CZU: 004.056(478)

VULNERABILITĂȚI ALE CANALELOR DE COMUNICARE ONLINE ÎN REPUBLICA MOLDOVA ȘI CAPACITATEA LIMITATĂ DE REGLEMENTARE

Oleg CASIADI,
doctor în filosofie, conferențiar universitar,
Catedra „Management și comunicare profesională"
a Academiei „Ștefan cel Mare" a MAI

Mihai SOLTAN,
masterand,
Academia „Ștefan cel Mare" a MAI

Rezumat

Presa scrisă și-a descoperit demult declinul în regiunea noastră, iar cea televizată pierde din audiențe în favoarea online-ului. Despre acest lucru știm cu toții, însă puțini dintre noi deschid parantezele referitor la ce este o redacție, un cod deontologic sau preluarea textelor (chiar și cu formații neverificate) din goana după audiență. Canalele de informare online au cunoscut o varietate de forme, care au dus și la o varietate de modalități de comunicare. Până a vorbi despre comunicare codificată, provocarea amenințătoare și evidentă vine din administrarea surselor media, sau a punctelor de propagare a informațiilor. Posibilitatea de a publica texte de către orice deținător de o tastatură conectată la internet îngreunează modul de control și protecție a celorlalți utilizatori. În același timp, protecția de informații false și instigatoare la ură trebuie aplicată într-un mod care să nu fie asociat sau confundat cu cenzura. Dificultatea apare îndeosebi atunci când măsura punitivă poate fi aplicată doar după împlinirea faptului, când informația propagată deja a ajuns la suficienți destinatari. În astfel de circumstanțe, ar fi necesare măsuri de prevenție, însă în cazul în care ne referim la platforme de distribuție precum rețelele de socializare, prevenția ar putea fi sub forma limitării răspândirii anumitor informații.

Cuvinte-cheie: platforme online, știri false, atacuri cibernetice, instituții de reglementare, dreptul la exprimare.

Summary

Print media has long experienced a decline in our region, while televised media is losing audiences to online platforms. We are all aware of this, but few of us open parentheses regarding what constitutes an editorial office, a code of ethics, or the adoption of unverified texts in the pursuit of audience numbers.

Online information channels have taken various forms, leading to a variety of communication methods. Before discussing coded communication, the threatening and evident challenge comes from managing media sources or information dissemination points. The ability for anyone with a keyboard connected to the internet to publish texts complicates the control and protection of other users. At the same time, protecting against false and hate-inciting information must be applied in a manner that is not associated or confused with censorship. Difficulty arises especially when punitive measures can only be applied after the fact, when the propagated information has already reached a sufficient number of recipients. In such circumstances, preventive measures would be necessary, but when referring to distribution platforms such as social networks, prevention could take the form of limiting the spread of certain information.

Keywords: Online platforms, cyber-attacks, fake-news, regulatory institutions, right of speech.

Introducere. Vulnerabilitățile din mediul online pot fi de diferite tipuri și de diferită amploare, iar în cazul Republicii Moldova ne putem referi la știri false, incitări la ură, furt de date și identitate, până la atacuri cibernetice ce ar crea perturbări în activitatea unui dispozitiv, serviciu sau unei instituții [1, p. 247]. Atacurile din acest spectru sunt mai dificil de observat datorită caracterului imaterial și a emițătorului care nu va ține mereu să-și dezvăluie identitatea atât timp cât își poate satisface interesele. Pentru a proteja potențialele victime, este necesar să le identificăm caracteristicile specifice care le fac să fie ținte, iar în cele din urmă să înlăturăm din vulnerabilități.

Propaganda Kremlinului este un fenomen despre care am auzit vorbindu-se tot mai des în ultimul deceniu, de la anexarea Crimeii până la Brexit și războiul din Ucraina început în 2022. Înainte de a ne aprofunda pe acest aspect, trebuie să amintim că și în mod normal presa ar putea fi de o orientare pro-europeană sau pro-rusă, acest lucru manifestându-se prin prioritatea subiectelor abordate, dar și modul de expunere a acestora. La aceasta se adăugă scopul intrinsec al publicațiilor de a avea o acoperire cât mai largă a audienței.

