării RM spre un proces de democratizare în era digitală, axat pe protejarea și promovarea demnității umane,acestea permițând comunității să soluționeze, cu ajutorul tehnologiilor informaționale moderne varii sarcini socio-politice, să acceadă la informații publice, să participe la procesele democratice, să-și exprime voința politică, digitalizarea deschizând oportinități și asigurând soluții la varii provocări,inclusiv în contextul crizei Covid-19 ,în domenii de importanță strategică precum sănătatea,educația,finanțele sau transportul, prin urmare, concomitent cu sporirea gradului de informatizare a societății, sporesc și riscurile din spațiul cibernetic, tehnologiile informaționale fiind interconectate la nivel global.

În condițiile în care RM în parcursul său european tinde către digitalizarea domeniilor strategice, în scopul consolidării instituțiilor și proceselor democratice și a bunei guvernări, democrația fiind un element-cheie al societății, se reliefează un șir de provocări contemporane de securitate.

În sens larg, prin provocare de securitate înţelegem ansamblul factorilor de naturi diverse ce pot declanşa riscuri, pericole şi ameninţări în materie de securitate la adresa societăţii umane [3,pag.8],astfel putem afirma că specificul procesului de democratizare autohton îl face vulnerabil la o serie de amenințări de securitate ce vizează atât infrastructura dar și participanții la procesul de digitalizare, în acest context, prin prisma provocărilor de securitate menționăm:

Dezinformarea și propaganda (tv,rețele de socializare),constituie amenințări majore care pun în pericol și perecliteză buna desfășurare a proceselor democratice,cu un impact puternic direct asupra securității ,constituind o amenințare directă, prezentând un prejudiciu public, dezinformările influențând opțiunile cetățeanului și diminuând încrederea în procesele democratice. Știrile și informațiile false ce pot distorsiona și afecta percepția publică sau pot influența

emoțiile umane, manipulând astfel,pentru a le afecta percepția asupra realității. [4,pag. 96].

Amenințările cibernetice, atacurile la adresa alegerilor sau a infrastructurii de vot ar putea fi inițiate atît din interiorul țării cît și din exteriorul acesteia. Scopurile urmărite de către cei care stau la baza atacurilor cibernetice, au mai multe consecințe nefaste, precum denigrarea imaginii entităților publice,prin demonstrarea incapacității acestora de a asigura buna desfășurare a procesului de democratizare în situații de criză, manipularea opiniei publice, drept urmare rezultând instabilitătea social-politică.

Atacuri cibernetice împotriva păcii și securității, desfășurate concomitent cu dezinformarea, presiunile economice sau atacuri armate convenționale, pun la încercare reziliența statelor și instituțiilor democratice, atentând în mod direct la pacea și securitatea UE. Conform ENISA, în timpul războiului rus în Ucraina atacurile cibernetice au loc în paralel cu acțiunile militare convenționale,urmărind să distrugă sau să perturbe funcționarea agențiilor guvernamentale și a entităților ce țin de infrastructura esențială, și de asemenea să submineze încrederea cetățenilor în conducerea țării. Astfel, constatăm că impactul asupra democrației se extinde dincolo de economie și finanțe, fiind afectate fundamentele democratice și amenințând funcționarea normală a societății.

*Criza cauzată de pandemia de Covid-19 ,c*are a afectar sever inlusiv RM, o provocare majoră ce presupune asigurarea unor măsuri eficiente din partea autorităților în combaterea riscurilor epidemice şi a consecinţelor acestora.

Comportamentul agresiv al unor actori statali şi non-statali , interesele cărora sunt contrar opuse celor ale RM, în condițiile în care acţiunile, planurile sau faptel acestora au ca scop subminarea autorităţilor şi afectarea atributelor fundamentale ale statului , caracterul, suveran și independent , inclusiv instigarea la fapte ce pot periclita ordinea statului de drept, blocaje în parcursul european și perpetuarea instabilităţii economice, acesta continuând să reprezinte o provocare la adresa securităţii naţionale.

*Provocări economice.*Legătura dintre economie şi securitate este una puternică, de interdependenţă, cele două consolidându-se reciproc. În condiţiile unei economii funcţionale şi competitive un actor se poate bucura de securitate şi, invers, starea de securitate are un aport considerabil în funcţionarea optimă a economiei. Prin urmare, prin provocări economice, înţelegem o serie de fenomene care se manifestă în plan economic şi care, prin evoluţia, implicaţiile şi consecinţelor, pot reprezenta riscuri de securitate identificabile [3, pag.13] .

