Univerzitet Sinergija
www.sinergija.edu.ba
Bijeljina

SINERGIJA 2026

XXVI NAUČNI SKUP
SA MEĐUNARODNIM UČEŠĆEM
ZBORNIK RADOVA

Inovacije, bezbjednost i etika u savremenom digitalnom i održivom poslovanju

Bijeljina, april 2026. godine

ZBORNIK RADOVA
"SINERGIJA"

XXVI NAUČNI SKUP SA MEĐUNARODNIM UČEŠĆEM
Bijeljina, 29. april 2026. godine

INOVACIJE, BEZBJEDNOST I ETIKA U SAVREMENOM DIGITALNOM I ODRŽIVOM POSLOVANJU

Izdavač:
UNIVERZITET SINERGIJA
Raje Baničića bb, Bijeljina
www.sinergija.edu.ba

Za izdavača:
prof. dr Saša Adamović

Glavni urednik:
prof. dr Saša Adamović

Tehnički urednik:
Aleksandar Sandro Cvetković, MSc

Tehnički sekretari:
Jelena Manojlović, MSc
Aleksandar Sandro Cvetković, MSc

Kontakt:
Univerzitet Sinergija
Raje Baničića bb, 76 300 Bijeljina
Bosna i Hercegovina
+387 55 21 71 01, lokal 109
naucni.skup@sinergija.edu.ba

On-line pristup: http://www.naucniskup.sinergija.edu.ba

eISSN: 2490-3825

*Naučni skup "Sinergija" je podržan od strane Ministarstva za naučnotehnološki razvoj i visoko obrazovanje Republike Srpske

NAUČNI ODBOR

- Saša Adamović, predsjednik,
  Univerzitet Sinergija, Bijeljina, BiH
- Milenko Stanić,
  Univerzitet Sinergija, Bijeljina, BiH
- Marko Šarac,
  Univerzitet Sinergija, Bijeljina, BiH
- Nikica Radović,
  Univerzitet Sinergija, Bijeljina, BiH
- Marijana Prodanović,
  Univerzitet Sinergija, Bijeljina, BiH
- Goran Filipić,
  Univerzitet Sinergija, Bijeljina, BiH
- Žaklina Spalević,
  Univerzitet Sinergija, Bijeljina, BiH
- Željko Stojanov,
  University of Novi Sad, Technical Faculty „Mihajlo Pupin“, Zrenjanin
- Ilija Hristoski,
  Faculty of Economics, „St. Kliment Ohridski“ University, Macedonia
- Daniel Dejica,
  Polytechnic University of Timisoara, Timişoara, Romania
- Vida Drąsutė,
  Faculty of Informatics, Kaunas University of Technology, Lithuania
- Giedrius Gecevicius,
  Univeristy of Applied Sciences · Technologies faculty, Lithuania
- Zaza Tsotniashvili,
  Caucasus International University, Georgia
- Milan Simić,
  RMIT University, Melbourne, Australia
- Velibor Spalevic,
  Univerzitet Crne Gore, Filozofski fakultet
- Igor Pelliciari,
  Faculty of World Economy and International Affairs, Italy
- Jurij Bajec,
  Faculty of Computer and Information Science, Slovenija
- Dragutin Gutić,
  Visoka škola za finansije i pravo „Efectus“, Hrvatska
- Tomislav Pavlović,
  Filološko-umetnički fakultet, Kragujevac, Srbija
- Milan Milosavljević,
  Elektrotehnički fakultet, Beograd, Srbija
- Mladen Veinović,
  Univerzitet Singidunum, Beograd, Srbija
- Aleksandar Jevremović,
  Univerzitet Singidunum, Beograd, Srbija
- Vladislav Mišković,
  Univerzitet Singidunum, Beograd, Srbija
- Nemanja Stanišić,
  Univerzitet Singidunum, Beograd, Srbija
- Goranka Knežević,
  Univerzitet Singidunum, Beograd, Srbija
- Goran Avlijaš,
  Univerzitet Sinergija, Bijeljina, BiH
- Marko Milojević,
  Univerzitet Sinergija, Bijeljina, BiH
- Snježana Stanišić,
  Univerzitet Sinergija, Bijeljina, BiH
- Sanel Jakupović,
  Univerzitet Apeiron, Banja Luka, BiH
- Ivana Ćirković Miladinović,
  Fakultet pedagoških nauka, Jagodina, Srbija
- Darko Marinković,
  Kriminalističko-policijska akademija, Zemun, Srbija
- Radovan Vukadinović,
  Pravni fakultet, Kragujevac, Srbija
- Mihailo Velimirović,
  Pravni fakultet, Podgorica, Crna Gora
- Milan Palević,
  Pravni fakultet, Kragujevac, Srbija
- Miodrag Mićović,
  Pravni fakultet, Kragujevac, Srbija
- Miodrag Savović,
  Fakultet za menadžment, Herceg Novi, Crna Gora

ORGANIZACIONI ODBOR

- prof. dr Saša Adamović, predsjednik
  Univerzitet Sinergija, Bijeljina, BiH
- prof. dr Milenko Stanić
  Univerzitet Sinergija, Bijeljina, BiH
- doc. dr Goran Filipić
  Univerzitet Sinergija, Bijeljina, BiH
- prof. dr Marijana Prodanović
  Univerzitet Sinergija, Bijeljina, BiH

SEKRETARIJAT

- Aleksandar Sandro Cvetković, MSc, tehnički urednik
  Univerzitet Sinergija, Bijeljina, BiH
- Jelena Manojlović, MSc, tehnički sekretar
  Univerzitet Sinergija, Bijeljina, BiH

KONTAKT

E-mail: naucni.skup@sinergija.edu.ba
www.sinergija.edu.ba
Tel. +387 55-217-100, +387 055-217-101
Faks +387 55-219-071

SADRŽAJ/CONTENTS

UDK 007.52:[005.96:004.8(4-672EU)
DOI 10.7251/ZRSNG2526001M

Optimization of Generative AI Efficiency: A Case Study Based on Professional Workshop Questionnaires

Milica Mravik[1], Marko Šarac[2]
Faculty of Informatics and Computing, Singidunum University[1], Belgrade,
Faculty of Computing and Informatics, Sinergija University[2], Bijeljina

In this research, we explored the strategic optimization of Microsoft 365 Copilot by examining the transition from theoretical readiness to practical user mastery. This research was based on a structured "Art of the Possible" (AOTP) workshop approach, which was the key method for discovering high-impact business scenarios. By analysing quantitative and qualitative information from an AI Workshop Questionnaire, we were able to determine the impact of specific organizational interventions on user adoption and technical efficiency. Our results showed that successful optimization was more than just a function of technical setup and was instead highly reliant on expertise in prompt engineering and addressing security issues, like data oversharing. In addition, we emphasized the need for a "Crawl-Walk-Run" approach and the critical role of internal "Champions" in maintaining digital transformation. We concluded that a feedback loop between end-users and stakeholders is necessary for aligning generative AI capabilities with organizational goals.

Keywords – ***Microsoft 365 Copilot, AI Optimization, Prompt Engineering, Digital Transformation, Art of the Possible (AOTP), User Adoption Framework***

I. INTRODUCTION

The current state of the organizational environment is in the midst of a paradigm shift that involves the integration of large language models (LLMs) into the very heart of workplace productivity [1, 2]. Microsoft 365 Copilot is a more advanced form of this technological shift, providing a seamless integration between generative artificial intelligence and traditional enterprise software [3]. Nevertheless, the literature on digital transformation and technology adoption implies that the mere possession of highly advanced technological assets does not automatically lead to enhanced performance. Rather, we noticed that the difference between technological potential and actual productivity is often bridged by aligning the technological asset with the socio-technical context of the organization [4, 5].

Before embarking on this research, we were cognizant of the fact that the major challenge to the successful implementation of AI technology is the absence of a structured pedagogical framework for end-users. While the adoption of traditional software technology is based on deterministic functional training, the adoption of generative AI technology is predicated on a heuristic understanding of prompt engineering and feedback. Hence, we aimed to explore the role of a methodology-driven intervention, namely the "Art of the Possible" (AOTP) workshop, in facilitating the shift from passive observation to active, high-value use [6].

One of the major academic concerns in the use of AI in the corporate setting is data governance and security. We highlighted that institutional concern about data oversharing and privacy tends to lead to a conservative adoption rate, which is fundamentally limiting to the tool's potential. To mitigate this, we incorporated a full analysis of the organization's data estate into our design, ensuring that technical setup and security posture was the basis for user engagement. This enabled us to investigate the relationship between perceived security and user willingness to test novel AI-based workflows.

In addition, we investigated the role of organizational change management through the prism of a "Champion" network. Our study assumed that innovation diffusion is most successful when facilitated by peer-to-peer knowledge sharing, rather than top-down directives. By encouraging internal early adopters to identify and record "Quick Wins," we created a knowledge base of localized success stories that appealed to the specific needs of different organizational departments. This enabled a transition from theoretical benefit to concrete task-specific optimization [7].

The primary research objective of this study is to assess the effectiveness of structured adoption processes in improving user expertise and ROI as a measure of organizational return on investment. By conducting a thorough analysis of the data collected from an AI Workshop Questionnaire, we sought to uncover the key success factors that distinguish a mature AI ecosystem. We focused on the degree to which a staged "Crawl-Walk-Run" strategy can counter the cognitive burden on users, thus ensuring the long-term viability of digital transformation.

In conclusion, this paper offers a comprehensive assessment of AI optimization, one that extends from the technical requirements of the software to the human and organizational factors that determine its success. We believe that this research has helped to advance the scientific

understanding of how generative AI can be systematically incorporated into the workplace to facilitate significant cognitive and functional progress [8].

II. METHODS AND MATERIALS

In order to scientifically assess the optimization of Microsoft 365 Copilot in a business setting, we adopted a mixed-methods research design. This allowed us to combine the results of quantitative diagnostic testing with qualitative pedagogical interventions. The research was conducted in two main phases: a diagnostic test using a standardized questionnaire, followed by a structured multi-stage instructional program called the "Art of the Possible" (AOTP) workshop. This two-pronged approach enabled us to measure the technical readiness level while also monitoring user adoption matrices.

A. Participant Selection and Cohort Structuring

The research employed a purposive sampling approach to build the initial deployment pool. Instead of launching the solution on a universal scale, we isolated a localized pool of 80 "Early Adopters" and internal "Champions" from various cross-functional departments, such as Human Resources, Marketing, and Operations. This pool was used as the experimental group to test the effectiveness of prompt engineering and isolate high-friction workflows.

B. Instrument Design: The AI Readiness Questionnaire

Before the intervention in the workshop, we administered an "AI Workshop Questionnaire" to evaluate organizational maturity on various digital fronts. This tool was designed to go beyond the subjective user excitement and instead measure the structural and technical readiness. We broke down the questionnaire into five different dimensions of operations, which became our key independent variables for evaluating the potential for optimization [9].

TABLE I. STRUCTURAL DIMENSIONS OF THE AI READINESS QUESTIONNAIRE

ID	AI READINESS QUESTIONNAIRE		
	Questionnaire Dimension	***Primary Research Focus***	***Key Metrics Evaluated***
1	Strategic Drivers	Organizational motivation for AI adoption	Generalized AI interest vs. specific Microsoft 365 integration intent
2	Target Scenarios	Departmental applicability	Expected impact on HR, Marketing, Operations, and Customer Service
3	Technical Architecture	Foundational software readiness	Current licensing, update channels, and device management protocols
4	Data Governance	Risk mitigation and compliance	Utilization of Data Loss Prevention (DLP) and sensitivity labelling
5	User Proficiency	Existing digital literacy	Frequency of cloud collaboration and automated workflow usage

Table 1 - Structural Dimensions of the AI Readiness Questionnaire

C. The "Art of the Possible" (AOTP) Workshop Framework

After the completion of the diagnostic process, we started the AOTP workshop series. The educational goal of these workshops was to move the users from a passive state of theoretical knowledge to an active state of application. The curriculum was designed to gradually decrease the cognitive load while increasing the complexity of AI interactions [10, 11].

The workshop was executed across four structured modules, as detailed in Table 2.

TABLE II. CURRICULUM STRUCTURE OF THE AOTP ENABLEMENT WORKSHOP

Phase	AOTP ENABLEMENT WORKSHOP		
	Module Phase	***Pedagogical Objective***	***Core Activities and Demonstrations***
1	Foundations	Establish theoretical literacy	Introduction to Large Language Models (LLMs), AI ethics, and Responsible AI frameworks.
2	Functional Demo	Showcase cross-platform utility	Live demonstrations of Copilot within Word, Excel, PowerPoint, and Teams environments.
3	Scenario Discovery	Contextualize AI to daily tasks	Collaborative mapping of departmental pain points into actionable "Persona" use cases.
4	Prompt Engineering	Optimize user-machine interaction	Practical exercises in constructing structured, context-rich queries to minimize AI hallucination.

Table 2 - Curriculum Structure of the AOTP Enablement Workshop

D. Governance Assessment and Risk Mitigation

One of the most critical aspects of our strategy was the aggressive audit of the data estate of the organization. We recognized that the generative AI model is optimized for data retrieval, which inherently leads to the risk of "oversharing" if the internal documents are not properly restricted. However, since large language models are based on semantic indexing to establish relationships across the entire Microsoft 365 tenant, traditional permission models, which are based on user obscurity rather than explicit restriction, are no longer adequate to protect sensitive information.