Elementul de *fake-news* este unul tot mai instrumentalizat de către autorii de știri și postări online. În presa ordinară, cum ar fi ziare, radio sau tv, avem la bază o redacție înregistrată și sub evidența la cel puțin a unei autorități cu caracter regulator, în cazul Republicii Moldova fiind Consiliul Audiovizualului. Această autoritate este în drept să ofere și să suspende autorizații de activitate/difuzare, furnizorii de servicii media audiovizuale având rezidență juridică și pe teritoriul țării. În acest mod putem vorbi despre o urmărire exactă a sursei unui mesaj emis de unul dintre cei peste 100 de

furnizori înregistrați la CA, și aplicarea măsurii punitive care poate include suspendarea autorizațiilor de difuzare. În această ordine de idei, editorii cu o rezidență juridică validă, vor modela *fake-news*-ul prin utilizarea informațiilor scoase din context, urmate de analiza sau concluziile redactorului, care pot fi părtinitoare și respectiv capabile să ofere consumatorului o perspectivă aparent deosebită, însă cu o tentă conspiraționistă.

În mediul online avem la bază platforme de distribuție/rețele de socializare, care nu au neapărat o rezidență juridică pe teritoriul țării noastre, și în acest caz pentru a păstra dreptul la libera exprimare a indivizilor care distribuie informații ce ar atenta la integritatea și securitatea ordinii publice, ca primă resursă nu ne rămâne decât să ne bazăm pe funcționarea algoritmilor de raportare și blocare a postărilor de către platforma gazdă.

După avalanșa știrilor false din pandemie, dar și odată cu începerea războiului din Ucraina, consumatorii de conținut online din Republica Moldova au devenit tot mai vulnerabili în fața acestui tip de conținut. Utilizatorii platformelor online cu drept de publicare nu sunt neapărat indivizi. În aceste cazuri, în spatele mesajului publicat poate fi un robot sau program automatizat de generare și publicare a mesajelor în conformitate cu instrucțiunile și cuvintele-cheie setate. Complexitatea acestora constă în capacitatea de a analiza modele de publicări media existente și de a reproduce formulări, limbaj și stil de scriere, cu toate acestea orientându-și resursele în raportul 10% pentru testare și 90% pentru învăța [2, p. 5-7].

În acest ritm, putem vorbi despre o amenințare în continuă creștere, care trebuie contracarată cu instrumente abile, fără a viola dreptul la libera exprimare a indivizilor. De subliniat este și faptul că orice acțiune de limitare a propagării mesajului unui individ ar putea fi identificată și ca o îngrădire a dreptului său la libera exprimare. Instrumentele online folosesc la bază algoritmi de o complexitate înaltă, iar modul în care aceștia influențează vizibilitatea unui mesaj ori a unei postări poate fi de asemenea suspectat de părtinire în unele cazuri.

Ca mecanism de reglare pentru securitatea online a cetățenilor, serviciile de securitate ar putea implementa și monitoriza modul de detecție cu ajutorul instrumentelor de tip *machine learning* [3, p. 2-4], însă acest lucru necesită o analiză continuă a evoluției comportamentului atacatorului, precum și a capacităților acestuia. Intervențiile în cazurile în care nu poate fi identificat individul din spatele profilului de utilizator, necesită a fi făcute într-un mod cu precizie de ordin chirurgical.

Există și profiluri de utilizatori gestionate de indivizi cu experiență în păstrarea anonimatului în mediului online, care prestează servicii de publicare și activitate online la comanda altor indivizi interesați. În aceste cazuri,

este la fel de dificil de urmărit sursa și de a aplica măsuri punitive, îndeosebi în cazul în care individul se află peste hotare, cu cetățenia altui stat, iar țara sa nu ține neapărat cont de acel tip de infracțiune. Reglementările eficiente și severe ar trebui să se bazeze pe urmărirea algoritmilor, precum și pe identificarea postărilor și a surselor problematice. Astfel vom putea să reducem din impactul accidental asupra indivizilor nevinovați care de fapt au fost victime ale atacatorilor. În astfel de acțiuni, entuziasmul nu ar trebui să depășească profesionalismul, pentru a nu avea parte de accidente cibernetice precum s-a întâmplat în Rusia la tentativele organelor speciale de a bloca activitatea platformei de mesagerie Telegram, care a dus la blocarea accidentală a mai multor pagini web, a generat pierderi unor companii, iar ținta funcționa în continuare.

