DOI: https://doi.org/10.53486/sstc2025.v1.79
CZU: 004.8:004.056.5:330(100)

ARTIFICIAL INTELLIGENCE AND SECURITY CHALLENGES IN THE DIGITAL ECONOMY

INTELIGENȚA ARTIFICIALĂ ȘI PROVOCĂRI DE SECURITATE ÎN ECONOMIA DIGITALĂ

ISAC Ariana, studentă, specialitatea: Relații internaționale și studii europene
Universitatea „Dunărea de Jos" din Galați, România,
e-mail author: ai425@student.ugal.ro

Abstract: *Artificial intelligence (AI) plays a key role in the digital economy, bringing both economic opportunities and security risks. The main threats identified include algorithmic vulnerabilities, automated cyberattacks, financial market manipulation and regulatory loopholes. AI algorithms can be exploited by adversarial attacks, and deep fakes and automated hacking represent emerging risks for sectors such as finance and cybersecurity. In addition, automated trading can destabilize markets, and insufficient regulation creates an environment conducive to the misuse of AI. To counter these challenges, it is necessary to develop strict regulatory policies, improve the resilience of algorithms and constantly monitor AI systems. Risk awareness and user education are also critical factors for a safer digital environment. One of the emerging security challenges in the digital economy is the expansion of the use of AI in cyberattacks. Thus, AI-based phishing systems can generate personalized messages, adapted to the target's behavior, which increases the likelihood of their effectiveness. AI is also used to develop advanced malware, capable of modifying its code to avoid detection by traditional security solutions. Another emerging security challenge in the digital economy is the exploitation of AI in disinformation and manipulation of public opinion. Thus, digital platforms use advanced algorithms to personalize the content displayed to users, but these algorithms can be exploited to spread false information on a large scale. AI-generated disinformation campaigns have been identified in electoral contexts, where deep fakes and automatically generated posts influenced voters' perceptions.*
Keywords: *Artificial intelligence, cybersecurity, adversarial attacks, deep fake, algorithms, regulation, digital economy, attack automation*

JEL CLASSIFICATION: O14

INTRODUCERE

Importanța cercetării inteligenței artificiale (IA) deține un rol semnificativ în provocările securității economiei digitale. Obiectivul major al lucrării rezidă în analiza inteligenței artificiale ca factor esențial în economia digitală ce influențează majoritatea sectoarelor, de la comerț electronic și finanțe la logistică și securitate cibernetică. Pe de o parte, IA permite automatizarea proceselor, optimizarea resurselor și generarea de noi oportunități economice. Pe de altă parte, evoluția sa rapidă creează riscuri considerabile în materie de securitate, precum atacuri cibernetice sofisticate, manipularea datelor și vulnerabilități ale algoritmilor. Acest articol analizează principalele provocări de securitate generate de IA în economia digitală și explorează soluții pentru mitigarea riscurilor.

CONȚINUTUL DE BAZĂ

Pentru a oferi o imagine clară asupra problemei, cercetarea se bazează pe mai multe surse relevante cum ar fi: portalul Consiliului Uniunii Europene (2023) oferă perspective asupra politicilor de securitate cibernetică și reglementărilor aplicabile în Uniunea Europeană. Studiul realizat de Stanford (2014) analizează impactul IA asupra economiei, subliniind cum algoritmii pot influența deciziile de piață. Lucrarea „Artificial Intelligence: A Modern Approach” de Stuart Russell și Peter Norvig reprezintă un ghid fundamental asupra metodelor IA. O altă lucrare cum ar fi „Idealizations of Uncertainty, and Lessons from Artificial Intelligence” explorează modul în care incertitudinea este gestionată în sistemele IA, cu implicații asupra securității. Pentru realizarea acestui studiu s-au

utilizat mai multe metode: analiza documentară - examinarea literaturii pentru identificarea riscurilor IA; studiu comparativ - compararea strategiilor de securitate utilizate de companii; metoda inductivă - derivarea concluziilor din studii de caz despre atacuri cibernetice asistate de IA.

În urma realizării acestei cercetări am identificat mai multe provocări critice legate de utilizarea IA în economia digitală. Una din acestea ține de vulnerabilitățile algoritmilor.

Algoritmii IA sunt expuși atacurilor adversariale, prin care datele de intrare sunt manipulate pentru a provoca erori în sistemele automate. Un exemplu concret este cel al vehiculelor autonome, care pot fi induse în eroare prin modificarea semnelor rutiere. Tesla a raportat cazuri în care autovehiculele au interpretat greșit indicatoarele, ceea ce ar putea duce la accidente grave. Totodată, sistemele de recunoaștere facială utilizate în sectorul financiar pot fi păcălite de deepfake-uri, ceea ce ridică probleme de securitate în ceea ce privește autentificarea și accesul la servicii bancare.

