DOI: https://doi.org/10.53486/sstc2026.v1.109

CZU: 004.8+004.056.53

ARTIFICIAL INTELLIGENCE AND SECURITY CHALLENGES IN THE DIGITAL ECONOMY

INTELIGENȚA ARTIFICIALĂ ȘI PROVOCĂRI DE SECURITATE ÎN ECONOMIA DIGITALĂ

VRABIE Dragoș, student, specialitatea: Tehnologii informaționale
Academia de Studii Economice din Moldova, MD-2005,
Chișinău, str. Bănulescu-Bodoni 61
Telefon: + 373 684 72 787
e-mail: vrabir.dragos@ase.md

Abstract. *The present study examines the dual role of artificial intelligence (AI) as both a catalyst for innovation and a source of emerging security threats in the digital economy. The research is grounded in the growing tension between the rapid adoption of AI technologies by economic actors and the evolving sophistication of AI-enabled cyberattacks. The methodology combines a systematic analysis of secondary data from institutional reports (IBM, World Economic Forum, Deloitte) with a comparative assessment of regulatory frameworks, notably the EU AI Act (Regulation 2024/1689). The findings indicate that the global average cost of a data breach reached USD 4.88 million in 2024, while organizations deploying AI-based security solutions reduced these costs by an average of USD 2.2 million. Nearly 47% of organizations identify generative AI-powered adversarial advances as their primary security concern, and the cybersecurity workforce deficit has widened by 8% since 2024. The study concludes that effective integration of AI in cybersecurity strategies, combined with coherent regulatory compliance, represents a necessary condition for sustainable digital economic growth.*
Key words: *artificial intelligence, cybersecurity, digital economy, data breach, EU AI Act, deepfake, phishing, cyber resilience*
JEL CLASSIFICATION: L86, O33, K24, G28

INTRODUCERE

Economia digitală contemporană se dezvoltă într-un ritm fără precedent, iar inteligența artificială (IA) a devenit unul dintre principalii factori care transformă modelele de afaceri, procesele organizaționale și interacțiunile economice la nivel global. Conform Raportului Global Cybersecurity Outlook 2025 al Forumului Economic Mondial (WEF), elaborat în colaborare cu Accenture, complexitatea peisajului cibernetic s-a intensificat semnificativ, fiind determinată de tensiunile geopolitice, de interdependențele din lanțurile de aprovizionare, de adoptarea rapidă a tehnologiilor emergente și de sofisticarea infracțiunilor cibernetice (WEF, 2025).

Contextul actual relevă o tensiune structurală: pe de o parte, IA oferă instrumente avansate de detecție și răspuns la amenințări, reducând costurile breșelor de securitate; pe de altă parte, aceleași tehnologii sunt exploatate de actori rău intenționați pentru a lansa atacuri mai precise, mai rapide și mai greu de detectat. Raportul IBM Cost of a Data Breach 2024, realizat de Ponemon Institute, a constatat că piața globală a securității cibernetice bazate pe IA a fost evaluată la aproximativ 25,35 miliarde USD în 2024, cu proiecții de creștere până la 93,75 miliarde USD până în 2030, la o rată compusă anuală de creștere (CAGR) de 24,4% (Grand View Research, 2024).

Obiectivul prezentei lucrări este de a analiza rolul dual al inteligenței artificiale în economia digitală – ca instrument de apărare cibernetică și ca vector de amenințare – și de a evalua cadrul de reglementare emergent, în special Regulamentul UE privind Inteligența Artificială (AI Act, Regulamentul (UE) 2024/1689). Cercetarea urmărește să identifice tendințele actuale în materie de costuri ale breșelor de date, eficiența instrumentelor de securitate bazate pe IA și provocările generate de deficitul de forță de muncă specializată.

CONȚINUTUL DE BAZĂ

Analiza surselor bibliografice

Problematica securității cibernetice în contextul economiei digitale a generat o literatură substanțială în ultimul deceniu. Darktrace (2024) subliniază că veniturile anuale din criminalitatea cibernetică depășesc deja 8 trilioane USD, ceea ce ar face din cybercrime a treia economie mondială, după SUA și China. Această estimare este coroborată de datele Mastercard (2025), conform cărora pierderile și daunele provocate de atacurile cibernetice au atins 9,5 trilioane USD în 2024.