În lumina vulnerabilităților socio-economice din Republica Moldova, este important să se recunoască existența unor viziuni divergente și chiar opuse în cadrul societății, ceea ce adâncește provocările pe care autoritățile de la Chișinău le întâmpină în procesul de construire a unei reziliențe socio-economice sustenabile. Aceste discrepanțe pot fi observate în mod special în contextul alegerilor electorale, unde diversitatea de opinii și interese complexifică eforturile de consolidare a unui sistem coerent și eficient, capabil să răspundă nevoilor și aspirațiilor atât la nivel individual, cât și societal.

Vulnerabilitățile socio-economice în R. Moldova sunt alimentate de disfuncționalități structurale și instituționale, care provoacă fracturi în societate și slăbesc capacitatea de adaptare și rezistență a țării la schimbările și șocurile economice. Aceste fracturi sunt înrădăcinate în discrepanțele de viziune și interese ale diferitelor grupuri sociale, care adesea percep politicile și acțiunile autorităților în mod diferit și manifestă opoziție și rezistență față de inițiativele propuse.

Războiul din Ucraina a avut un impact semnificativ asupra mai multor domenii, provocând atrofieri și disfuncționalități în diverse domenii, cum ar fi lanțurile de aprovizionare logistică și importurile de produse specifice din Ucraina sau tranzitate prin teritoriul acesteia [4. p. 210]. După declanșarea războiului, au avut loc creșteri semnificative de prețuri la produsele de primă necesitate și la resursele energetice, generând dezbateri privind cauzele și vinovații pentru aceste scumpiri. Canalele media, inclusiv cele propagate de Rusia, au jucat un rol important în modelarea percepției publice, în timp ce Consiliul Audiovizualului din Chișinău a intervenit pentru a controla și reglementa aceste canale. De asemenea, unii funcționari publici din Chișinău au evitat să facă declarații publice privind poziția lor față de războiul de agresiune din Ucraina, generând incertitudini și opinii divergente în rândul populației [5, p. 317].

Unul dintre aspectele care generează îngrijorare în Republica Moldova este nivelul de educație al populației din mediul rural și conținutul pe care îl consumă. Este important să recunoaștem că persoanele în vârstă pot avea preconcepții și viziuni despre viață și lume bazate pe experiențele lor anterioare, chiar dacă acestea pot fi eronate. Comunicarea cu aceste persoane, prin argumente bine fundamentate, este un proces de lungă durată, deoarece viziunile lor sunt adesea construite pe baza mesajelor false și dezinformării. Aceste persoane pot influența în mod semnificativ membrii familiilor și apropiații lor. Prin urmare, accentul pe incluziunea socială devine crucial, deoarece grupurile izolate sunt mai predispuse să caute și să accepte informații alternative, inclusiv teorii ale conspirației sau știri din surse dubioase.

Dezinformarea în rândul maselor de cetățeni, combinată cu sărăcia cu care se confruntă, îi face pe aceștia să accepte mai ușor anumite oferte sau propuneri politice, atâta timp cât li se furnizează argumente plauzibile, chiar dacă acestea sunt scoase din context și legate de o promisiune logică care pare să ofere un beneficiu. Protestele din toamna și iarna anului 2022-2023, organizate de politicienii de opoziție, au reușit să mobilizeze această categorie socială menționată anterior. Aceste persoane au în mare parte viziuni construite pe baza experiențelor recente și nu sunt neapărat pro-europene sau pro-estice. Cu toate acestea, cel care reușește să ajungă primul la indivizi cu argumente convingătoare și să le ofere o perspectivă cu care aceștia se pot identifica, devine câștigător și aduce de partea sa noi simpatizanți. Dacă se vor adăuga și stimulentele materiale, există șansa de a câștiga încrederea acestor cetățeni cu drept de vot, însă cu prețul de a le pierde complet responsabilitatea civică [6, p. 154].

Și infrastructura critică a Republicii Moldova rămâne expusă și vulnerabilă în fața acțiunilor malițioase, reprezentând un aspect deosebit de preocupant pentru securitatea națională și stabilitatea socio-economică a țării. Infrastructura critică cuprinde sectoare esențiale precum energie, transport, comunicații, apă și alimente, sănătate și altele, care sunt fundamentale pentru funcționarea normală a societății și economiei. Unul dintre principalele motive ale vulnerabilității infrastructurii critice este dependența excesivă de tehnologii și sisteme informatice interconectate. Această interconectivitate creează un teren propice pentru acțiuni malițioase, cum ar fi atacurile cibernetice sau infiltrarea și manipularea sistemelor informatice. Astfel, sistemele de energie electrică, rețelele de comunicații sau sistemele de transport pot fi expuse riscului de întreruperi sau sabotaje, cu consecințe grave asupra activităților cotidiene și economiei în ansamblu [7, p. 2-3]. De asemenea, infrastructura critică este vulnerabilă la atacuri fizice sau teroriste. Clădirile, instalațiile și rețelele care susțin aceste sectoare cheie pot fi expuse riscului

de sabotaj, distrugere sau blocare, afectând astfel funcționarea lor normală și provocând daune semnificative.