From the questionnaire, we were able to establish that the target infrastructure did not have automated Data Loss Prevention (DLP) protocols and sensitivity labels. Therefore, our strategy had to establish a "governance-first" baseline. Before allowing users to query the organizational data graph, we had to enforce the use of basic sensitivity labels. This targeted remediation sprint included the process of classifying existing documents based on clear confidentiality levels, such as public, internal, and highly restricted.

This ensured that the data collected for the subsequent optimization was done in a secure and compliant environment,

and not in an environment where the results were biased by the concerns of data leakage.

E. The Phased Implementation Model

To implement the results of the workshop and questionnaire, we aligned our deployment plan with a staged "Crawl-Walk-Run" approach to adoption.

1. "Crawl" Stage (Assess & Prepare): Primarily aimed at proving the scenarios identified in the AOTP workshops and supporting the initial 80 users.
2. "Walk" Stage (Execute): Primarily aimed at raising awareness, supporting peer-to-peer knowledge sharing through "Champions", and validating the quality of initial semantic indexing.
3. "Run" Stage (Optimize): Primarily aimed at full-scale deployment, where optimization was measured through tangible time-savings in the specific use cases identified (e.g., HR resume summarization, Marketing text creation).

Through the alignment of the quantitative readiness results (Table 1) with the qualitative results of the workshop scenarios (Table 2), this approach offered a comprehensive framework for measuring exactly how technical implementation and human training interact to optimize AI efficiency.

III. RESULTS AND DISCUSSION

The empirical evidence gathered from the diagnostic stage and the "Art of the Possible" (AOTP) workshops provided invaluable information on the organizational dynamics of the adoption of generative AI. The results of our study reveal an important gap between the strong user interest in the operational efficiency of AI and the weaknesses in the data architecture.

A. Quantitative Readiness and Data Governance Posture

The results of the AI Readiness Questionnaire provided a conclusive basis for understanding both the strategic intent and the technical maturity of the organization. Significantly, the results showed that the driving force behind the adoption of generative AI was not a generic, reactive response to the global AI phenomenon. Rather, the strategic intent of the organization was to have a specific, deliberate approach to integrating Microsoft 365 Copilot as a native extension of their existing productivity suite. This is a crucial point, as it indicates a transition from theoretical AI research to practical, workflow-integrated technological adoption with the goal of reducing user context-switching.

When asked about expected operational use cases, the respondents showed a universal acceptance for all business units polled: Customer Service, Sales & Marketing, Research & Development, Supply Chain & Operations, and Internal Finance/HR.

This universal acceptance suggests that the organization's workforce recognizes the value of generative AI not only as a vertical IT solution but also as a horizontal capability that can be leveraged to drive efficiency in multiple operational areas. For example, while the Marketing function expected rapid content creation, the Supply Chain function recognized the potential for automated logistical forecasting and process documentation.

However, a key dichotomy that emerged was through the Data Governance section of the diagnostic questionnaire. Despite the strong user enthusiasm and readiness for adoption, the technical architecture was found to be extremely vulnerable to severe data protection risks.

The integration of Large Language Models (LLMs) in a corporate setting alters the paradigm of data exposure and synthesis. Microsoft 365 Copilot uses semantic indexing to index the entire data graph of the organization. Hence, if the data is not classified and controlled, the AI system has the potential to bypass the traditional security measures by exposing confidential data to unauthorized personnel [12, 13].

These structural issues were clearly identified through the results of the questionnaire. The organization was failing to protect data at the content level by not using rights management, nor were they using active Data Loss Prevention (DLP) protocols for cloud-based content. More seriously, the organization was failing to use active sensitivity labels to manage document access. In the context of generative AI, the lack of sensitivity labels immediately put the organization at risk of "oversharing." Without these cryptographic controls, a generic user request could easily ask the AI system to analyse and summarize files that were unrestricted but highly confidential, such as internal HR salary structures, unpublished financial data, or proprietary R&D information. Therefore, these results immediately made it necessary that a remediation sprint occur before any kind of deployment was possible.

TABLE III. BASELINE DATA GOVERNANCE AND RISK ASSESSMENT RESULTS

ID	DATA GOVERNANCE AND RISK ASSESSMENT		
	Governance Control Parameter	***Current Organizational Status***	***Identified Optimization Risk***
1	Content-Level Encryption	Not implemented	High risk of unauthorized data parsing by LLMs.
2	Data Loss Prevention (DLP)	Not deployed	Inability to track or restrict the external sharing of AI-generated sensitive data.
3	Sensitivity Labeling	Not deployed	High risk of internal "oversharing," allowing unauthorized employees to surface confidential HR or financial data via Copilot prompts.
4	Mobile Device Management	Implemented (Intune)	Baseline security met for external device access, reducing end-point vulnerabilities.

Table 3 - Baseline Data Governance and Risk Assessment Results

These results empirically verified our hypothesis that technical configuration had to occur before widespread user enablement. The absence of sensitivity labelling created an immediate risk of internal data oversharing once the semantic index of Copilot was turned on, requiring a delay in the full organizational rollout until a basic governance structure could be put in place.

B. Scenario Discovery and Operational Optimization

In the AOTP workshops, we were able to successfully translate the theoretical need for AI into actionable, localized workflows. By employing a persona-based framework ("As someone in [Role], I want to use Copilot to [Action], to achieve [Result]"), we were able to identify the precise pain points where AI optimization would provide the greatest Return on Investment (ROI).

The workshops provided us with a very specific set of operational scenarios. These were organized into a functional adoption matrix, as seen in Table 4, which became the roadmap for our prompt engineering modules.

TABLE IV. PRIORITIZED BUSINESS SCENARIOS IDENTIFIED DURING AOTP WORKSHOPS

Business Unit	**BUSINESS SCENARIOS IDENTIFIED DURING AOTP WORKSHOPS**		
	Target Persona / Role	***AI Optimization Action (Prompt Focus)***	***Strategic Objective / Expected ROI***
HR	HR Recruiter	Summarize candidate resumes and applicant profiles.	Shorten the hiring process and facilitate faster callback decisions.
Marketing	Content Creator	Generate advertising texts, relevant metatexts, keywords, and tags.	Rapid and efficient creation of tailored marketing collateral.
Marketing & Supply	Project Lead	Accelerate the creation of complex PowerPoint presentation structures.	Save time and resources while generating "food for thought" frameworks.
Cross-Functional	Meeting Facilitator	Generate meeting agendas, outlining main topics and training content.	Prevent omission of critical topics and achieve measurable time savings.
Cross-Functional	Knowledge Worker	Summarize lengthy PDF documents and convert generated Word text into PowerPoint bases.	Decrease time spent processing documentation and accelerate output formatting.

Table 4 - Prioritized Business Scenarios Identified During AOTP Workshops

The discovery of these scenarios was essential. We found that users who tried to use Copilot for general queries soon suffered from tool fatigue. However, users who used Copilot for the specific scenarios listed in Table 4 reported immediate cognitive relief and time savings, thus establishing that the discovery of structured scenarios is a necessary antecedent for AI optimization.

C. Evaluating the "Crawl-Walk-Run" Implementation Strategy

To address the governance risks outlined in Section 3.1 while leveraging the high-value scenarios outlined in Section 3.2, we performed the deployment using the "Crawl-Walk-Run" approach.

Rather than a global deployment, we chose to enable Microsoft 365 Copilot for a carefully controlled initial set of 80 early adopters and internal Champions. This "Crawl" phase was closely tracked. We observed that a delayed assignment of licenses directly impacted the quality of Semantic Indexing in the first few weeks, as the AI model needed time to understand the relationships in the data graph of the organizational data.

At the same time, the IT leadership was challenged to complete an aggressive data governance sprint, cleaning up old external access and implementing sensitivity labels, before entering the "Walk" phase. This approach ensured that while the AI model's speed to uncover information increased, the security guardrails kept pace. This study asserts that achieving full user adoption and realizing ROI (the "Run" phase) will only be possible in late Q3 and Q4, as AI optimization is a long-term organizational marathon, not an IT sprint.

IV. CONCLUSION

The inclusion of generative artificial intelligence within the corporate environment is a paradigm shift in the way organization's function. Based on our analysis of the "Art of the Possible" (AOTP) workshop framework and the AI Readiness Questionnaire, we determined that the optimization of Microsoft 365 Copilot cannot be accomplished by technical implementation alone. To achieve true optimization, there must be a harmonious convergence of strong data governance, user enablement, and well-defined operational use cases.

Our research has shown that there is a high level of passion for AI, but there is a lack of the underlying data security infrastructure, such as Data Loss Prevention (DLP) and sensitivity labelling, necessary to implement these solutions in a secure manner. By recognizing this gap early in our diagnostic questionnaire, we have shown that a "governance-first" strategy is a necessary precursor to avoid the potential risk of internal data over-sharing [14].

Moreover, our results underscore the essential role of scenario discovery. Users interacting with Copilot via generic queries saw minimal improvements in productivity. However, when users started applying the tool to very specific, persona-related tasks such as summarizing HR applicant resumes or creating structured marketing materials, the ROI was immediate and quantifiable. This suggests that prompt engineering is more than a technical competence, it is a fundamental competence for the contemporary worker.

In conclusion, this study confirms the effectiveness of the "Crawl-Walk-Run" model of adoption. By limiting initial access to a controlled group of "Early Adopters" and

"Champions," organizations can deliberately observe the quality of semantic indexing and user feedback before rolling out to the broader enterprise. We propose that AI optimization is not a discrete IT initiative but a continuous, socio-technical process. Future studies should investigate the long-term cognitive effects of these tools on the creativity and task fatigue of the workforce over longer fiscal cycles.

ACKNOWLEDGEMENT

We would like to thank the IT leadership in the organizations, the internal network of AI Champions, and the early adopters who took part in the diagnostic questionnaires and workshops. Their open feedback and readiness to refine new operational processes were critical to the development of the findings of this research.

REFERENCES

[1] E. Brynjolfsson i A. McAfee , The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies, New York: W. W. Norton & Company, 2016.

[2] M. Corporation, „Will AI Fix Work?," Microsoft Corporation, May 2023. [Online]. Available: https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work. [Last access: February 2026].

[3] C. Vasilescu i M. Gheorghe, „Improving the Performance of Corporate Employees through the Use of Artificial Intelligence: The Case of Copilot Application," u *Proceedings of the International Conference on Business Excellence*, Warsaw, 2024.

[4] M. Mravik, T. Vetriselvi, K. Venkatachalam, M. Sarac i N. Bacanin, „Diabetes Prediction Algorithm Using Recursive Ridge Regression L2," *Computers, Materials & Continua, vol*. 71, no. 1, pp. 457-471, 2022.

[5] M. Šarac, M. Mravik, J. Dijana, Š. Ivana, Ž. Miodrag i B. D. Nebojša, „Intelligent diagnosis of coronavirus with computed tomography images using a deep learning model," *Journal of Electronic Imaging, vol*. 32, no., pp. 1-10, 2022. doi: 10.1117/1.JEI.32.2.021406.

[6] V. Venkatesh, M. G. Morris, G. B. Davis i F. D. Davis, „User Acceptance of Information Technology: Toward A Unified View," *MIS Quarterly, vol*. 27, no. 3, pp. 425-478, 2003.

[7] S. Noy i W. Zhang, „Experimental evidence on the productivity effects of generative artificial intelligence," *Science, vol*. 381, no. 6654, pp. 187-192, 2023.

[8] M. Corporation, „Microsoft 365 Copilot: Architecture and Data Governance Frameworks," unpublished internal technical documentation, Belgrade, 2023.

[9] M. Corporation, „What Can Copilot's Earliest Users Teach Us About Generative AI at Work?," Microsoft Corporation, November 2023. [Online]. Available: https://www.microsoft.com/en-us/worklab/work-trend-index/copilots-earliest-users-teach-us-about-generative-ai-at-work. [Last access February 2026].

[10] N. Carlini, M. Jagielski, A. Herbert-Voss, K. Lee, A. Roberts, T. Brown, C. Raffel, D. Song, Ú. Erlingsson i A. Oprea, „Extracting Training Data from Large Language Models," USENIX Security Symposium, 2021.

[11] J. White, Q. Fu, S. Hays, M. Sandborn, C. Olea, H. Gilbert, A. Elnashar, J. Spencer-Smith i D. C. Schmidt, „A Prompt Pattern Catalog to Enhance Prompt Engineering with ChatGPT," *arXiv preprint,* p. arXiv:2302.11382, 2023.

[12] I. D. W. Team, „AI Readiness and Copilot Implementation Questionnaire Results," Quantitative organizational data, unpublished, Belgrade, 2024.

[13] I. P. M. Office, „Art of the Possible (AOTP): Workshop Methodology and Scenario Discovery Framework," Corporate adoption guide, unpublished, Belgrade, 2024.

[14] A. Hasegawa i H. Shimizu, „The Role of Generative AI in Transforming Data Engineering Workflows and Automating Computational Infrastructure Design," *AIJCST, vol*. 4, no. 6, pp. 1-11, 2022.