Raportul WEF Global Cybersecurity Outlook 2025 identifică o serie de factori care amplifică complexitatea peisajului cibernetic: tensiunile geopolitice (care influențează strategia de securitate cibernetică a aproximativ 60% dintre organizații), interdependențele lanțurilor de aprovizionare (54% dintre organizațiile mari le consideră principala barieră în calea rezilienței cibernetice) și adoptarea rapidă a tehnologiilor emergente fără evaluarea adecvată a riscurilor de securitate (WEF, 2025).

IBM, prin raportul său anual Cost of a Data Breach (2024), oferă o bază empirică esențială. Studiul, realizat de Ponemon Institute pe un eșantion de 604 organizații din 17 industrii și 16 țări, a constatat că costul mediu global al unei breșe de date a atins 4,88 milioane USD – o creștere de aproximativ 10% față de anul anterior și cel mai mare salt de la pandemia COVID-19 (IBM, 2024). În sectorul financiar, costurile sunt și mai ridicate, ajungând la 6,08 milioane USD per incident, cu 22% peste media globală (IBM, 2024).

Deloitte (2025), prin raportul Global Cyber Threat Intelligence, confirmă că inteligența artificială generativă reprezintă o provocare nouă pentru organizații, amplificând amenințările existente. Lakera (2025) semnalează un paradox relevant: 93% dintre profesioniștii în securitate consideră că IA poate îmbunătăți securitatea cibernetică, dar în același timp 77% dintre organizații se consideră nepregătite să se apere împotriva amenințărilor bazate pe IA.

Metodologia cercetării

Prezenta lucrare adoptă o abordare metodologică bazată pe analiza sistematică a datelor secundare și pe sinteza comparativă a surselor instituționale. Principalele surse de date includ: raportul IBM Cost of a Data Breach 2024 (bazat pe interviuri cu 3.556 de lideri din domeniile securității și managementului), raportul WEF Global Cybersecurity Outlook 2025 (realizat în colaborare cu Accenture), rapoartele Deloitte Global Cyber Threat Intelligence 2025, datele de piață furnizate de Grand View Research (2024) și Statista (2024), precum și cadrul legislativ european (Regulamentul (UE) 2024/1689 – AI Act).

Metoda de cercetare combină analiza cantitativă a indicatorilor de cost și frecvență a breșelor de securitate cu analiza calitativă a cadrelor de reglementare și a strategiilor organizaționale de răspuns. Datele au fost verificate prin triangularea surselor, utilizând cel puțin două surse independente pentru fiecare indicator major.

Rezultatele obținute

1. Costurile breșelor de date și impactul IA. Conform raportului IBM (2024), costul mediu global al unei breșe de date a crescut la 4,88 milioane USD, marcând o creștere de 10% față de anul precedent. Aproximativ 70% dintre organizațiile studiate au raportat perturbări operaționale semnificative sau moderate ca urmare a breșelor. Costurile combinate ale activităților post-breșă – incluzând suportul pentru clienți, amenzile de reglementare și remedierea – au totalizat 2,8 milioane USD, cea mai ridicată valoare din ultimii șase ani (IBM, 2024).

Cea mai semnificativă constatare privește impactul utilizării IA și automatizării în prevenirea breșelor. Organizațiile care au implementat extensiv soluții bazate pe IA în fluxurile de prevenire au înregistrat costuri medii ale breșelor cu 2,2 milioane USD mai mici decât cele care nu au utilizat astfel de tehnologii: 3,76 milioane USD față de 5,98 milioane USD, o diferență de 45,6% (IBM, 2024). De asemenea, aceste organizații au identificat și au remediat breșele în medie cu 98 de zile mai rapid, iar ciclul de viață mediu al unei breșe a scăzut la 258 de zile – cel mai redus nivel din ultimii 7 ani (IBM, 2024).

Tabelul 1 prezintă o sinteză comparativă a costurilor medii ale breșelor de date în funcție de nivelul de utilizare a IA și automatizării.

Tabelul 1. Costul mediu al breșelor de date în funcție de utilizarea IA (2024)

Nivel de utilizare IA	Cost mediu breșă (mil. USD)	Timp detecție (zile)	Economii (mil. USD)
Fără IA/automatizare	5,72	~356	–
Utilizare limitată	4,88	~280	0,84
Utilizare extensivă	3,84	~258	1,88
Extensivă (prevenție)	3,76	~258	2,22

Sursa: elaborat de autor pe baza IBM Cost of a Data Breach Report 2024

2. Amenințările cibernetice bazate pe IA. Conform WEF (2025), 72% dintre respondenți raportează o creștere a riscurilor cibernetice organizaționale, iar aproape 47% dintre organizații citează progresele adversariale alimentate de IA generativă drept principala lor preocupare. Atacurile de tip phishing potențate de IA au înregistrat o creștere de 1.265% în perioada recentă, iar deepfake-urile au crescut cu 680% de la an la an, cu 179 de incidente separate numai în primul trimestru al anului 2025 (Darktrace, 2024; WEF, 2025).