Ca și subiect al vulnerabilității societale, prin implicare cibernetică cu impact asupra societății, ar putea fi sistemele de informații din sistemul medical (HIM) referitoare la istoricul pacienților sau managementul informațiilor de sănătate. Cu toate că pentru R. Moldova dosarele medicale electronice nu sunt extrem de răspândite, în conformitate cu tendințele existente ar fi recomandat să luăm măsurile cele mai protective care ar asigura un maxim de siguranță a datelor, păstrând un echilibru în comunicare și accesibilitate [8].

Încât vorbeam mai devreme despre necesitatea de a lua în calcul și riscurile din partea actorilor non-statali[1], în acest caz companii farmaceutice sau investitori în domeniul sănătății fără o bună etică de lucru, avem responsabilitatea de a proteja societatea și de acest tip de amenințare. În cazul Republicii Moldova, aceste informații de tip HIM ar prezenta mai degrabă un risc asupra societății în cazul în care se face uz de vulnerabilitatea economică a acesteia, decât riscul bioterorismului (care de asemenea nu trebuie exclus).

În *a concluziona*, vulnerabilitățile de ordin informațional sunt cele mai des utilizate de către actori interesați în a le testa și folosi. Acest lucru prezintă o amenințare asupra securității statului, dar și a elementelor sale. R. Moldova s-a arătat a fi un teren fertil în testarea și implementarea diferitelor moduri de comunicare și retorici propagandistice, care ar putea fi ulterior utilizate la o scară mai largă. Dacă vom recunoaște statutul de *element tranzitoriu* al Republicii Moldovei în fața propagandei de la Kremlin, am putea să-l prezentăm comunității europene și să solicităm măsuri eficiente de protecție comune. În final, tindem să credem că suntem departe pentru a prezenta ținta unor atacuri cibernetice din categoria războiului cognitiv și a sindromului Havana [9, p. 1-3].

Referințe bibliografice

1. Raiyn Jamal. 2014. *A survey of cyber attack detection strategies*. International Journal of Security and Its Applications 8 (1): 247-256.

2. Solopova Veronika, Popescu Oana-Iuliana, Benzmüller Christoph, Landgraf Tim. 2023. *Automated multilingual detection of Pro-Kremlin propaganda in newspapers and Telegram posts*. Datenbank-Spektrum. Vol. 23 (1), p. 5-14.

3. Ahmad Iftikhar, Muhammad Yousaf, Suhail Yousaf, Muhammad Ovais Ahmad. 2020. *Fake news detection using machine learning ensemble methods*. Complexity, 2020. p. 1-11.

[1] Atacul cibernetic de la spitalul Sf. Treime din Chișinău, din august 2023, nu a fost revendicat.

4. Uvalić Milica. 2023. *The uncertain impact of the Russian–Ukraine war on the Western Balkans*. A Year Later: War in Ukraine and Western Balkan (Geo) Politics. p. 210.

5. Albu Natalia, f.a. *National Security of the Republic of Moldova in the Context of Actual Risks and Threats*. Bucharest, 2014, p. 317.

6. Haigh Maria, Haigh Thomas, Matychak Tetiana. 2019. *Information literacy vs. fake news: the case of Ukraine*. Open Information Science 3 (1).p. 154-165.

7. Große Christine. 2023. *A review of the foundations of systems, infrastructure and governance*. Safety Science 160: 106060. 2023, p. 1-17.

8. Wiedemann L.A. (2010). Homeland Security Act, Patriot Act, Freedom of Information Act, and HIM (2010 update). Journal of AHIMA. Retrieved 4 30, 2023, from http://bok.ahima.org/doc?oid=106172. (accesat la 30.04.2023).

9. Hughes, Chase K.. *Havana Syndrome, Cognitive Warfare, and Psychogenic Symptoms of Neurotoxins*. 2022.