DOI: https://doi.org/10.53486/sstc2026.v1.107

CZU: 004.8:004.056.53

ARTIFICIAL INTELLIGENCE BETWEEN INNOVATION AND SECURITY RISKS IN THE DIGITAL ECONOMY

INTELIGENȚA ARTIFICIALĂ ÎNTRE INOVAȚIE ȘI RISCURI DE SECURITATE ÎN ECONOMIA DIGITALĂ

ROTARU Andreea, studentă, specialitatea: Business și Administrare
Academia de Studii Economice din Moldova, Republica Moldova, Chișinău, str. Bănulescu-Bodoni 61, www.ase.md
e-mail autor: andreea.rotaru.t0fo@ase.md

Abstract: *The rapid development of artificial intelligence is transforming the digital economy by generating new opportunities for innovation, efficiency and business growth. At the same time, this transformation introduces complex security challenges, including cyberattacks, data breaches, algorithmic manipulation and digital fraud. The importance of this topic is determined by the increasing dependence of organizations and consumers on digital technologies powered by artificial intelligence. The aim of the study is to analyze the dual role of artificial intelligence in the digital economy, focusing on both its contribution to innovation and the risks it creates in terms of cybersecurity. The research is based on the analysis of scientific literature and recent international reports. The findings indicate that while artificial intelligence enhances productivity and competitiveness, it also amplifies vulnerabilities in digital systems, requiring stronger regulation, monitoring and risk management strategies. Ensuring a balance between technological progress and security is essential for the sustainable development of the digital economy.*
Key words: *Artificial intelligence, digital transformation, cybersecurity threats, innovation, data protection, risk management.*
JEL CLASSIFICATION: O33, D83, L86

INTRODUCERE

În ultimii ani, dezvoltarea rapidă a tehnologiilor digitale a determinat transformări majore în economie, iar inteligența artificială (IA) a devenit unul dintre principalii factori ai acestei schimbări. Utilizarea inteligenței artificiale în domenii precum business, comerț electronic, finanțe sau servicii digitale contribuie la automatizarea proceselor, creșterea eficienței și îmbunătățirea procesului decizional. Astfel, economia digitală devine tot mai dependentă de sisteme inteligente și de prelucrarea volumelor mari de date.

Cu toate acestea, pe lângă avantajele evidente, integrarea inteligenței artificiale generează și o serie de provocări semnificative, în special în domeniul securității. Creșterea numărului de atacuri cibernetice, riscurile legate de protecția datelor și apariția unor forme avansate de fraudă digitală evidențiază necesitatea unei abordări mai atente asupra utilizării acestor tehnologii (World Economic Forum, 2023). În același timp, utilizarea algoritmilor inteligenți poate crea vulnerabilități suplimentare în sistemele digitale, ceea ce impune dezvoltarea unor mecanisme eficiente de protecție și reglementare (European Commission, 2024).

Importanța cercetării este determinată de rolul tot mai mare al inteligenței artificiale în dezvoltarea economiei digitale și de impactul acesteia asupra securității informaționale și economice. În acest context, este esențială analiza atât a beneficiilor, cât și a riscurilor generate de utilizarea inteligenței artificiale, pentru a identifica soluții care să permită o dezvoltare sustenabilă și sigură.

Scopul cercetării constă în analiza rolului inteligenței artificiale în economia digitală, cu accent pe relația dintre inovație și riscurile de securitate asociate utilizării acesteia.

Obiectivele principale ale cercetării sunt:

- examinarea modului în care inteligența artificială contribuie la transformarea economiei digitale;

- evaluarea impactului tehnologiilor bazate pe inteligență artificială asupra eficienței și competitivității economice;
- analiza principalelor riscuri de securitate generate de utilizarea inteligenței artificiale în mediul digital;
- identificarea unor măsuri și soluții care pot reduce vulnerabilitățile și îmbunătăți protecția datelor.

CONȚINUTUL DE BAZĂ

Analiză succintă a surselor bibliografice în domeniul problemei cercetate. În ultimii ani, inteligența artificială a devenit tot mai prezentă în economie, influențând modul în care companiile funcționează și iau decizii. Din analiza surselor bibliografice, se observă clar că această tehnologie nu mai este doar un avantaj competitiv, ci o necesitate în mediul digital.

Conform (OECD, 2019), inteligența artificială contribuie la dezvoltarea economică prin optimizarea proceselor și crearea unor noi oportunități, însă utilizarea acesteia trebuie gestionată atent pentru a evita efectele negative. În aceeași direcție, (McKinsey & Company, 2023) evidențiază faptul că IA poate crește semnificativ productivitatea, dar în același timp accelerează schimbările din piață.