UDK 004.777:004.738.5(100)
DOI 10.7251/ZRSNG2526006S

Arhitekture računarstva u oblaku: modeli, evolucija i komparativna analiza savremenih distribuiranih sistema

Cloud computing architectures: models, evolution and comparative analysis

Lazar Stošić[*1,2], Olja Krčadinac[1]
Faculty of Informatics and Computer Science, University Union—Nikola Tesla, Belgrade, Serbia[1];
Don State Technical University, Rostov-on-Don, Russian Federation[2]; lstosic@unt.edu.rs; okrcadinac@unionnikolatesla.edu.rs

Sažetak - Računarstvo u oblaku predstavlja dominantnu paradigmu za isporuku skalabilnih i fleksibilnih računarskih resursa putem Interneta. Brza evolucija cloud arhitektura—od tradicionalnih modela zasnovanih na virtualizaciji do savremenih paradigmi kao što su kontejnerizacija i serverless računarstvo—dovela je do povećane kompleksnosti u projektovanju i implementaciji sistema. Ovaj rad pruža sveobuhvatan pregled arhitektura računarstva u oblaku, sa fokusom na njihove modele, razvoj i komparativne karakteristike. Analizirani su modeli IaaS, PaaS i SaaS, kao i noviji pristupi poput kontejnera i serverless okruženja. Komparativna analiza zasnovana je na kriterijumima performansi, skalabilnosti, troškova i bezbednosti. Takođe su razmotreni aktuelni izazovi i budući pravci razvoja, uključujući edge računarstvo i primenu veštačke inteligencije u upravljanju resursima. Rezultati rada pružaju osnovu za razumevanje kompromisa između različitih arhitekturnih pristupa.

Ključne reči - računarstvo u oblaku; arhitektura; virtualizacija; kontejnerizacija; serverless; skalabilnost

Abstract **— Cloud computing represents the dominant paradigm for delivering scalable and flexible computing resources over the Internet. The rapid evolution of cloud architectures—from traditional models based on virtualization to modern paradigms such as containerization and serverless computing—has led to increased complexity in system design and implementation. This paper provides a comprehensive overview of cloud computing architectures, focusing on their models, development and comparative characteristics. IaaS, PaaS and SaaS models are analyzed, as well as newer approaches such as containers and serverless environments. The comparative analysis is based on performance, scalability, cost and security criteria. Also discussed are current challenges and future development directions, including edge computing and the application of artificial intelligence in resource management. The results of the work provide a basis for understanding the trade-offs between different architectural approaches.**

Keywords – ***cloud computing; architecture; virtualization; containerization; serverless, scalability***

I. INTRODUCTION

Cloud computing represents a fundamental change in the way computing resources are provided, managed and used. Instead of relying on local infrastructure, organizations are increasingly using cloud solutions to increase flexibility, reduce costs and improve system scalability.

The development of cloud technologies has led to the emergence of different architectural models with specific characteristics and limitations. Early systems were based on virtualization, while modern approaches include microservices, containerization, and the serverless paradigm.

The aim of this work is:

- analysis of cloud architecture evolution
- identification of key models
- comparative evaluation of their characteristics

II. CLOUD SERVICE DELIVERY MODELS

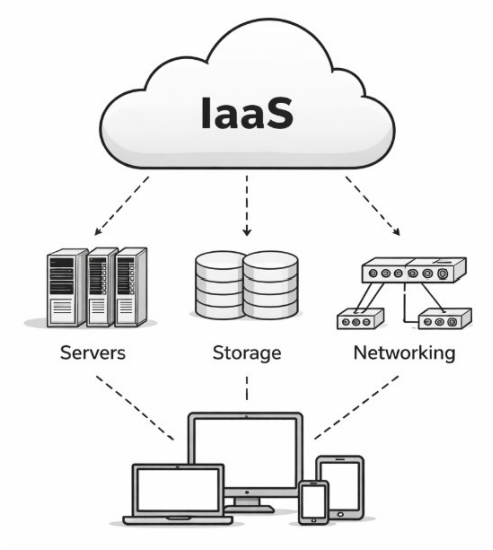
Cloud service delivery models define how IT resources and functionality are delivered to users over the Internet. Cloud computing is a model that uses a shared set of resources such as networks, servers, storage, virtual machines that can be quickly added and removed with minimal management overhead.[1] Basic models include IaaS (Infrastructure as a Service), which provides infrastructure (servers, networks, storage), PaaS (Platform as a Service), which provides a development environment and tools for applications, and SaaS (Software as a Service), where users directly use ready-made applications without infrastructure management.

These models allow for different levels of control, flexibility and accountability between providers and users,

thereby optimizing the use of resources and reducing IT system costs.

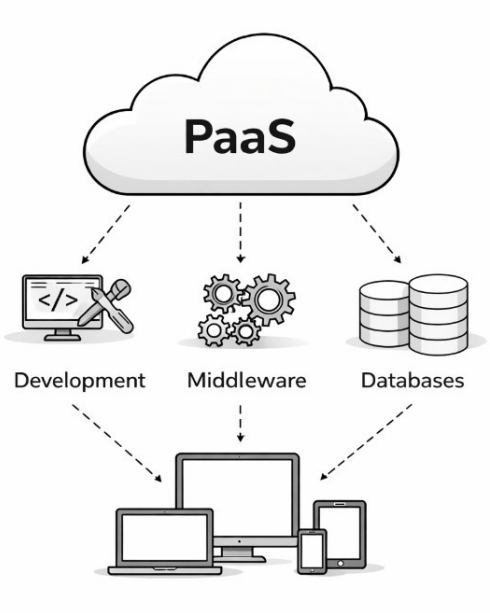
Service models

IaaS - (Infrastructure as a Service) represents the basic layer of the cloud model, which allows users to access virtualized computer resources, including virtual machines, storage and network infrastructure. The user has full control over the operating system, applications and configuration of the environment, while the cloud provider manages the physical infrastructure and virtualization layer. IT resources in the IaaS architecture are not preconfigured, which increases the administrator's responsibility. This model is best for cloud users who require more control over their environment. It happens that service providers sometimes use the services of other cloud servers in order to expand their own cloud. In the evolution of cloud architectures, the IaaS model marks the transition from physically bound systems to flexible, scalable and software-defined resources, while in a comparative analysis it provides the highest degree of control and responsibility compared to more abstract models such as PaaS and SaaS. The cloud-computing market is growing and the leaders in public- and private-cloud services can change. [2]



IaaS – Infrastructure as a Service

PaaS - (Platform as a Service) represents the middle layer of the cloud model that provides a development and execution environment for building, testing and implementing applications without the need to manage the basic infrastructure. The provider manages the operating system, middleware, databases and development tools, while the user focuses on developing the application logic. In the evolution of cloud architectures, the PaaS model enables acceleration of development and standardization of processes through automation and integrated services, while in a comparative analysis it represents a balance between flexibility (characteristic of IaaS) and ease of use (typical of the SaaS model). Briefly stated, PaaS is a "ready-to-use" model that contains already installed and configured IT resources. PaaS also serves as a platform for the industrialization of the software industry. [3]



PaaS – Platform as a Service

SaaS - (Software as a Service) represents the highest level of abstraction in cloud models, where users access complete applications via the Internet, without the need for installation, maintenance or management of the infrastructure and platform. All system components, including application logic, data and security, are fully under the control of the service provider. The SaaS framework is a software distribution model that allows clients to access applications over a network, with hosting managed by the provider. This process is known as the most sophisticated manifestation of cloud computing. [4] In the evolution of cloud architectures, the SaaS model enables mass availability and standardization of software solutions, while in a comparative analysis it offers the highest level of ease of use with minimal control over the system compared to IaaS and PaaS models. In the market, SaaS is taking over cloud computing, and globally, industries are showing interest in creating their own SaaS add-ons and renting services to grow on their desktops.[5]

SaaS – Software as a Service

III. COMPARATIVE ANALYSIS OF CLOUD ARCHITECTURES

Performance is a key criterion in the evaluation of cloud architectures and refers to the system's ability to efficiently process requests with minimal delay and optimal use of resources. This criterion includes metrics such as latency, bandwidth, response time and throughput, which directly affect the quality of user experience and reliability of applications. In a comparative analysis, different architectures (e.g. virtualized, containerized, serverless) show variations in performance due to differences in abstraction layers and resource management. Modern cloud-native and serverless architectures enable performance optimization through automatic scaling and load distribution, but may introduce additional latencies in specific scenarios (e.g. cold start effect).

Scalability represents the ability of the cloud architecture to effectively adjust system capacity to growing or decreasing load requirements, without performance degradation. This criterion includes horizontal scaling (adding new instances) and vertical scaling (increasing the resources of existing instances), whereby modern cloud-native and serverless architectures favor automated horizontal scaling. In a comparative analysis, container and microservice architectures enable finer granularity and faster response to load changes compared to traditional and virtualized systems. Scalability is a key indicator of cloud system efficiency, as it directly affects availability, cost optimization and the ability of the system to respond to the dynamic requirements of modern applications.

Costs represent a key criterion in the comparative analysis of cloud architectures and refer to the total expenses associated with the implementation, maintenance and scaling of the system. In the cloud environment, the billing model based on actual consumption (pay-as-you-go) dominates, which enables the optimization of operating costs compared to traditional infrastructures with high capital investments (CAPEX). In a comparative analysis, serverless and cloud-native architectures often enable more efficient cost management thanks to automatic scaling and elimination of unused resources, while IaaS models can generate higher costs due to the need for more detailed resource management. Effective cost management requires continuous monitoring and optimization of consumption, especially in complex and distributed cloud environments.

Security represents one of the most critical criteria in the evaluation of cloud architectures and refers to the system's ability to protect data, applications and infrastructure from various threats and vulnerabilities. This criterion covers aspects such as authentication and authorization, encryption, data integrity, network security and access management. In a comparative analysis, different cloud models offer different levels of control and responsibility within the shared responsibility model, where the private cloud allows a higher level of control, while the public cloud provides advanced security mechanisms through standardized and automated services. Modern architectures, such as cloud-native and serverless models, integrate security through the principles of security-by-design and Zero Trust, but require careful configuration management to avoid vulnerabilities due to system complexity.

Complexity refers to the level of technical complexity in the design, implementation, and management of cloud architecture, including the number of components, system interdependencies, and required maintenance competencies. This criterion includes factors such as infrastructure configuration, service orchestration, integration of different technologies, and application lifecycle management. In a comparative analysis, traditional and monolithic architectures have a lower level of initial complexity, but limited flexibility, while cloud-native, container and multi-cloud architectures introduce significantly greater complexity due to their distributed nature and the need for automation. Although increased complexity enables greater scalability and agility, it requires advanced DevOps practices, standardization, and appropriate tools for effective system management.

IV. FUTURE RESEARCH DIRECTIONS

Autonomous cloud systems represent an advanced research direction in which cloud infrastructure and services have the ability to manage themselves without direct human intervention, relying on artificial intelligence and machine learning. These systems integrate functionalities such as self-configuration, self-optimization, self-healing and self-protection, thus achieving a high level of adaptability and resilience. In an evolutionary context, the autonomous cloud represents the next stage of development after automated and AI-assisted systems. In a comparative analysis, this approach promises a significant improvement in performance, reliability and efficiency of resource management, but at the same time it raises issues of transparency, control and ethical implications of decision-making without human supervision.

Optimization of serverless environments represents an important research direction aimed at improving performance, reducing latency and more efficiently managing costs in Function-as-a-Service (FaaS) models. Key challenges include minimization of cold start latency, optimization of function scheduling, as well as efficient resource management under dynamic and unpredictable load conditions. In an evolutionary context, the focus is shifting towards intelligent mechanisms that use predictive models to proactively scale and cache execution environments. In a comparative analysis, an optimized serverless architecture can achieve a high level of efficiency and scalability with minimal operating costs, but requires advanced management techniques and balancing between performance and resource consumption.

AI orchestration represents an advanced approach to managing cloud and distributed systems in which artificial intelligence is used for automatic coordination, deployment and optimization of resources and services. This concept integrates machine learning into orchestration processes (e.g. in container and microservices environments), enabling adaptive decision-making based on real-time data and historical patterns. In an evolutionary context, AI orchestration marks the transition from static and rule-driven systems to dynamic and self-learning platforms. In a comparative analysis, this approach enables improvement of performance, reliability and resource utilization, but introduces additional complexity in terms of model interpretability, data management and control over automated decisions. Artificial Intelligence of Things (AIoT) relies on a service-oriented IoT architecture and at the same time supports decentralized, dynamic management of large-scale AI. With AI control, in AIoT, every component of a product or cost of knowledge is AI-based.[6]

Quantum computing in the cloud represents an innovative direction that enables access to quantum processors via cloud infrastructure, which eliminates the need for expensive and complex local quantum equipment. This model allows researchers and organizations to experiment with quantum algorithms (e.g. for optimization, cryptography and simulations) using hybrid classical-quantum approaches. In the evolutionary context, the quantum cloud represents a potential disruptive phase of computing development, which can significantly change data processing paradigms. In a comparative analysis, although the technology is still at an early stage and faces limitations such as quantum bit errors and a limited number of qubits, its potential for solving complex problems exceeds the capabilities of classical cloud systems in specific domains. Vendors should try to allocate machine resources as efficiently as possible to improve system availability, while customers should try to use efficient resource allocation strategies to schedule jobs and maximize uptime. To achieve all of this, it is crucial to understand the characteristics of quantum job execution, as well as those on cloud machines.[7]

V. CONCLUSION

The paper provides a systematic overview of cloud computing architectures and their evolution. The results indicate that modern models, especially container and serverless approaches, offer significant advantages in terms of scalability and flexibility, but introduce new challenges in the area of security and system complexity. Future research should be directed towards the automation and sustainability of cloud environments.

Analysis of models, architectures and modern trends in cloud computing confirms that this paradigm represents the key foundation of the digital transformation of modern information systems. The evolution from traditional IT infrastructure, via virtualization, to cloud-native, container and serverless architectures indicates a continuous shift towards greater flexibility, automation and efficiency of resource management. At the same time, the development of different service models (IaaS, PaaS, SaaS) and implementation approaches (public, private, hybrid and multi-cloud) enables system adaptation to specific organizational and technological requirements.