Sondajul global realizat de Mastercard (2025) relevă că 76% dintre consumatori sunt mai preocupați de riscurile cibernetice decât în urmă cu doi ani, iar aproape trei sferturi consideră că IA va face imposibilă distincția între conținutul real și cel fals în mediul online. Doar 13% dintre respondenți s-au declarat foarte încrezători în capacitatea lor de a identifica amenințările generate de IA (Mastercard, 2025).

Un aspect relevant îl constituie și atacurile asupra sistemelor IA propriu-zise. Cele mai frecvente tipuri de atacuri cibernetice asupra instrumentelor IA includ: otrăvirea datelor de antrenament (data poisoning), atacurile de inferență, extracția modelelor și evaziunea algoritmică (Tech Advisors, 2025). Raportul IBM 2025 evidențiază că breșele generate de utilizarea neautorizată a IA (shadow AI) costă organizațiile cu 670.000 USD mai mult decât media, ajungând la 4,63 milioane USD per incident (IBM, 2025).

3. Cadrul de reglementare: EU AI Act. Regulamentul (UE) 2024/1689 privind Inteligența Artificială (AI Act), adoptat de Parlamentul European la 13 martie 2024 și de Consiliul UE la 21 mai 2024, constituie primul cadru legislativ cuprinzător dedicat inteligenței artificiale la nivel mondial. Regulamentul a intrat în vigoare la 1 august 2024 și urmează a fi pe deplin aplicabil la 2 august 2026, cu anumite excepții treptate (Parlamentul European, 2024).

AI Act adoptă o abordare bazată pe risc, clasificând sistemele IA în categorii: risc inacceptabil (practici interzise, aplicabile din 2 februarie 2025), risc ridicat (sisteme IA utilizate în produse reglementate, cu obligații aplicabile din august 2026–2027), risc limitat (obligații de transparență) și risc minim. Amenzile pentru încălcări pot ajunge până la 35 de milioane de euro sau 7% din cifra de afaceri globală, în funcție de tipul și gravitatea încălcării (Parlamentul European, 2024).

În noiembrie 2025, Comisia Europeană a propus pachetul Digital Omnibus on AI, menit să simplifice implementarea AI Act, să extindă sandbox-urile de reglementare și să reducă sarcinile administrative, în special pentru IMM-uri (Consiliul UE, 2026). Această evoluție legislativă indică recunoașterea faptului că reglementarea trebuie să echilibreze protecția drepturilor fundamentale cu stimularea inovației.

4. Deficitul de competențe și asimetria în securitatea cibernetică. WEF (2025) raportează că deficitul de competențe în securitate cibernetică a crescut cu 8% între 2024 și 2025, iar două din trei organizații semnalează deficiențe moderate sau critice în materie de talent specializat. Doar 14% dintre organizații declară că dispun de personalul necesar pentru a-și atinge obiectivele de securitate cibernetică. Sectorul public este cel mai afectat: 49% dintre organizațiile publice nu au forța de muncă necesară, o creștere de 33% față de 2024 (WEF, 2025).

Tabelul 2 sintetizează principalele provocări identificate de WEF în peisajul securității cibernetice în 2025.

Tabelul 2. Principalele provocări în securitatea cibernetică (2025)

Provocare identificată	**Pondere respondenți (%)**
Creșterea riscurilor cibernetice organizaționale	72%
Impactul IA asupra securității cibernetice	66%
Tensiuni geopolitice ca factor în strategia de securitate	~60%
Provocări ale lanțurilor de aprovizionare (org. mari)	54%
Amenințări adversariale bazate pe IA generativă	47%
Procese de evaluare a securității IA înainte de implementare	37%
Deficit de competențe specializate (organizații afectate)	~67%

Sursa: elaborat de autor pe baza WEF Global Cybersecurity Outlook 2025

Această asimetrie în reziliență se reflectă și la nivel regional. În Europa și America de Nord, doar 15% dintre organizații nu au încredere în capacitatea țării lor de a răspunde la incidente cibernetice majore vizând infrastructura critică. În Africa și America Latină, aceste cifre cresc la 36%, respectiv 42% (WEF, 2025). Inegalitatea cibernetică afectează disproporționat organizațiile mici, dintre care 35% declară că reziliența lor cibernetică este insuficientă – o creștere semnificativă față de 2022 (WEF, 2025).