Fluctuațiile de pe piața energetică, precum şi acţiunile sau inacţiunile care lezează interesele economice strategice ale RM , afectează eforturile de asigurare a unui nivel suficient al securității energetice.

În vederea asigurării unui sistem de protecție și dezvoltare a spațiului informațional în condițiile globalizării și liberei circulații a informațiilor, în

RM a fost adoptată Strategia de securitate informațională pentru anii 2019-2024 [5] . Strategia prezintă o evaluare a situației actuale în domeniul securității informaționale, enumeră performanțele înregistrate și punctează noi tendințe de dezvoltare a societăţii informaţionale, or aceste obiective constituie o preocupare majoră a Serviciul Tehnologia Informațieișisi Securitate Cibernetică [9] .

Un aspect important al securității este reprezentat de protecția datelor cu caracter personal,în acest sens cadrul normativ este reglementat de LEGEA Nr. 133 din 08-07-2011 privind protecţia datelor cu caracter personal [6] ,dar și de un set de legi ce vin să sporească și să asigure obligațiile de răspundere, precum:

- Constituţia Republicii Moldova (1994);
- LEGEA Nr. 618 din 31-10-1995 securităţii statului;
- LEGEA Nr. 120 din 21-09-2017 cu privire la prevenirea şi combaterea terorismului;
- LEGEA Nr. 241 din 15-11-2007 comunicaţiilor electronice;
- LEGEA Nr.299 din 21-12-2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova;
- LEGEA cu privire la Concepţia Sistemului informaţional automatizat de stat “Alegeri”;
- LEGEA Nr. 239/2008 privind transparenţa în procesul decizional;
- LEGEA Nr. 982/2000 privind accesul la informaţie;
- Concepţia Securităţii Naţionale (2008).

Observăm,că sub aspectul legislației naționale in vigoare a Republicii Moldova, există o serie de acte juridice care ne permit să conturăm o imagine cu privire la politica de securitate naţională, inclusiv interesele naţionale, ameninţările, riscurile, obiectivele, mecanismele de implementare, instituţiile şi mandatele acestora în domeniul dat.

Este de subliniat faptul că la nivel european au fost întreprinse demersuri pentru a adopta noi politici privind lupta împotriva criminalității informatice și asigurarea securității cibernetice. *Directiva NIS privindsecuritatea rețelelor și a sistemelor informatice1*, adoptată de Parlamentul European și Consiliul Uniunii Europene la data de 6 iulie 2016, a intrat în vigoare în luna august a aceluiași an șibeneficiază de o perioadă de 21 de luni pentru a fi implementată de statele membre. Scopul Directivei NIS este de a asigura un nivel comun de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană și cere operatorilor, respectiv furnizorilor de servicii digitale, să adopte măsuri adecvate pentru prevenirea atacurilor cibernetice și managementul riscului, și să raporteze incidentele grave de securitate către autoritățile naționale competente [8] .

Un aspect important al securității UE este reprezentat de protecția datelor cu caracter personal. În acest sens, Parlamentul European și Consiliul au adoptat în data de 27 aprilie 2016 Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera

circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor - RGPD). Regulamentul (UE) 2016/679 a intrat în vigoare pe 25 mai 2016, iar prevederile lui vor fi aplicabile în toate statele membre UE, având caracter obligatoriu începând cu data de 25 mai 2018.

Conform datelor Agenției europene pentru securitate cibernetică (Enisa) amenințările la adresa securității cibernetice în Uniunea Europeană afectează sectoare vitale pentru societate. Primele șase sectoare cele mai afectate între iunie 2021 și iunie 2022, conform Agenției europene pentru securitate cibernetică (Enisa), au fost:

1. administrația publică și guvernele (24% dintre incidentele raportate)
2. furnizorii de servicii digitale (13%)
3. publicul larg (12,4%)
4. sectorul serviciilor (11,8%)
5. sectorul financiar/bancar (8,6%)
6. sectorul sănătății (7,2%)

În scopul creării unui cadru legal, stabil şi predictibil care să răspundă provocărilor contemporane de securitate, în octombrie 2020, liderii UE au solicitat consolidarea capacității UE de a:

- se proteja împotriva amenințărilor cibernetice
- asigura un mediu de comunicare securizat
- asigura accesul la date în scopuri judiciare și de asigurare a respectării legii [7].