Comparative analysis shows that the choice of optimal cloud architecture depends on the balance between performance, scalability, costs, security and complexity. Although modern architectures offer significant advantages over traditional systems, challenges such as vendor lock-in effect, security risks and resource management remain relevant and require careful strategic planning.

Contemporary trends, including edge computing, the application of artificial intelligence in the management of cloud environments and the concept of the green cloud, point to a further transformation towards intelligent, distributed and sustainable systems. Future research directions, such as autonomous cloud systems, AI orchestration and quantum computing in the cloud, open up new possibilities, but also new questions related to control, security and ethical implications. In conclusion, cloud computing continues to develop as a dynamic and complex field, whose further progress will depend on the ability to integrate innovation with reliable and sustainable architectural solutions.

REFERENCES

[1] S. Satpathy, B. Sahoo, and A. K. Turuk, “Sensing and actuation as a service delivery model in cloud edge centric internet of things,” *Future Generation Computer Systems*, vol. 86, pp. 281–296, 2018, doi: 10.1016/j.future.2018.04.015.

[2] N. Serrano, G. Gallardo, and J. Hernantes, “Infrastructure as a service and cloud technologies,” *IEEE Software*, vol. 32, no. 2, pp. 30–36, 2015, doi: 10.1109/MS.2015.43.

[3] D. Beimborn, T. Miletzki, and S. Wenzel, “Platform as a service (PaaS),” *Wirtschaftsinformatik*, vol. 53, no. 6, pp. 371–375, 2011, doi: 10.1007/s11576-011-0294-y.

[4] S. Saeed, Z. M. Zainal, F. A. Ghaleb, and B. A. S. Al-Rimy, “Enhancing public cloud resilience: An analytical review of detection and mitigation strategies against economic denial of sustainability attacks,” *Discover Internet of Things*, vol. 5, no. 1, p. 79, 2025, doi: 10.1007/s43926-025-00183-9.

[5] M. Gupta, D. Gupta, and P. Rai, "Exploring the impact of software as a service (SaaS) on human life," *EAI Endorsed Transactions on Internet of Things*, 2024, doi: 10.4108/eetiot.4821.

[6] A. Nadar and J. Härri, "An AI-as-a-service platform for an artificial intelligence of things (AIoT)," in *Proc. IEEE 99th Vehicular Technology Conference (VTC2024-Spring)*, Jun. 2024, pp. 1–7, doi: 10.1109/VTC2024-Spring62846.2024.10683357.

[7] G. S. Ravi, K. N. Smith, P. Gokhale, and F. T. Chong, "Quantum computing in the cloud: Analyzing job and machine characteristics," in *Proc. IEEE Int. Symp. Workload Characterization (IISWC)*, Nov. 2021, pp. 39–50, doi: 10.1109/IISWC53511.2021.00015.

UDK 007.52:[65.012.4:005.334
DOI 10.7251/ZRSNG2526011R

Risk Management in AI-Assisted Clinical Trials: Regulatory and Ethical Dimensions

Filip Radonić, Singidunum University

Abstract – **The integration of artificial intelligence (AI) models into clinical trials has accelerated significantly over the past decade, offering substantial potential to optimise patient recruitment, endpoint analysis, and pharmacovigilance. However, this integration also introduces a complex web of regulatory and ethical risks that must be systematically managed. This paper examined the principal risk categories associated with AI deployment in clinical research, with particular focus on algorithmic bias, the erosion of informed consent through opaque decision-making, and the evolving regulatory landscape shaped by the EU AI Act (Regulation EU 2024/1689), the European Medicines Agency (EMA) Reflection Paper on AI, and the U.S. Food and Drug Administration (FDA) draft guidance on AI in drug development. A structured review of peer-reviewed literature and regulatory documents was conducted. The findings indicated that, while regulatory convergence between the FDA and EMA is advancing, significant gaps persist in practice concerning transparency, explainability, and equitable participant selection. The paper proposed a multi-layered risk governance framework that integrates lifecycle monitoring, ethics review, and human oversight as foundational components of responsible AI use in clinical trials.**

Keywords – Artificial intelligence; clinical trials; risk management; regulatory compliance; algorithmic bias; EU AI Act; informed consent; EMA; FDA

I. INTRODUCTION

Artificial intelligence (AI) models are transforming the design, execution, and monitoring of clinical trials. Sponsors now routinely employ machine learning (ML) algorithms for tasks ranging from patient recruitment and stratification to safety signal detection and adaptive trial design. The promise of AI in this domain is considerable: by processing large, heterogeneous datasets at a speed and scale that exceeds human capacity, AI models can accelerate drug development timelines and reduce per-trial costs. Yet this promise is inseparable from a set of profound regulatory and ethical risks that, if unaddressed, may compromise patient safety, the integrity of scientific evidence, and public trust in clinical research.

This paper examines the regulatory and ethical risk landscape associated with AI deployment in clinical trials. It draws on recent regulatory guidance from the U.S. Food and Drug Administration (FDA)[1][1] and the European Medicines Agency (EMA),[2][2] the EU Artificial Intelligence Act (AI Act),[3][3] and peer-reviewed literature on algorithmic bias and informed consent. The central argument is that effective risk management in AI-assisted clinical trials requires not only compliance with formal regulatory requirements, but also a proactive governance culture that embeds transparency, accountability, and equity into every phase of the AI lifecycle.

II. REGULATORY LANDSCAPE

The regulatory environment governing AI in clinical trials has evolved rapidly since 2023. The FDA's 2023 Discussion Paper on AI in drug development, revised in February 2025, acknowledged the value of AI models while emphasising data transparency, algorithm explainability, and verifiable model performance.[4][1] In January 2025, the FDA issued draft guidance titled "Considerations for the Use of Artificial Intelligence to Support Regulatory Decision-Making for Drug and Biological Products," introducing a risk-based credibility assessment framework requiring sponsors to establish and document the credibility of any AI model used in regulatory submissions.[5][16]

In parallel, the EMA published its Reflection Paper on AI in the Medicinal Product Lifecycle in September 2024, adopted by both the Committee for Human Medicinal Products (CHMP) and the Committee for Veterinary Medicinal Products (CVMP). The paper introduced the concepts of "high patient risk" and

[1]U.S. Food and Drug Administration, "Using Artificial Intelligence and Machine Learning in the Development of Drug and Biological Products: Discussion Paper and Request for Feedback" (May 2023, revised February 2025). U.S. Department of Health and Human Services.

[2]European Medicines Agency, "Reflection Paper on the Use of Artificial Intelligence (AI) in the Medicinal Product Lifecycle," EMA/CHMP/CVMP, adopted September 2024. Amsterdam: EMA.

[3]European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 12 July 2024.

[4]U.S. Food and Drug Administration, "Using Artificial Intelligence and Machine Learning in the Development of Drug and Biological Products: Discussion Paper and Request for Feedback" (May 2023, revised February 2025). U.S. Department of Health and Human Services.

[5]FDLI, "Regulating the Use of AI in Drug Development: Legal Challenges and Compliance Strategies," Food and Drug Law Institute, July 2025. Available at: https://www.fdli.org/2025/07/regulating-the-use-of-ai-in-drug-development/.

"high regulatory impact" to categorise AI applications by the severity of potential consequences, and mandated lifecycle governance, human oversight, and data integrity across all development stages.[6][2]

A landmark development occurred in January 2026, when the EMA and FDA jointly published ten guiding principles for good AI practice in the medicines lifecycle.[7][4] These non-binding principles emphasise a human-centric, risk-based approach, multidisciplinary expertise, and transparent model development. They represent the first concerted EU-US regulatory convergence on AI and are intended to underpin future binding guidance in both jurisdictions.

The EU AI Act (Regulation EU 2024/1689), which entered into force on 1 August 2024, constitutes the world's first comprehensive legal framework for AI. It adopts a risk-tiered approach, classifying AI systems into prohibited, high-risk, transparency-requiring, and general-purpose categories. AI systems used in clinical trials, including patient recruitment tools, clinical decision support software, endpoint adjudication systems, and synthetic control arm generators, are highly likely to be classified as high-risk under Annex III of the Act.[8][8] High-risk classification triggers extensive compliance obligations: comprehensive technical documentation, risk management plans, data governance aligned with the GDPR, transparency to deployers, human oversight mechanisms, and registration with EU competent authorities.[9][9]

Importantly, the AI Act intersects with, but does not replace, existing pharmaceutical and medical device regulations, including the EU Clinical Trials Regulation (No 536/2014), the Medical Device Regulation (EU 2017/745), and the GDPR. Navigating this overlapping regulatory framework represents a significant compliance challenge for trial sponsors, particularly those operating across multiple jurisdictions.[10][3]

III. ALGORITHMIC BIAS AS AN ETHICAL AND SCIENTIFIC RISK

Among the ethical risks posed by AI in clinical trials, algorithmic bias is perhaps the most pervasive and consequential. Bias in medical AI arises and compounds throughout the AI lifecycle: in data collection and labelling, in model architecture and training, in deployment settings, and in the interpretation of outputs.[11][6] The foundational principle that governs this risk is often described as "bias in, bias out", which captures how biases embedded in training data propagate into model outputs and, ultimately, into clinical decisions.

In the context of clinical trials, algorithmic bias manifests most acutely in patient selection and recruitment. AI-driven tools that analyse electronic health records (EHRs) or genomic databases may systematically under-recruit patients from minority ethnic groups, elderly populations, or those with lower socioeconomic status, either because these groups are underrepresented in training data, or because the model's optimization objective inadvertently encodes existing healthcare inequities.[12][7] When such biased tools are deployed at scale, they threaten the generalisability of trial findings and may expose already-marginalised populations to the dual harm of exclusion from trials and subsequent receipt of treatments validated on non-representative cohorts.

A widely cited demonstration of this risk was provided by Obermeyer et al. (2019), who showed that a commercially deployed healthcare algorithm assigned equal risk scores to Black and white patients despite Black patients being significantly sicker, because the model used healthcare costs as a proxy for medical need a variable that reflects historical patterns of racial discrimination in healthcare spending.[13][7] This finding illustrated that algorithmic bias can be implicit and structural rather than deliberate, making it especially difficult to detect without systematic fairness auditing.

Traditional ethical frameworks for clinical research, including the Nuremberg Code, the Declaration of Helsinki, the Belmont Report, and the CIOMS Guidelines, enumerate fair participant selection as a core principle. A qualitative study by Youssef et al. (2024), drawing on interviews with investigators in AI-based diabetic retinopathy screening trials, found that ensuring equitable participant selection was one of the most challenging ethical issues unique to AI clinical trials.[14][5] Traditional ethics review processes, designed for conventional research, may be ill-equipped to evaluate the fairness properties of ML models without specialist input from data scientists and ethicists.

Mitigation strategies include diverse dataset curation, algorithmic fairness audits prior to deployment, stratified performance evaluation across demographic subgroups, and continuous post-deployment monitoring. Both the EMA Reflection Paper and the FDA credibility assessment framework call for ongoing performance monitoring

[6]European Medicines Agency, "Reflection Paper on the Use of Artificial Intelligence (AI) in the Medicinal Product Lifecycle," EMA/CHMP/CVMP, adopted September 2024. Amsterdam: EMA.

[7]European Medicines Agency and U.S. Food and Drug Administration, "Ten Principles for Good Artificial Intelligence Practice in the Medicines Lifecycle," Joint EMA-FDA Statement, January 2026.

[8]Busch, F., Kather, J.N., and Johner, C., "Navigating the EU AI Act: Implications for Regulated Digital Medical Products," npj Digital Medicine 7 (2024): 210. doi:10.1038/s41746-024-01213-6.

[9]Advarra, "Understanding the Impact of the New EU Artificial Intelligence Act on Clinical Research," Advarra Blog, February 2025. Available at: https://www.advarra.com/blog/understanding-the-impact-of-the-new-eu-artificial-intelligence-act-on-clinical-research/.

[10]European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 12 July 2024.

[11]Cross, J.L., Choma, M.A., and Onofrey, J.A., "Bias in Medical AI: Implications for Clinical Decision-Making," PLOS Digital Health 3, no. 11 (2024): e0000651. doi:10.1371/journal.pdig.0000651.

[12]Obermeyer, Z., Powers, B., Vogeli, C., and Mullainathan, S., "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations," Science 366, no. 6464 (2019): 447-453. doi:10.1126/science.aax2342.

[13]Obermeyer, Z., Powers, B., Vogeli, C., and Mullainathan, S., "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations," Science 366, no. 6464 (2019): 447-453. doi:10.1126/science.aax2342.

[14]Youssef, A., et al., "Ethical Considerations in the Design and Conduct of Clinical Trials of Artificial Intelligence," JAMA Network Open 7, no. 9 (2024): e2432643. doi:10.1001/jamanetworkopen.2024.32643.

throughout the model lifecycle.[15][16][2][14] The AI Act further reinforces this by mandating incident reporting and post-market surveillance for high-risk AI systems.[17][3]

IV. INFORMED CONSENT AND THE EXPLAINABILITY PROBLEM

A second major ethical risk concerns the compatibility of AI-based decision-making with patients' right to informed consent. In clinical research, informed consent requires that participants understand the nature, purpose, risks, and foreseeable consequences of their participation. When AI models are involved in decisions about participant selection, treatment allocation, or safety monitoring, the question arises: can meaningful consent be obtained for decisions made, at least in part, by algorithms whose internal reasoning is not transparent?[18][13]

The "black box" problem refers to the inability of many high-performing AI models, particularly deep neural networks, to provide human-interpretable explanations for their outputs. Chan (2023) argued that physicians' use of black-box AI undermines their ethical duty to advise patients, because communicating an AI recommendation without being able to explain the reasoning behind it erodes patient understanding, autonomy, and dignity.[19][11] This argument has particular force in clinical trials, where participants occupy a vulnerable position and where the research-clinical boundary requires heightened ethical scrutiny.