Pe partea de securitate, (IBM Security, 2023) arată că riscurile cibernetice sunt în creștere, iar utilizarea inteligenței artificiale poate face atacurile mai rapide și mai greu de detectat. De asemenea, (World Economic Forum, 2023) subliniază că tehnologiile digitale aduc atât beneficii, cât și riscuri majore la nivel global.

Din punct de vedere legislativ, (European Commission, 2024) propune un cadru clar de reglementare prin "Artificial Intelligence Act", cu scopul de a controla utilizarea IA și de a reduce riscurile. Totodată, (European Parliament, 2023) atrage atenția asupra impactului dual al inteligenței artificiale - atât pozitiv, cât și negativ.

În completare, (Russell și Norvig, 2020) oferă o bază teoretică solidă pentru înțelegerea modului în care funcționează sistemele de inteligență artificială și a implicațiilor acestora.

În ansamblu, sursele analizate arată că inteligența artificială este un factor esențial în economia digitală, dar vine la pachet cu provocări serioase, mai ales în domeniul securității.

Descrierea metodelor de cercetare utilizate. Pentru realizarea acestei lucrări au fost utilizate mai multe metode de cercetare, adaptate temei analizate.

În primul rând, s-a folosit *analiza documentară*, care a presupus studierea rapoartelor, articolelor și publicațiilor relevante din domeniul inteligenței artificiale. Această metodă a ajutat la înțelegerea situației actuale și a principalelor tendințe.

În al doilea rând, a fost aplicată *metoda comparativă*, prin care au fost analizate diferite opinii și abordări privind impactul inteligenței artificiale asupra economiei și securității digitale. Astfel, s-au putut observa atât avantajele, cât și riscurile.

De asemenea, s-a utilizat *metoda analitică*, prin care informațiile colectate au fost interpretate și corelate, pentru a evidenția legătura dintre dezvoltarea IA și apariția vulnerabilităților.

Rezultatele obținute. În urma analizei realizate, se poate observa că inteligența artificială are un impact major asupra economiei digitale. Aceasta contribuie la automatizarea proceselor, reducerea costurilor și creșterea eficienței în cadrul organizațiilor.

În același timp, utilizarea IA aduce și riscuri importante, în special în domeniul securității cibernetice. Atacurile devin mai sofisticate, iar tehnologiile precum „deepfake" sau „phishing automatizat" sunt din ce în ce mai frecvente.

Un alt aspect important este faptul că dezvoltarea rapidă a inteligenței artificiale nu este întotdeauna însoțită de reglementări suficiente. Acest lucru poate duce la utilizarea necontrolată a tehnologiei și la apariția unor probleme la nivel economic și social.

De asemenea, s-a constatat că nivelul de protecție depinde nu doar de tehnologie, ci și de modul în care aceasta este utilizată. Educația digitală și măsurile de securitate adoptate de organizații joacă un rol esențial în prevenirea riscurilor.

Tabelul 1. Analiza impactului IA asupra economiei digitale și riscurilor de securitate

Domeniul analizat	**Impact pozitiv**	**Riscuri asociate**
Procese economice	Automatizare, eficiență crescută, reducerea costurilor	Dependență de tehnologie
Securitate cibernetică	Detectarea rapidă a amenințărilor	Atacuri cibernetice mai sofisticate
Protecția datelor	Analiza și monitorizarea datelor în timp real	Scurgeri de date, utilizare abuzivă
Mediul online	Personalizarea serviciilor și experienței utilizatorului	Manipulare informațională
Piața muncii	Crearea locurilor de muncă	Dispariția unor locuri de muncă tradiționale
Sector financiar	Analiză predictivă și detectarea fraudelor	Fraudă digitală, phishing automatizat

Sursa: elaborată de autor în baza analiticei

Pentru a evidenția mai clar impactul inteligenței artificiale asupra economiei digitale, (Tabelul 1) prezintă principalele domenii în care aceasta influențează activitatea economică, atât din perspectivă pozitivă, cât și din punct de vedere al riscurilor asociate.

Analizând informațiile din tabel, se observă că inteligența artificială contribuie semnificativ la creșterea eficienței și automatizarea proceselor, în special în domenii precum securitatea cibernetică și sectorul financiar. Totodată, aceasta permite o analiză rapidă a datelor și o personalizare mai bună a serviciilor oferite utilizatorilor.

Cu toate acestea, utilizarea acestor tehnologii implică și o serie de riscuri importante. Printre cele mai relevante se numără atacurile cibernetice avansate, scurgerile de date și manipularea informației în mediul online. De asemenea, dezvoltarea inteligenței artificiale poate duce la schimbări semnificative pe piața muncii, prin reducerea unor activități tradiționale.