Ca urmare, de către Comisia Europeană, în anul 2020 au fost întreprinse un șir de măsuri menite în vederea elaborării unei noi strategii de securitate cibernetică a UE. Scopul acestei strategii este de a consolida reziliența Europei la amenințările cibernetice și de a asigura faptul că toți cetățenii și toate întreprinderile pot beneficia pe deplin de servicii și instrumente digitale fiabile și de încredere. Noua strategie conține propuneri concrete de punere în aplicare a unor instrumente de reglementare, de investiții și de politică.

Concluzii

Concluzionând, provocările de securitate în era digitală, sunt, prin esența lor, interdependente cu procesul de democratizare a Republicii Moldova, necesitând o abordare contemporană, ori, tehnologiile implementate și utilizate la scară largă în RM în procesul de democratizare și modernizare, aduc incontestabil oportunități pentru promovarea unei democrații pluraliste și a drepturilor omului, concomitent însă, aplicarea acestora poate genera noi provocări, riscuri și amenințări, în domeni-cheie precum cel social, politic, economic, medical, ecologic sau cultural.

Criza pandemică COVID-19 a accentuat importanța tehnologiilor informaționale în domeniul educațional, al sănătății publice și a protecției sociale,

dar a și scos în evidență riscurile și amenințările ce survin drept urmare a utilizării tehnologiilor și încălcarea drepturilor omului, lacunele din legislația națională și necesitatea alinierii acestora la legislația internațională, consolidarea standardelor, inclusiv ,dezvoltarea și creșterea gradului de conștientizare a cetățenilor.

Sporirea rolului statului, dar și a organizațiilor societății civile, este esențial în dezvoltarea politicilor și prevederilor legale în scopul dezvoltării și utilizării cu succes a noilor tehnologii, inclusiv în scopul protejări drepturilor fundamentale și axarea acestora pe respectarea drepturilor omului offline și online, cu atenuarea riscurilor și deficiențelor ce survin din acestea.

În procesul de modernizare și democratizare, problemele din sectorul de sănătate, educație, mediu, incluziune, migrație, combatere a sărăciei devin prioritare pentru pacea și securitatea statului, conturând un set de provocări ale securității în era digitală, abordând mai vast conceptul de securitate, fapt ce necesită identificarea unor soluții inovatoare, sustenabile și eficiente.

Progresul și implementarea tehnologiilor informaționale determină diversificarea și creșterea complexității riscurilor și amenințărilor de securitate, precum dezinformarea, atacurile cibernetice, răspândirea de știri false, generând noi provocări de securitate, impunându-se în acest sens, o elaborare și gestionare corectă a riscurilor, a amenințărilor și vulnerabilităților de către autorități.

Referințe bibliografice:

1. Consiluil Uniunii Europene. Securitatea cibernetică: în ce fel combate UE amenințările cibernetice. [citat: 02.10.2022] . Disponibil: https://www.consilium.europa.eu/ro/policies/cybersecurity/
2. Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, Jurnalul Oficial al Uniunii Europene, 19 iulie 2016.
3. Duţu P., Bogzeanu C. *Provocări actuale pentru securitatea europeană.* Bucureşti:Editura Universităţii Naţionale de Apărare „Carol I”, 2010 .ISBN 978-973-663-835-0
4. Ferrara, E., Varol, O., Davis, C., Menczer, F., Flammini, A. (2016). *The Rise of Social Bots*. Communications of the ACM – Vol. 59 No. 7.
5. Hotărâre Nr. 257 din 22-11-2018 privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și a Planului de acțiuni pentru implementarea acesteia.[citat 03.10.2022]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=111979&lan
6. LEGE Nr. 133 din 08-07-2011 privind protecţia datelor cu caracter personal. .[citat 03.10.2022]. Disponibil:https://www.legis.md/cautare/getResults?doc_id=108552&lang=ro

7. ParlamentulEuropean. [citat: 02.10.2022].Disponibil:https://www.enisa.europa.eu/topics/cyber-threats
8. Parlamentul European. [citat: 02.10.2022]. Disponibil::https://www.europarl.europa.eu/news/ro/headlines/society/20220120STO21428/securitate-cibernetica-principalele-amenintari
9. Serviciul Tehnologia Informației și Securitate Cibernetică.[citat 04.10.2022]. Disponibil: https://stisc.gov.md/ro/strategia-securitatii-informationale-republicii-moldova-2019-2024