The legal dimension of this problem is equally complex. Under European human rights instruments and patient rights law, the extent to which informed consent requires patient understanding of the AI's decision-making process remains contested. Cohen and Slottje (2024) concluded that the introduction of AI creates genuine uncertainty about disclosure obligations, particularly when AI systems generate recommendations that deviate from standard clinical guidelines without the physician being able to explain why.[20] [13]

Amann et al. (2020) provided a multidisciplinary framework for AI explainability in healthcare, distinguishing between interpretability (understanding the model's general structure) and explainability (understanding why a specific output was produced for a specific patient).[21][12] They argued that different stakeholders, including regulators, clinicians, and patients, require different levels and types of explanation, and that a one-size-fits-all approach is insufficient. The AI Act's transparency requirements for high-risk systems, which include clear instructions for use and disclosure of system limitations, provide a regulatory floor for explainability.[22][9] The GDPR's provisions on automated decision-making (Article 22) further require that data subjects be informed about the logic of automated decisions significantly affecting them and retain the right to obtain human review.[23][15]

V. MULTI-LAYERED RISK MANAGEMENT FRAMEWORK

Drawing on the regulatory and ethical analysis above, this paper proposes a multi-layered risk management framework for AI in clinical trials, structured around four interdependent pillars.

A. Pre-Deployment Risk Assessment

Before any AI model is deployed in a clinical trial, a structured credibility assessment should be conducted, aligned with the FDA's draft guidance and the EMA's Reflection Paper. This assessment should document: (1) the model's intended context of use; (2) the training, validation, and test datasets, including an explicit analysis of demographic representativeness; (3) performance metrics disaggregated by relevant subgroups; (4) potential failure modes and their patient safety consequences; and (5) the rationale for the chosen model complexity and any explainability trade-offs.[24][25]

B. Ethics Review and Consent Redesign

Institutional review boards (IRBs) and ethics committees should be equipped with multidisciplinary expertise to evaluate AI-specific ethical risks, including fairness audits and explainability assessments. Informed consent documents for AI-assisted trials should clearly disclose the role of AI in participant selection, the nature and limitations of algorithmic

[15]European Medicines Agency, "Reflection Paper on the Use of Artificial Intelligence (AI) in the Medicinal Product Lifecycle," EMA/CHMP/CVMP, adopted September 2024. Amsterdam: EMA.

[16]Chin, M.H., et al., "Guiding Principles to Address the Impact of Algorithm Bias on Racial and Ethnic Disparities in Health and Health Care," JAMA Network Open 6, no. 12 (2023): e2345050. doi:10.1001/jamanetworkopen.2023.45050.

[17]European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 12 July 2024.

[18]Cohen, I.G., and Slottje, A., "Artificial Intelligence and the Law of Informed Consent," in Research Handbook on Health, AI and the Law (Cheltenham: Edward Elgar Publishing, 2024), pp. 167-182.

[19]Chan, B., "Black-box Assisted Medical Decisions: AI Power vs. Ethical Physician Care," Medicine, Health Care and Philosophy 26, no. 3 (2023): 285-292. doi:10.1007/s11019-023-10153-z.

[20]Cohen, I.G., and Slottje, A., "Artificial Intelligence and the Law of Informed Consent," in Research Handbook on Health, AI and the Law (Cheltenham: Edward Elgar Publishing, 2024), pp. 167-182.

[21]Amann, J., et al., "Explainability for Artificial Intelligence in Healthcare: A Multidisciplinary Perspective," BMC Medical Informatics and Decision Making 20 (2020): 310. doi:10.1186/s12911-020-01332-6.

[22]Advarra, "Understanding the Impact of the New EU Artificial Intelligence Act on Clinical Research," Advarra Blog, February 2025. Available at: https://www.advarra.com/blog/understanding-the-impact-of-the-new-eu-artificial-intelligence-act-on-clinical-research/.

[23]Stibbe, "Legal Considerations for Artificial Intelligence in the Life Sciences Sector," Stibbe Publications and Insights, 2024. Available at: https://www.stibbe.com.

[24]European Medicines Agency and U.S. Food and Drug Administration, "Ten Principles for Good Artificial Intelligence Practice in the Medicines Lifecycle," Joint EMA-FDA Statement, January 2026.

[25]FDLI, "Regulating the Use of AI in Drug Development: Legal Challenges and Compliance Strategies," Food and Drug Law Institute, July 2025. Available at: https://www.fdli.org/2025/07/regulating-the-use-of-ai-in-drug-development/.

decision-making, patients' rights to human oversight, and any data uses beyond the immediate trial scope.[2627][5][13]

C. Lifecycle Monitoring and Governance

AI model performance must be continuously monitored throughout the trial and during post-authorisation surveillance. Model drift, changes in performance over time due to shifts in patient populations or clinical practice, represents a significant risk in long-running trials. Sponsors should establish documented procedures for detecting and responding to performance degradation, including pre-specified criteria for model retraining or suspension.[28][2] Human-in-the-loop mechanisms, whereby clinical experts retain ultimate decision-making authority over AI-generated recommendations, are a non-negotiable component of lifecycle governance.[29][10]

D. Regulatory Engagement and Documentation

Sponsors should engage proactively with regulatory authorities through FDA pre-submission meetings, EMA scientific advice, or qualification opinion procedures, to align on the credibility of AI models used in pivotal trials before submission. Comprehensive technical documentation, including model cards, data governance protocols, and change management logs, should be maintained throughout the trial lifecycle and be available for regulatory inspection.[3031][9][8]

VI. CONCLUSION

AI models hold genuine transformative potential for clinical trial design and execution. However, this potential can only be responsibly realised if the regulatory and ethical risks associated with AI deployment are rigorously and proactively managed. This paper has identified algorithmic bias and the erosion of meaningful informed consent as the two most pressing ethical risks, and has shown how the evolving regulatory frameworks of the FDA, EMA, and EU AI Act are progressively addressing, though not yet fully resolving, these challenges.

The multi-layered risk management framework proposed here, spanning pre-deployment assessment, ethics review and consent redesign, lifecycle monitoring, and regulatory engagement, offers a practical architecture for sponsors, investigators, and regulators seeking to embed responsible AI governance into clinical research practice. As the FDA-EMA joint principles of January 2026 affirm, international regulatory convergence on AI in drug development is both necessary and underway.[32][4] The responsibility now lies with the research community to translate these principles into operational governance that places patient safety and scientific integrity at the centre of the AI clinical trial enterprise.

REFERENCES

[1] U.S. Food and Drug Administration, "Using Artificial Intelligence and Machine Learning in the Development of Drug and Biological Products," Discussion Paper, May 2023, revised February 2025.

[2] European Medicines Agency, "Reflection Paper on the Use of Artificial Intelligence (AI) in the Medicinal Product Lifecycle," EMA/CHMP/CVMP, September 2024.

[3] European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 12 July 2024.

[4] European Medicines Agency and U.S. Food and Drug Administration, "Ten Principles for Good Artificial Intelligence Practice in the Medicines Lifecycle," Joint EMA-FDA Statement, January 2026.

[5] Youssef, A., et al., "Ethical Considerations in the Design and Conduct of Clinical Trials of Artificial Intelligence," JAMA Network Open 7, no. 9 (2024): e2432643.

[6] Cross, J.L., Choma, M.A., Onofrey, J.A., "Bias in Medical AI: Implications for Clinical Decision-Making," PLOS Digital Health 3, no. 11 (2024): e0000651.

[7] Obermeyer, Z., Powers, B., Vogeli, C., Mullainathan, S., "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations," Science 366, no. 6464 (2019): 447-453.

[8] Busch, F., Kather, J.N., Johner, C., "Navigating the EU AI Act: Implications for Regulated Digital Medical Products," npj Digital Medicine 7 (2024): 210.

[9] Advarra, "Understanding the Impact of the New EU Artificial Intelligence Act on Clinical Research," Advarra Blog, February 2025.

[10] Goktas, P., et al., "Shaping the Future of Healthcare: Ethical Clinical Challenges and Pathways to Trustworthy AI," PMC11900311, February 2025.

[11] Chan, B., "Black-box Assisted Medical Decisions: AI Power vs. Ethical Physician Care," Medicine, Health Care and Philosophy 26, no. 3 (2023): 285-292.

[12] Amann, J., et al., "Explainability for Artificial Intelligence in Healthcare: A Multidisciplinary Perspective," BMC Medical Informatics and Decision Making 20 (2020): 310.

[13] Cohen, I.G., Slottje, A., "Artificial Intelligence and the Law of Informed Consent," in Research Handbook on Health, AI and the Law. Edward Elgar Publishing, 2024, pp. 167-182.

[14] Chin, M.H., et al., "Guiding Principles to Address the Impact of Algorithm Bias on Racial and Ethnic Disparities in Health and Health Care," JAMA Network Open 6 (2023): e2345050.

[15] Stibbe, "Legal Considerations for Artificial Intelligence in the Life Sciences Sector," Stibbe Publications and Insights, 2024.

[16] FDLI, "Regulating the Use of AI in Drug Development: Legal Challenges and Compliance Strategies," Food and Drug Law Institute, July 2025.

[26]Youssef, A., et al., "Ethical Considerations in the Design and Conduct of Clinical Trials of Artificial Intelligence," JAMA Network Open 7, no. 9 (2024): e2432643. doi:10.1001/jamanetworkopen.2024.32643.

[27]Cohen, I.G., and Slottje, A., "Artificial Intelligence and the Law of Informed Consent," in Research Handbook on Health, AI and the Law (Cheltenham: Edward Elgar Publishing, 2024), pp. 167-182.

[28]European Medicines Agency, "Reflection Paper on the Use of Artificial Intelligence (AI) in the Medicinal Product Lifecycle," EMA/CHMP/CVMP, adopted September 2024. Amsterdam: EMA.

[29]Goktas, P., et al., "Shaping the Future of Healthcare: Ethical Clinical Challenges and Pathways to Trustworthy AI," Frontiers/PMC, PMC11900311, February 2025.

[30]Advarra, "Understanding the Impact of the New EU Artificial Intelligence Act on Clinical Research," Advarra Blog, February 2025. Available at: https://www.advarra.com/blog/understanding-the-impact-of-the-new-eu-artificial-intelligence-act-on-clinical-research/.

[31]Busch, F., Kather, J.N., and Johner, C., "Navigating the EU AI Act: Implications for Regulated Digital Medical Products," npj Digital Medicine 7 (2024): 210. doi:10.1038/s41746-024-01213-6.

[32]European Medicines Agency and U.S. Food and Drug Administration, "Ten Principles for Good Artificial Intelligence Practice in the Medicines Lifecycle," Joint EMA-FDA Statement, January 2026.

UDK 340.137(497.6):007.52(497.6RS)
DOI 10.7251/ZRSNG2526015S

Pravo i etika u primeni veštačke inteligencije pri selekciji kandidata za zapošljavanje u javnom sektoru Republike Srpske sa osvrtom na nivo BiH

Law and Ethics in the Application of Artificial Intelligence in the Selection of Job Candidates in the Public Sector of the Republic of Srpska, with Reference to the Level of Bosnia and Herzegovina

Željko Stevanović, Ministarstvo odbrane, OS BiH

***Sažetak*— Javna uprava Republike Srpske i institucije Bosne i Hercegovine suočavaju se sa imperativom modernizacije. Svedoci smo sve veće primene veštačke inteligencije (AI) u svim sektorima pa tako i upotreba iste u selekciji kadrova, što obećava eliminaciju subjektivizma ali istovremeno otvara kompleksna pitanja pravne sigurnosti. Savremena javna uprava teži digitalizaciji kao sredstvu za postizanje veće efikasnosti i objektivnosti. Uvođenjem sistema veštačke inteligencije u procese selekcije kandidata, promoviše se kao rešenje za eliminaciju ljudske pristrasnosti i nepotizma. Ovaj rad istražuje i drugu stranu a koja se odnosi na rizik da AI postane takozvani digitalni paravan za netransparentne odluke. Osnovni problem leži u koliziji između automatizovanog odlučivanja i ustavnih prava građana na jednak pristup javnim funkcijama. Rad analizira neophodnost usklađivanja domaćeg zakonodavstva sa Evropskom unijom AI Act-om i postavljanje etičkih brana koje će osigurati da tehnologija služi meritokratiji a ne da je obesmišljava.**

***Ključne riječi* – veštačka inteligencija, digitalizacija, automatizovano odlučivanje, sistem**

Abstract –The public administration of the Republic of Srpska and the institutions of Bosnia and Herzegovina are facing an imperative for modernization. We are witnessing an increasing use of artificial intelligence (AI) across all sectors, including its application in candidate selection processes, which promises the elimination of subjectivity while simultaneously raising complex issues of legal certainty. Modern public administration strives for digitalization as a means of achieving greater efficiency and objectivity. The introduction of artificial intelligence systems into candidate selection processes is promoted as a solution for eliminating human bias and nepotism. However, this paper also explores the other side, referring to the risk that AI may become a so-called digital façade for non-transparent decision-making. The core problem lies in the conflict between automated decision-making and the constitutional rights of citizens to equal access to public positions. The paper analyzes the necessity of harmonizing domestic legislation with the European Union's AI Act and establishing ethical safeguards to ensure that technology serves meritocracy rather than undermining it.