O altă provocare legată de utilizarea IA în economia digitală este legată de automatizarea atacurilor cibernetice. IA este utilizată atât pentru protecția cibernetică, cât și pentru atacuri sofisticate. Hackeri avansați folosesc tehnologia pentru a crea atacuri personalizate, precum campanii de phishing generate automat sau viruși informatici ce se adaptează în timp real la măsurile de securitate implementate. Un exemplu relevant este utilizarea IA pentru spargerea parolelor. Prin tehnici de învățare automată, sistemele pot analiza modele și prezice parole probabile, reducând timpul necesar pentru compromiterea conturilor. De asemenea, deepfake-urile au fost utilizate pentru fraudă bancară, atacatorii reușind să creeze apeluri video false cu identități fabricate pentru a induce în eroare reprezentanți ai băncilor.

O altă provocare legată de utilizarea IA în economia digital este caracterizată de manipularea piețelor financiare. Algoritmii de tranzacționare automată sunt susceptibili la manipulări. Un caz celebru este cel al „flash crash”-ului din 2010, când un algoritm a declanșat o cădere bruscă a pieței bursiere. În plus, există temeri că IA ar putea fi folosită pentru a influența prețurile acțiunilor prin tranzacții rapide, generând instabilitate economică. O altă provocare este legată de sistemele de credit scoring. Algoritmii care analizează bonitatea clienților pot fi păcăliți prin generarea de date false, ceea ce ar putea duce la acordarea de credite unor persoane neeligibile.

Pentru a contracara aceste probleme ne-am ciocnit cu dilema lacunelor legislative care, la rândul lor, constituie un obstacol în calea utilizării fără impedimente a IA în economia digitală.

Reglementările privind IA și securitatea cibernetică sunt încă insuficient dezvoltate pentru a acoperi toate riscurile. Uniunea Europeană a propus documentul „AI Act”, un cadru de reglementare menit să stabilească standarde stricte pentru dezvoltarea și utilizarea IA, dar aplicabilitatea acestuia rămâne limitată în context global. În SUA și China, reglementările sunt mai flexibile, ceea ce poate duce la o competiție inegală pe piața globală și la exploatarea unor breșe legislative pentru utilizarea IA în scopuri malițioase. Pentru a diminua riscurile asociate IA în economia digitală, este esențială implementarea unor măsuri pro active, inclusiv:

1. Elaborarea unor politici stricte de reglementare – guvernele trebuie să colaboreze pentru a crea standarde internaționale pentru utilizarea IA, astfel încât să fie prevenite utilizările neetice și atacurile cibernetice.
2. Dezvoltarea unor algoritmi rezilienți – cercetătorii și companiile din domeniu trebuie să creeze sisteme mai sigure, capabile să detecteze atacurile adversariale și să răspundă la amenințările emergente.
3. Monitorizarea constantă a sistemelor IA – audituri de securitate și revizuiri regulate ale algoritmilor utilizați pot preveni exploatarea acestora.
4. Colaborarea internațională – Partajarea informațiilor despre atacuri și amenințări între state și corporații poate contribui la crearea unei apărări mai solide împotriva utilizării abuzive a IA.
5. Educație și conștientizare – utilizatorii trebuie informați despre riscurile IA și despre metodele de protecție împotriva atacurilor cibernetice bazate pe inteligență artificială.

CONCLUZII ȘI RECOMANDĂRI

IA aduce numeroase beneficii economiei digitale dar și provocări semnificative de securitate. O abordare echilibrată, bazată pe inovație responsabilă și măsuri de protecție eficiente, este esențială pentru a preveni amenințările emergente și a asigura un mediu digital sigur.

REFERINȚE:

1. Einav L., & Levin J. (2014). *Economics in the age of big data*. https://web.stanford.edu/~leinav/pubs/Science2014.pdf
2. Kyburg H. E. Jr. (1996). *Idealizations of Uncertainty, and Lessons from Artificial Intelligence*.
3. Portalul Consiliului Uniunii Europene.(2025). https://www.consilium.europa.eu/ro/policies/cybersecurity/
4. Russell S., & Norvig P. (2009). *Artificial Intelligence: A Modern Approach*. Pearson.

Coordonator ştiinţific: CORLOTEANU Silvia, dr. hab., prof. univ.,
Universitatea „Dunărea de Jos” din Galați, Facultatea Transfrontalieră,
Strada Domnească nr. 111, corp K, Campus Științei, Galaţi, România.
Tel: +373 78922462
e-mail: silvia.corloteanu@ugal.ro