CONCLUZII ȘI RECOMANDĂRI

Analiza efectuată evidențiază câteva concluzii esențiale pentru înțelegerea relației dintre inteligența artificială și securitatea cibernetică în economia digitală.

În primul rând, IA are un rol dual verificat empiric: organizațiile care implementează extensiv soluții de IA și automatizare în fluxurile de prevenire economisesc în medie 2,2 milioane USD per breșă și identifică incidentele cu 98 de zile mai rapid, conform IBM (2024). Această constatare susține argumentul că investiția în IA defensivă produce un randament pozitiv măsurabil.

În al doilea rând, amenințările cibernetice bazate pe IA generativă se amplifică într-un ritm care depășește capacitatea de adaptare a multor organizații. Creșterea de 1.265% a atacurilor de phishing alimentate de IA și proliferarea deepfake-urilor indică faptul că bariera tehnologică pentru lansarea atacurilor sofisticate s-a redus semnificativ.

În al treilea rând, cadrul de reglementare european, reprezentat de AI Act și completat de pachetul Digital Omnibus on AI, oferă un model bazat pe risc care, deși apreciat pentru coerență, necesită simplificare continuă pentru a nu inhiba inovația, în special în rândul IMM-urilor.

În al patrulea rând, deficitul de competențe în securitate cibernetică – cu doar 14% dintre organizații declarând că dispun de talentul necesar – rămâne una dintre cele mai acute vulnerabilități sistemice.

Pe baza acestor constatări, se pot formula următoarele recomandări: (1) integrarea sistematică a IA în toate cele patru domenii ale operațiunilor de securitate (prevenție, detecție, investigare, răspuns); (2) investiții prioritare în formarea și recrutarea specialiștilor în securitate cibernetică, cu accent pe parteneriate public-private; (3) implementarea proactivă a cadrului de reglementare AI Act, inclusiv prin utilizarea sandbox-urilor de reglementare; (4) dezvoltarea de politici organizaționale de guvernanță a IA care să adreseze riscurile generate de utilizarea neautorizată a instrumentelor IA (shadow AI).

REFERINȚE:

1. Consiliul Uniunii Europene. (2026). Council agrees position to streamline rules on Artificial Intelligence – Digital omnibus on AI. Comunicat de presă, 13 martie 2026. Disponibil la: https://www.consilium.europa.eu/
2. Darktrace. (2024). AI and Cybersecurity: Predictions for 2025. Darktrace Blog. Disponibil la: https://www.darktrace.com/blog/ai-and-cybersecurity-predictions-for-2025

3. Deloitte. (2025). Cybersecurity Report 2025: AI Threats, Email Server Security, and Advanced Threat Actors. Global Cyber Threat Intelligence Annual Report. Disponibil la: https://www.deloitte.com/
4. Grand View Research. (2024). AI In Cybersecurity Market Size, Share & Trends Analysis Report. Disponibil la: https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-cybersecurity-market-report
5. IBM. (2024). Cost of a Data Breach Report 2024. Ponemon Institute, sponsored by IBM. Disponibil la: https://www.ibm.com/reports/data-breach
6. IBM. (2025). Cost of a Data Breach Report 2025: The AI Oversight Gap. Ponemon Institute, sponsored by IBM. Disponibil la: https://www.ibm.com/reports/data-breach
7. Lakera. (2025). AI Security Trends 2025: Market Overview & Statistics. Disponibil la: https://www.lakera.ai/blog/ai-security-trends
8. Mastercard. (2025). New cybersecurity survey 2025: AI, scam fears and fraud risks. Disponibil la: https://www.mastercard.com/global/en/news-and-trends/stories/2025/consumer-cybersecurity-survey.html
9. Parlamentul European. (2024). EU AI Act: first regulation on artificial intelligence. Disponibil la: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/
10. Tech Advisors. (2025). AI Cyber Attack Statistics 2025. Disponibil la: https://tech-adv.com/blog/ai-cyber-attack-statistics/
11. World Economic Forum. (2025). Global Cybersecurity Outlook 2025. In collaboration with Accenture. Geneva: WEF. Disponibil la: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

Coordonator științific: CATRUC Adriana, drd., asistent universitar
ORCID: 0000-0002-9024-8610
Academia de Studii Economice din Moldova
mun. Chișinău, str. Bănulescu-Bodoni 61
Telefon: +373 (022) 402-988
e-mail: catruc@ase.md