***Keywords* –artificial intelligence, digitalization, automated decision-making, system**

I. UVOD

Savremena javna uprava u Republici Srpskoj i Bosni i Hercegovini nalazi se na prekretnici između tradicionalnog birokratskog aparata i imperativa digitalne transformacije. Uvođenje sistema veštačke inteligencije (AI) [6] u procese selekcije i zapošljavanja kadrova (tzv. Algorithmic Recruitment) promoviše se kao tehnološki superiorno rešenje namenjeno objektivizaciji procesa i eliminaciji ljudske pristrasnosti, nepotizma i političkog uticaja. Međutim, dok tehnologija nudi brzinu i analitičku dubinu, ona istovremeno otvara kompleksna pravna i etička pitanja koja duboko zadiru u temelje upravnog prava i ljudskih prava.

Osnovni naučni problem koji ovaj rad istražuje jeste očuvanje principa meritokratije u uslovima automatizovanog odlučivanja [7]. U pravnom sistemu koji počiva na ustavnom pravu građana na jednak pristup javnim funkcijama pod jednakim uslovima, upotreba netransparentnih algoritama — poznatih kao sistemi „crne kutije" (eng. Black Box) — predstavlja direktan izazov za načelo pravne sigurnosti. Ako u konkursnoj proceduri kandidat ne može da „dokuči" logiku iza odluke kojom je eliminisan, pravo na efikasan pravni lek i obrazloženu upravnu odluku postaje tek deklaratorna kategorija.

Dodatno, rad analizira etičku dimenziju algoritamske pristrasnosti. Postoji opravdan rizik da AI sistemi, učeći na istorijski kontaminiranim podacima, nesvesno perpetuiraju postojeće obrasce diskriminacije, dajući im pri tome privid naučne nepogrešivosti [1]. U ambijentu gdje su konkursne

procedure često predmet javne kritike i sumnje u njihovu ispravnost, veštačka inteligencija može postati ili najmoćnije oružje u borbi za integritet institucija ili najsofisticiraniji paravan za prikrivanje institucionalne nepravde [8].

Fokus rada biće usmeren na nužnost harmonizacije domaćeg zakonodavstva sa najnovijim evropskim standardima, prvenstveno Aktom o veštačkoj inteligenciji Evropske unije (EU AI Act) [5], koji sisteme u zapošljavanju svrstava u kategoriju visokog rizika. Cilj je ponuditi regulatorni okvir koji će osigurati da „vladavina algoritama“ nikada ne nadvlada vladavinu prava, te da tehnologija ostane u službi najkvalitetnijih kadrova, a ne sredstvo njihove automatizovane marginalizacije.

II. EVROPSKI REGULATIVNI OKVIR EU AI ACT KAO IMPERATIV HARMONIZACIJE

Evropski regulatorni okvir postavljen kroz Akt o veštačkoj inteligenciji (EU AI Act) predstavlja prekretnicu u globalnom pravnom poretku, ali i neizbežnu obavezu za Bosnu i Hercegovinu u okviru procesa pridruživanja Evropskoj uniji. Ovaj pravni akt uvodi strogu podelu sistema veštačke inteligencije prema nivou rizika koji generišu, pri čemu su sistemi namenjeni zapošljavanju, oceni kandidata i donošenju odluka o napredovanju u karijeri eksplicitno klasifikovani kao sistemi visokog rizika. Ovakva klasifikacija proizlazi iz činjenice da algoritamske greške u ovoj oblasti mogu dovesti do trajne povrede ljudskih prava i ekonomske marginalizacije pojedinca.

Za zakonodavstvo Republike Srpske, imperativ harmonizacije sa ovim Aktom podrazumeva napuštanje dosadašnje pasivnosti i uvođenje rigoroznih tehničkih standarda prije nego što bilo koji automatizovani sistem postane dio konkursne procedure. EU AI Act nalaže da visokorizični sistemi moraju biti dizajnirani na način koji osigurava njihovu „objašnjivost“, što u praksi znači da rešenje o izboru kandidata mora sadržavati logičku argumentaciju koju je proizveo algoritam, a koju pravni stručnjak može validirati.

Poseban akcenat u procesu harmonizacije mora biti stavljen na uspostavljanje sistema upravljanja podacima koji se koriste za obuku algoritama. Prema evropskim standardima, podaci moraju biti relevantni i reprezentativni kako bi se spriječila automatizovana diskriminacija. U kontekstu BiH, ovo je posebno osetljivo pitanje zbog ustavnih obaveza o ravnopravnoj zastupljenosti i zabrani diskriminacije po bilo kom osnovu. Harmonizacija takođe zahteva implementaciju člana 14. Akta, koji propisuje obavezan ljudski nadzor. To znači da institucije u Republici Srpskoj ne mogu delegirati suvereno pravo odlučivanja softveru, već on mora služiti isključivo kao alat koji olakšava rad konkursnim komisijama, uz obavezno postojanje mehanizma kojim fizičko lice može poništiti algoritamski rezultat ukoliko on nije u skladu sa zakonskim i etičkim normama.

Osim tehničkih aspekata, imperativ harmonizacije uključuje i uvođenje strogih kaznenih odredbi za zloupotrebu AI sistema u javnom sektoru. Akt o veštačkoj inteligenciji predviđa visoke novčane kazne, ali za domaći pravni sistem još je važnije uvođenje instituta „algoritamske odgovornosti“ donosilaca odluka. Bez usklađivanja domaćih zakona o državnoj upravi sa ovim standardima, Republika Srpska i BiH rizikuju da stvore digitalni sistem koji je pravno neusklađen sa evropskim prostorom, čime bi se dodatno otežao proces integracija i narušila pravna sigurnost građana. Harmonizacija, dakle, nije samo administrativna obaveza, već suštinska zaštita meritokratskog principa od netransparentne tehnokratije.

III. USTAVNOPRAVNI ASPEKT I PRISTUP JAVNOJ UPRAVI RS I BIH

Ustavnopravni aspekt upotrebe veštačke inteligencije u selekciji kadrova unutar javne uprave Republike Srpske i Bosne i Hercegovine duboko je ukorenjen u zaštiti osnovnih ljudskih prava i sloboda, prvenstveno prava na rad i ravnopravnog pristupa javnim funkcijama. Ustavi oba entiteta, kao i Ustav BiH, proklamuju princip nediskriminacije kao vrhovni postulat pravnog poretka. Kada se u proces odlučivanja uvede algoritam, postavlja se fundamentalno pitanje: da li mašina može garantovati ustavno pravo na „jednake uslove“ ako je njena logika procesiranja podataka nedostupna javnosti? [4] Ustavna garancija prava na rad ne podrazumeva samo pravo na zaposlenje, već i pravo na pravičan i zakonit proces selekcije.

Ukoliko AI sistem koristi parametre koji nisu eksplicitno navedeni u zakonu ili konkursu, on vrši tihu eroziju ustavnosti, uvodeći arbitrarnost tamo gdje mora vladati isključivo norma. Pristup javnoj upravi u Republici Srpskoj zakonski je definisan kao meritokratski proces, ali ustavna sudska praksa nalaže da svaka odluka organa vlasti mora biti podložna proveri. Ovde se javlja kolizija između tehnološke efikasnosti i prava na žalbu kao ustavne kategorije. Ako kandidat ne može da ospori odluku algoritma jer mu je uskraćeno razumevanje načina na koji je softver vrednovao njegove kvalifikacije, dolazi do povrede prava na pravično suđenje i efikasan pravni lek. Ustavni sudovi bi u ovakvim slučajevima morali stati na stranu pojedinca, jer se suverenitet odlučivanja u javnom sektoru ne može preneti na privatni softver bez jasnog ustavnog ovlaštenja i mehanizama ljudske kontrole. Institucionalna pravda nalaže da tehnologija bude instrument koji olakšava ostvarivanje prava, a ne barijera koja kandidata ostavlja u sferi pravne nesigurnosti.

Dodatni izazov predstavlja ustavni princip proporcionalnosti. Upotreba invazivnih AI alata, poput analize mikromimike tokom intervjua ili dubinskog skeniranja digitalnog otiska kandidata, može predstavljati nesrazmeran zahvat u pravo na privatnost.

U Republici Srpskoj i BiH, gdje je poverenje u institucije često poljuljano spornim konkursnim procedurama, ustavnopravna zaštita mora biti proaktivna. To podrazumeva da se pristup javnoj upravi mora zaštititi od „tehničkog formalizma“ koji bi mogao služiti za prikrivanje diskriminacije na osnovu političkog mišljenja ili socijalnog porekla, što su kategorije koje AI može veoma lako kvantifikovati kroz indirektne podatke. Ustavni okvir BiH i Republike Srpske zahtijeva da svaki tehnološki napredak u

administraciji bude podređen ljudskom dostojanstvu i principu zakonitosti, osiguravajući da najkvaliteniji kadar svoje mesto u sistemu dobiju na osnovu merljivih zasluga, a ne na osnovu netransparentnih algoritamskih proračuna.

IV. NEPRISTRASNOST I ALGORITAMSKA PRAVIČNOST

Koncept nepristrasnosti u javnom sektoru Republike Srpske i Bosne i Hercegovine tradicionalno se vezuje za subjektivni integritet članova konkursnih komisija, međutim, uvođenjem veštačke inteligencije, težište se pomera ka fenomenu algoritamske pravičnosti. Postoji duboko ukorenjena zabluda da su algoritmi inherentno neutralni jer operišu sa brojevima, a ne sa emocijama ili interesima. Ipak, naučna praksa pokazuje da AI sistemi mogu postati instrumenti „automatizovane nepravde“ ukoliko su podaci na kojima uče (training data) opterećeni istorijskim predrasudama ili sistemskim manjkavostima društva. U kontekstu našeg podnevlja, gde su konkursne procedure često bile izložene kritikama zbog netransparentnosti, algoritamska pravičnost nalaže da se svaki softverski model mora podvrgnuti rigoroznom testiranju na pristrasnost pre nego što mu se poveri selekcija ljudskih sudbina. Pravičnost ovde ne znači samo odsustvo direktne diskriminacije, već i osiguranje da indirektni korelati — kao što su mesto stanovanja, naziv fakulteta ili dužina studiranja — ne postanu prikriveni eliminatorni faktori koji produbljuju socijalni jaz.

Algoritamska pravičnost zahteva implementaciju principa distribuirane pravde, gde sistem mora osigurati jednak tretman za slične kandidate. U Bosni i Hercegovini, ovo pitanje dobija i dodatnu ustavnu dimenziju u pogledu ravnopravne zastupljenosti konstitutivnih naroda i ostalih građana [13]. Ako bi algoritam bio programiran da favorizuje određene obrasce ponašanja ili specifične rečnike koji su dominantni samo u jednoj društvenoj grupi, on bi de facto vršio diskriminaciju pod paravanom „tehničke optimizacije“. Nepristrasnost sistema, dakle, nije statično stanje, već dinamički proces koji zahteva stalnu reviziju (algorithmic auditing). Institucije u Republici Srpskoj ne smu prihvatiti rešenja „ključ u ruke“ od stranih dobavljača bez prethodne kalibracije softvera prema lokalnim pravnim i etičkim standardima [9].

Etički integritet procesa selekcije zavisi od mogućnosti da se algoritamska odluka ospori sa stanovišta ljudske pravičnosti. Veštačka inteligencija teži statističkom proseku i često ne prepoznaje izuzetnost pojedinca čiji profil može odudarati od „standardno uspešnog“ kandidata kojeg je mašina naučila da prepoznaje [12]. Zbog toga, algoritamska pravičnost u javnom sektoru BiH mora biti dopunjena obaveznim ljudskim korektivom. Pravo na nepristrasan postupak podrazumeva da tehnologija služi kao filter za eliminaciju subjektivizma, a ne kao neprobojni zid koji onemogućava prepoznavanje istinskog kvaliteta i meritornosti. Samo kroz simbiozu matematičke logike i pravničke etike moguće je izgraditi sistem u kojem će digitalizacija biti garant, a ne „grobar“ institucionalne pravde [14].

V. ALGORITAMSKI MENADŽMENT KAO PARAVAN ZA INSTITUCIONALNU NEPRAVDU

Uvođenje algoritamskog menadžmenta u procese selekcije kadrova u javnom sektoru Republike Srpske i Bosne i Hercegovine nosi sa sobom latentnu opasnost da tehnologija, umesto garanta meritokratije, postane sofisticiran paravan za održavanje i produbljivanje institucionalne nepravde. U pravnom sistemu koji se još uvek bori sa visokim stepenom diskrecionog odlučivanja i političkog uticaja na zapošljavanje, automatizacija procesa može poslužiti kao sredstvo za "pranje" nelegalnih odluka kroz privid tehničke nepogrešivosti. Na taj način, tradicionalna zloupotreba položaja članova konkursnih komisija biva zamenjena tehnokratskim determinizmom, gdje se iza kompleksnih matematičkih operacija krije svesna namera da se favorizuje kandidat koji ne ispunjava zakonske ili stručne kriterijume.

Ovakav scenario stvara opasnu pravnu prazninu u kojoj se odgovornost za kršenje konkursnih procedura disperzuje sa donosilaca odluka na softversko rešenje, čime se direktno podriva pravo kandidata na pravni lijek i sudsku zaštitu. Kada algoritamski sistem generiše rang-listu na osnovu netransparentnih parametara, on zapravo onemogućava relevantne faktore, uključujući sudsku vlast i resorna ministarstva, da izvrše adekvatan nadzor nad zakonitošću procesa. Institucionalna nepravda se ovdje manifestuje kroz "crnu kutiju" odlučivanja, gdje se svaki prigovor na neregularnost odbacuje argumentom objektivnosti mašine, dok se u pozadini zadržava stari obrazac ignorisanja zakonskih normi u korist podobnosti [10].