Tabelul 2. Comparația între securitatea tradițională și securitatea bazată pe IA

Criteriu	**Securitatea tradițională**	**Securitatea bazată pe IA**
Metodă de funcționare	Reguli fixe, sisteme predifinite	Algoritmi adaptivi și învățare automată
Detectarea amenințărilor	Lentă, bazată pe semnături cunoscute	Rapidă, identificată și amenințări necunoscute
Reacția la atacuri	Analiza și monitorizarea datelor în timp real	Scurgeri de date, utilizare abuzivă
Eficiență	Limitată în fața atacurilor complexe	Ridicată, datorită analizelor automate
Adaptabilitate	Scăzută	Foarte ridicată
Costuri	Mai mici inițial	Mai mari, dar eficiente pe termen lung
Tipuri de riscuri	Atacuri clasice	Atacuri avansate
Necesitatea factorului uman	Ridicată	Redusă, dar necesită supraveghere

Sursa: elaborată de autor în baza studiului

Pentru a înțelege diferențele dintre metodele clasice și cele moderne, de protecție, datele din (Tabelul 2) prezintă o comparație între securitatea tradițională și securitatea bazată pe inteligență artificială.

Datele prezentate evidențiază faptul că sistemele tradiționale sunt bazate pe reguli fixe și reacționează în general după producerea incidentelor, ceea ce le face mai puțin eficiente în fața

amenințărilor complexe. În schimb, securitatea bazată pe inteligență artificială utilizează algoritmi avansați, capabili să identifice și să prevină atacurile în timp real.

Un alt aspect important este nivelul de adaptabilitate. Sistemele inteligente pot învăța din date și se pot adapta rapid la noi tipuri de atacuri, spre deosebire de metodele tradiționale, care necesită actualizări constante.

Totuși, utilizarea inteligenței artificiale implică și anumite provocări, cum ar fi costurile mai ridicate și necesitatea unei monitorizări continue pentru a evita utilizarea necorespunzătoare.

CONCLUZII

În urma analizei realizate, se poate afirma că inteligența artificială joacă un rol esențial în dezvoltarea economiei digitale, contribuind semnificativ la creșterea eficienței, automatizarea proceselor și îmbunătățirea performanței organizațiilor. Utilizarea acesteia oferă oportunități reale pentru inovare și competitivitate, în special în domenii precum comerțul electronic, sectorul financiar și serviciile digitale.

Totodată, rezultatele cercetării evidențiază faptul că dezvoltarea rapidă a inteligenței artificiale este însoțită de o serie de riscuri importante, în special în domeniul securității cibernetice. Atacurile devin mai complexe, iar utilizarea tehnologiilor avansate poate facilita fraudele digitale, manipularea informației și compromiterea datelor.

Un aspect relevant este necesitatea unui echilibru între beneficiile și riscurile generate de utilizarea inteligenței artificiale. În acest context, implementarea unor reglementări clare și eficiente, precum și dezvoltarea unor sisteme de securitate adaptate noilor tehnologii, devin esențiale.

De asemenea, este important ca organizațiile să investească în protecția datelor și în instruirea utilizatorilor, pentru a reduce vulnerabilitățile și a preveni incidentele de securitate. Conștientizarea riscurilor și utilizarea responsabilă a tehnologiilor digitale reprezintă factori cheie pentru dezvoltarea unui mediu digital sigur.

În concluzie, inteligența artificială reprezintă atât o oportunitate majoră pentru economia digitală, cât și o sursă de provocări, iar gestionarea eficientă a acesteia depinde de capacitatea de a combina progresul tehnologic cu măsuri adecvate de securitate.

REFERINȚE:

1. European Commission. (2024). Artificial Intelligence Act. European Union. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
2. European Parliament. (2023). Artificial intelligence: threats and opportunities. European Union. https://www.europarl.europa.eu/topics/en/article/20200918STO87404/artificial-intelligence-threats-and-opportunities
3. IBM Security. (2023). Cost of a Data Breach Report. IBM. https://www.ibm.com/reports/data-breach
4. McKinsey & Company. (2023). The economic potential of generative AI. McKinsey. https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier
5. OECD. (2019). Artificial Intelligence in Society. OECD Publishing. https://www.oecd.org/en/publications/artificial-intelligence-in-society_eedfee77-en.html
6. Russell, S., & Norvig, P. (2020). Artificial Intelligence: A Modern Approach. Pearson.
7. World Economic Forum. (2023). Global Risks Report 2023. World Economic Forum. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

Coordonator științific: CAPAȚINA Valentina, dr., conf. univ.
Academia de Studii Economice din Moldova, www.ase.md
Republica Moldova, Chișinău, str. Bănulescu-Bodoni, 61
e-mail: valentina@ase.md