Takva praksa ne samo da kompromituje integritet javne službe, već obesmišljava samu suštinu vladavine prava, pretvarajući modernizaciju uprave u puki dekor za nastavak sistemske diskriminacije i kršenje etičkih postulata struke.

VI. SISTEM ODGOVORNOSTI I MEHANIZAM PRAVNE ZAŠTITE

Uspostavljanje jasnog sistema odgovornosti i efikasnih mehanizama zaštite prava kandidata u procesima selekcije putem veštačke inteligencije predstavlja ultimativni izazov za pravni poredak Republike Srpske i Bosne i Hercegovine. Postojeći zakonski okvir, primarno oslonjen na Zakon o opštem upravnom postupku i zakone o državnim službenicima [2],[3] nije projektovan za situacije u kojima algoritamski entiteti postaju ključni faktori odlučivanja. Stoga se odgovornost ne smije završiti na pukoj tehničkoj ispravnosti softvera, već mora biti locirana u sferi institucionalnog subjektiviteta – onoga ko je takav sistem odobrio, implementirao i nadzirao [15], [16].

Mehanizam zaštite u ovakvom kontekstu zahteva evoluciju prava na obrazloženje odluke, koje u digitalnom dobu podrazumeva obavezu institucije da na razumljiv način prezentuje logiku algoritamskog rangiranja [10], [11]. Ukoliko kandidat, uprkos ispunjavanju svih zakonskih i stručnih kriterijuma, biva eliminisan netransparentnim procesom, pasivnost nadležnih faktora, poput resornih ministarstava ili sudskih instanci, predstavlja direktno saučesništvo u

institucionalnoj nepravdi. Efikasna zaštita podrazumeva pravo na ljudsku intervenciju i reviziju svake automatizovane odluke, čime se sprečava da tehnologija postane nepremostiva barijera za sudsku kontrolu zakonitosti konkursa.

Bez rigoroznih kontrolnih mehanizama koji bi omogućili sankcionisanje odgovornih lica u slučajevima kada AI služi za prikrivanje diskriminacije, pravna sigurnost građana ostaje samo deklarativna kategorija. Tek kroz strogo definisanu hijerarhiju odgovornosti, od ministra pravde do članova konkursnih komisija, veštačka inteligencija može biti transformisana iz potencijalnog alata nepravde u instrument objektivnosti, pod uslovom da svaki njen korak ostane podložan beskompromisnoj pravnoj i etičkoj proveri.

VII. ZAKLJUČAK

Dosadašnja analiza nedvosmisleno ukazuje na to da implementacija veštačke inteligencije u procese selekcije u javnom sektoru Republike Srpske i Bosne i Hercegovine ne sme biti posmatrana isključivo kao tehničko unapređenje, već kao prvorazredno pravno i etičko pitanje. Da bi se izbeglo pretvaranje algoritama u digitalne paravane za institucionalnu nepravdu, neophodna je hitna reforma zakonodavstva koja će jasno definisati pojam algoritamske odgovornosti. Ključni pravni prijedlozi moraju uključivati obavezu uvođenja "objašnjive veštačke inteligencije" (XAI) u sve javne konkurse, čime bi se osiguralo pravo kandidata na transparentno obrazloženje svake faze procesa.

Pored toga, neophodno je uspostaviti nezavisni mehanizam eksterne revizije algoritama koji bi periodično proveravao prisustvo diskriminatornih obrazaca u bazi podataka. Pravo na ljudski nadzor i obaveznu intervenciju nadležnih komisija mora ostati neotuđivo, kako bi se spriječilo da mašinska odluka postane konačna bez mogućnosti efikasne sudske kontrole. Samo kroz sinergiju stroge pravne regulative, koja predviđa ličnu odgovornost donosilaca odluka – od članova komisija do resornih ministara – i visokoetno postavljenih tehnoloških standarda, moguće je vratiti poverenje u meritokratiju i vladavinu prava. Uvođenje veštačke inteligencije treba da služi eliminaciji korupcije, a ne njenom sofisticiranom prikrivanju, čime bi se konačno osiguralo da najbolji kandidati, bez obzira na institucionalne pritiske, zauzmu mesta koja im po zakonu i struci pripadaju.

LITERATURA

[1] Zakon o zabrani diskriminacije Bosne i Hercegovine ("Službeni glasnik BiH", br. 59/09 i 66/16).

[2] Zakon o državnim službenicima Republike Srpske ("Službeni glasnik Republike Srpske", br. 118/08, 117/11, 37/12 i 57/16).

[3] Zakon o opštem upravnom postupku Republike Srpske ("Službeni glasnik Republike Srpske", br. 13/02, 87/07, 50/10 i 66/18).

[4] Zakon o zaštiti ličnih podataka BiH ("Službeni glasnik BiH", br. 49/06, 76/11 i 89/11).

[5] Uredba EU o vještačkoj inteligenciji (EU AI Act, 2024) – ključni dokument koji klasifikuje sisteme zapošljavanja kao "visokorizične".

[6] Etičke smjernice za pouzdanu vještačku inteligenciju (HLEG AI, Evropska komisija, 2019).

[7] Opšta uredba o zaštiti podataka (GDPR) – u kontekstu prava na objašnjenje automatizovanog odlučivanja (Član 22).

[8] Civitarese Matteucci, S. (2021). Public Administration Algorithm Decision-Making and the Rule of Law, European Public Law.

[9] Alon-Barkat, S. & Busuioc, M. (2023). Human–AI Interactions in Public Sector Decision Making: “Automation Bias” and “Selective Adherence”.

[10] Akter, S., et al. (2021). Algorithmic bias in data-driven innovation in the age of AI, International Journal of Information Management.

[11] Zbornici radova i priručnici: Vodič o radnim i digitalnim pravima u Bosni i Hercegovini (UG "Nešto više", 2023).

[12] Službeni sajt Agencije za državnu upravu RS / ADU BiH: Za analizu postojećih pravilnika o konkursnim procedurama.

[13] Portal pravosudje.ba: Za pristup sudskoj praksi u vezi sa diskriminacijom pri zapošljavanju.

[14] Evropski parlament (europarl.europa.eu): Dokumentacija o implementaciji AI Act-a.

[15] Forbes / N1 Info (BiH sekcija): Analize uticaja AI Act-a na lokalne firme i javni sektor u 2024. i 2025. godini.

[16] Fondacija Konrad Adenauer (KAS): Analize o budućnosti poslovanja i AI u BiH.

UDK 005.334:001.101(4-672EU)
DOI 10.7251/ZRSNG2526019P

Evolutionary Paradigms in University Knowledge Management: A Comparative Analysis of Intent-Based Architectures and Vectorized Semantic Retrieval

Bojan Papaz, Singidunum University, Miloš Mravik, Singidunum University

***Abstract* - This research examines the transition of conversational artificial intelligence within higher education administrative systems, specifically focusing on the shift from traditional intent-based architectures to vectorized semantic retrieval models. By analyzing the current implementation at Singidunum University, which utilizes the Rasa framework and a Dual Intent and Entity Transformer (DIET) pipeline, the study identifies a "knowledge bottleneck" when dealing with unstructured regulatory corpora. The investigation compares this deterministic model with emerging vector database technologies such as Pinecone and Weaviate, which employ high-dimensional embeddings and Cosine Similarity to retrieve information based on semantic proximity. The results suggest that while intent-based systems provide high precision for frequent queries, a hybrid model incorporating Retrieval-Augmented Generation (RAG) is essential for navigating complex institutional statutes.**

Keywords - Artificial Intelligence; Vector Databases; Knowledge Management; Natural Language Understanding; Higher Education Administration

I. INTRODUCTION

The global landscape of higher education is undergoing a profound digital transformation, necessitated by the increasing complexity of administrative regulations and the rising expectations of a digitally native student population. Conversational artificial intelligence has moved beyond the role of simple automated responders, evolving into sophisticated administrative ecosystems that must navigate intricate legal frameworks.

The core challenge within these systems is effective knowledge management: the capacity to not only decipher the linguistic intent of a user query but to retrieve accurate, verified, and institutionally aligned information from a diverse array of sources. At institutions like Singidunum University, current implementations rely heavily on intent-based architectures where Natural Language Understanding (NLU) [1] models map student inquiries to predefined answers stored in structured databases and accessed via RESTful APIs.

While these systems demonstrate high precision for standard queries such as enrollment dates or tuition costs as they frequently encounter a "knowledge bottleneck" [2] when faced with the extensive, unstructured regulatory corpus of a modern university. This corpus includes statutes, rulebooks, and specialized regulations often trapped in static PDF formats, which are difficult for traditional intent-labeling systems to process. The limitations of such models have prompted an investigation into more flexible, semantic-driven retrieval systems utilizing vector databases like Pinecone [3] or Weaviate [4]. By representing regulatory text as high-dimensional vectors, these systems allow for retrieval based on the underlying meaning of a query rather than exact keyword matches, representing a significant shift in institutional digital strategies.

The following analysis evaluates the architectural foundations of existing systems, the mathematical theory behind vectorized retrieval, and the operational advantages of a hybrid model that combines deterministic reliability with exhaustive semantic depth.

II. METHODS OF ANALYSIS

The comparative analysis performed in this study was structured around the evaluation of two distinct knowledge management paradigms. The first is the existing intent-based architecture deployed at Singidunum University, which utilizes the Rasa framework [5] for message processing and dialogue management. [6] This system was analyzed based on its NLU pipeline configuration, specifically the use of the DIET [6,7] classifier and mBERT [7] embeddings. Performance was assessed through historical macro-F1 scores and the operational efficacy of the Rasa Action Server [8] in handling synchronous API requests [9] for structured Q&A content.

The second paradigm involves the proposed transition to a vectorized semantic retrieval model. This approach was evaluated by examining the technical requirements for document ingestion, chunking, and indexing of the university's regulatory corpus. The study reviewed several vector database candidates: Pinecone, Weaviate, and Qdrant [10]. comparing their latency, throughput, and support for hybrid search techniques. Furthermore, the research investigated the implementation of a Retrieval-Augmented Generation (RAG) pipeline, which utilizes a vector database to provide context to a Large Language Model (LLM) for generating natural language responses grounded in official statutes.

Data for the comparison was synthesized from technical documentation, university acts, and performance benchmarks associated with each architecture. The analysis also considered security and privacy [11] requirements, including compliance

with GDPR standards for data pseudonymization and the ethical implications of using generative AI in an administrative context. The goal was to establish a framework for a hybrid knowledge management system that maximizes accuracy while minimizing the frequency of system fallbacks during high-stress administrative periods, such as the June enrollment cycle.

III. RESULTS OF COMPARATIVE ANALYSIS

The investigation yielded detailed technical and operational insights into the two primary knowledge management models. The results are categorized into the mechanics of the current intent-based system, the mathematical and structural foundations of vectorized retrieval, and a technical comparison of their performance metrics. [12]

A. Architectural Foundations of Intent-Based Systems

The current system at Singidunum University is built on the Rasa framework, which provides a modular architecture for separating natural language understanding from dialogue logic. [6, 12] This system is specifically tuned for the Serbian language, which presents unique linguistic challenges such as complex morphology and the frequent omission of diacritics in informal digital communication.

The NLU pipeline utilizes a multi-layered approach to feature extraction. [13] Sparse features are generated using the CountVectorsFeaturizer, which processes words and character n-grams. The use of character-level n-grams (char_wb) is essential for maintaining robustness against typographical errors and the lack of Serbian diacritics (e.g., using "c" instead of "č" or "ć"). These sparse features are complemented by dense features from mBERT, which provide contextual embeddings that allow the system to differentiate between identical words used in different syntactic contexts. [14] The classification and entity extraction tasks are handled by the DIET model, a transformer-based architecture that learns both tasks simultaneously to improve overall accuracy. [15] This pipeline achieves macro-F1 scores above 0.85 for the 65 most common administrative intents. [16]

TABLE I. SUMMARY OF THE CURRENT ARCHITECTURAL STATE OF THE SINGIDUNUM ADMINISTRATIVE CHATBOT

ID	**Summary of the current architectural state**	
	Feature	***Current Intent-Based System Subhead***
1	NLU Model	DIETClassifier + mBERT
2	Language Support	Serbian (Robust to diacritics/lapsuses)
3	Knowledge Source	Structured Q&A API (Editorially controlled)
4	Dialogue Logic	RulePolicy + TEDPolicy
5	Latency (P50)	~180 ms (Warm cache)
6	Primary Limitation	Returns fallback for unmapped regulatory content

B. The Knowledge Bottleneck and Fallback Mechanism

Despite the precision of the DIET-based pipeline, the system faces a critical "knowledge bottleneck" because its operational success is binary: it can either answer a query for which an intent has been explicitly defined and trained, or it must trigger a fallback. A FallbackClassifier [17, 18] is employed to monitor the confidence scores of NLU predictions; if the score for the top intent falls below the 0.45 threshold, or if there is excessive ambiguity between two possible intents, the system defaults to a standard failure response. [17] While this prevents the delivery of incorrect information, it reveals a fundamental "wall" in the architecture: as the number of intents scales to accommodate the long-tail of university statutes, the system becomes computationally expensive to manage, and label correlation errors increase. [18]

This limitation is most evident when students inquire about specific regulatory articles sequestered in unstructured PDF documents, such as the Regulation on Conditions and Procedures for Student Enrollment or the Rulebook on Disciplinary Responsibility. Because the current structured Q&A API [9] typically contains only high-level, "pre-canned" summaries for frequently asked questions, it fails to retrieve the nuanced legal data required for specialized inquiries. Consequently, complex procedures such as the recognition of foreign qualifications or specific departmental operational protocols which often trigger fallbacks even though the information is legally defined within the university's internal documents. [19] Furthermore, the system is susceptible to "semantic drift," where the meaning of student queries shifts seasonally, often outpacing the manual and front-loaded effort required for administrative staff to update the intent-based model. This creates persistent information silos where the institution's official "source of truth" remains inaccessible to the automated agent.

C. Vectorized Semantic Retrieval and Mathematical Theory

To overcome the knowledge bottleneck, the research evaluated a paradigm shift toward vectorized semantic retrieval. In this model, the entire regulatory corpus is transformed into high-dimensional vectors, or embeddings, using deep learning models such as Sentence-Transformers. These embeddings place the text into a multi-dimensional space (typically 768 to 1536 dimensions) where the semantic relationship between different segments of text can be calculated mathematically. [20]

The primary metric for determining similarity in this space is Cosine Similarity [21], which measures the angle between a query vector and a document vector. The formula is expressed as follows:

$$similarity = \cos(\theta) = \frac{A \cdot B}{\| A \| \| B \|}$$

This approach is highly effective for institutional regulations because it prioritizes the thematic direction of the text over keyword frequency. A student's question about "transferring credits" can be semantically matched to a regulatory article about the "recognition of foreign degrees" even if the specific word "transfer" does not appear in the document.

D. Comparative Analysis of Vector Databases

The implementation of semantic retrieval requires a specialized database to store and query these high-dimensional vectors. The research analyzed three leading candidates for institutional deployment: Pinecone, Weaviate, and Qdrant. Pinecone is notable for its serverless architecture and low latency, making it ideal for high-traffic environments. Weaviate, however, offers superior flexibility for enterprise knowledge management through its support for hybrid search, which combines vector similarity with traditional keyword-based (BM25) search. This hybrid approach is particularly valuable for university regulations that contain specific article numbers or legal terms.

TABLE II. COMPARATIVE ANALYSIS OF VECTOR DATABASE CANDIDATES FOR INSTITUTIONAL DEPLOYMENT

Vector Database	**Comparative analysis of vector database candidates**	
	Key Advantages	***Operational Context***
Pinecone	Serverless, zero-ops, <50ms P95 latency	Fast-moving startups, rapid prototyping
Weaviate	Hybrid search, native multi-tenancy, GraphQL	Complex enterprise knowledge management
Qdrant	Rust-based, high throughput, in-memory speed	Real-time applications with custom infra

The technical performance comparison between the current intent-based API and the proposed vector database search reveals significant differences in throughput and accuracy for unmapped content. Vector search is optimized for scale, utilizing Approximate Nearest Neighbor (ANN) algorithms to find relevant matches among millions of documents in milliseconds.

TABLE III. TECHNICAL PERFORMANCE COMPARISON OF INTENT-BASED VS. VECTOR-BASED RETRIEVAL

Metric	**Technical performance comparison**	
	Intent-Based API (Current)	***Vector Database Search***
Query Time (P95)	~480 ms (Pipeline + API)	< 50-70 ms (Vector Lookup)
Throughput	Moderate (Rasa Action Server limited)	High (5,000 - 10,000 QPS)
Memory Usage	High (mBERT loading)	Efficient (Optimized vector stores)
Accuracy (Unmapped)	0% (Fallback)	~70-90% (Semantic Match)

E. Transitioning to a Hybrid Knowledge Management Model

The results indicate that the most effective strategy for university administration is a hybrid model that integrates the deterministic precision of intent-based APIs with the expansive coverage of vectorized retrieval. In this architecture, the intent-based system serves as the primary layer for high-confidence, frequently asked questions (FAQs). When the NLU confidence falls below the established threshold, the query is automatically routed to a Retrieval-Augmented Generation (RAG) pipeline.

In the RAG workflow, the vector database retrieves the most relevant passages from the university statutes. These passages are then provided as context to a generative LLM, which constructs a natural language response. This grounding ensures that the model's output is based strictly on institutional regulations, effectively eliminating the risk of hallucinations. Furthermore, the system can provide direct citations to the source material, such as "Article 15 of the Rulebook on Enrollment," thereby increasing transparency and student trust.

F. Operational Targets for Implementation

To ensure the success of the hybrid system, several operational targets have been established, focusing on uptime, accuracy, and user satisfaction. These targets reflect the rigorous requirements of educational administration, particularly during peak periods like the enrollment windows.

TABLE IV. OPERATIONAL TARGETS FOR THE HYBRID KNOWLEDGE MANAGEMENT SYSTEM

Metric	**Operational targets for the hybrid knowledge system**	
	Goal	***Implementation Strategy***
Uptime	99.9%	Cloud-native hosting with high availability
Hallucination Rate	< 5%	Vector-grounded responses with strict prompt engineering
Response Accuracy	> 92%	Hybrid search combining vector and keyword retrieval
User Satisfaction	> 8.0/10	Intuitive natural language interface with citations

IV. CONCLUSION OF THE STUDY

The comparative analysis of knowledge management models for higher education administration demonstrates that a hybrid approach is the most effective solution for bridging the gap between precision and comprehensive coverage. While intent-based architectures using DIET and mBERT provide a high level of accuracy for common administrative tasks, they are inherently limited by the need for explicit manual modeling. The integration of vectorized semantic retrieval through databases like Pinecone or Weaviate allows for the efficient processing of unstructured regulatory documents, effectively eliminating the current "knowledge bottleneck."

The implementation of a Retrieval-Augmented Generation pipeline ensures that AI-generated responses are grounded in the university's official statutes, meeting the high standards for accuracy, security, and ethics required in institutional governance. By leveraging these advanced retrieval techniques, universities can provide students with transparent, cited, and reliable information, even for complex and rare inquiries. This evolutionary shift not only improves the success rate of user queries but also significantly reduces the maintenance burden on administrative staff. Ultimately, the move toward a hybrid, semantic-driven model positions the university as a leader in digital transformation, ensuring that its "source of truth" remains accessible and effective in an increasingly complex educational environment.

ACKNOWLEDGEMENT

The authors express their gratitude to Singidunum University for providing the data and technical environment required for this comparative study. Support for this research was facilitated by the institutional commitment to digital transformation and the ongoing development of conversational AI systems for administrative support. Special thanks are extended to the administrative staff and technical teams whose work on the existing Rasa-based chatbot served as the foundational baseline for this analysis.

REFERENCES

[1] Rasa, “Tuning Your NLU Model,” 2025. [Online]. Available: https://legacy-docs-oss.rasa.com/docs/rasa/tuning-your-model/.

[2] X. L. D. Y. a. J. T. H. Chen, “A Survey on Dialogue Systems: Recent Advances and New Frontiers,” *ACM SIGKDD Explorations Newsletter,* vol. 19, pp. 25-35, 2017.

[3] P. Systems, “Pinecone Documentation,” 2025. [Online]. Available: https://docs.pinecone.io/.

[4] W. B.V., “Weaviate Documentation,” 2025. [Online]. Available: https://weaviate.io/developers/weaviate.

[5] Rasa, “Knowledge Base Actions,” 2025. [Online]. Available: https://rasa.com/docs/reference/integrations/action-server/knowledge-bases/.

[6] J. E. M. M. a. A. N. V. Vlasov, “Dialogue Transformers,” arXiv, 2019.

[7] J. Devlin, M.-W. Chang, K. Lee and K. Toutanova, “BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding,” arXiv / NAACL-HLT 2019, 2018-2019.

[8] Rasa, “Introduction to Rasa Action Server,” 2025. [Online]. Available: https://rasa.com/docs/action-server/.

[9] Rasa, “HTTP API,” 2025. [Online]. Available: https://legacy-docs-oss.rasa.com/docs/rasa/reference/http-api/.

[10] Qdrant, “Qdrant Documentation,” 2025. [Online]. Available: https://qdrant.tech/documentation/.

[11] R. Kamp and N. Weinbaum, “The myth of anonymization: Why AI needs a new privacy paradigm,” 26 March 2025. [Online]. Available: https://iapp.org/news/a/the-myth-of-anonymization-why-ai-needs-a-new-privacy-paradigm.

[12] s.-l. developers, “sklearn.feature_extraction.text.CountVectorizer — parametar analyzer,” 2023. [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.feature_extraction.text.CountVectorizer.html.

[13] J. F. N. P. a. A. N. T. Bocklisch, “Rasa: Open Source Language Understanding and Dialogue Management,” 15 December 2017. [Online]. Available: https://arxiv.org/abs/1712.05181.

[14] H. Face, “bert-base-multilingual-cased - model card,” 2024. [Online]. Available: https://huggingface.co/google-bert/bert-base-multilingual-cased.

[15] Rasa, “Custom Actions,” [Online]. Available: https://rasa.com/docs/reference/primitives/custom-actions/.

[16] M. Mantha, “Introducing Dual Intent and Entity Transformer (DIET) - state-of-the-art for intent and entity recognition,” 9 March 2020. [Online]. Available: https://rasa.com/blog/introducing-dual-intent-and-entity-transformer-diet/.

[17] Rasa, “Default Actions,” 2025. [Online]. Available: https://rasa.com/docs/reference/primitives/actions/.

[18] Rasa, “FallbackClassifier,” 2025. [Online]. Available: https://legacy-docs-oss.rasa.com/docs/rasa/reference/rasa/nlu/classifiers/fallback_classifier/.

[19] Rasa, “Fallback and Human Handoff,” [Online]. Available: https://legacy-docs-oss.rasa.com/docs/rasa/fallback-handoff/.

[20] Rasa, “TEDPolicy (Transformer Embedding Dialogue),” 2025. [Online]. Available: https://legacy-docs-oss.rasa.com/docs/rasa/reference/rasa/core/policies/ted_policy/.

[21] C. D. Manning, P. Raghavan and H. Schütze, Introduction to Information Retrieval, Cambridge: Cambridge University Press, 2008.

UDK 658.8:502.131.1]:339.13(4)
DOI 10.7251/ZRSNG2526023B

Zeleni marketing kao instrument izgradnje održive konkurentske prednosti preduzeća

Green Marketing as a Strategic Instrument for Building Sustainable Competitive Advantage

Kristina Balotić, Univerzitet Sinergija, Bijeljina

Sažetak — **Savremeni međunarodni sistem suočava se sa rastućim izazovima koji proizlaze iz klimatskih promjena, neodržive eksploatacije prirodnih resursa i intenzivnog zagađenja životne sredine. Ovi procesi ne utiču isključivo na ekološku ravnotežu, već se odražavaju i na globalne ekonomske tokove, konkurentnost preduzeća i dugoročnu stabilnost tržišta. Kao odgovor na navedene izazove, u okviru koncepta održivog razvoja, cirkularne ekonomije i zelene tranzicije, razvijaju se savremeni modeli poslovanja zasnovani na principima društvene odgovornosti i resursne efikasnosti. U tom kontekstu, zeleni marketing dobija na značaju kao važan strateški instrument koji omogućava preduzećima da integrišu ekološke vrijednosti u svoje poslovne strategije, diferenciraju se na tržištu i ostvare održivu konkurentsku prednost. Njegova primjena omogućava izgradnju pozitivnog imidža, jačanje povjerenja potrošača i dugoročno pozicioniranje preduzeća kao društveno odgovornog i tržišno održivog subjekta.**

Ključne riječi – ***zeleni marketing; konkurentnost; održivi razvoj; cirkularna ekonomija; resursi; klimatske promjene***

Abstract – The contemporary international system is facing growing challenges arising from climate change, the unsustainable exploitation of natural resources, and increasing environmental pollution. These processes affect not only ecological balance but also global economic flows, corporate competitiveness, and long-term market stability. In response to these challenges, within the framework of sustainable development, the circular economy, and the green transition, modern business models based on the principles of social responsibility and resource efficiency are being developed. In this context, green marketing is gaining importance as a significant strategic instrument that enables companies to integrate environmental values into their business strategies, differentiate themselves in the market, and achieve sustainable competitive advantage. Its implementation contributes to building a positive corporate image, strengthening consumer trust, and ensuring the long-term positioning of companies as socially responsible and market-sustainable entities.

Keywords **– Green marketing; competitiveness; sustainable development; circular economy; resources; climate change**

I.UVOD

Rast globalne populacije i ubrzana potrošnja u savremenim društvima doveli su do sve većeg pritiska na prirodne resurse. [11] Težnja da se odgovori na sve strožije zahtjeve velikog broja potrošača rezultira ne samo iscrpljivanjem osnovnih resursa, već i nizom ozbiljnih ekoloških problema, uključujući oštećenje ozonskog omotača, globalno zagrijavanje, smanjenje zelenih površina i degradaciju ekosistema. [1] Takvi procesi ne samo da ugrožavaju životnu sredinu, već i dugoročno ometaju poslovnu konkurentnost, jer negativna reputacija i neusklađenost sa savremenim ekološkim standardima smanjuju povjerenje potrošača. [7]

Pored ekoloških posljedica, ovaj fenomen ima i društveno-ekonomske implikacije. [21] Sve veća potrošnja povećava potražnju za energijom i sirovinama, što dovodi do nesigurnosti u snabdijevanju i rasta cijena resursa. Istovremeno, nedostatak adekvatnih politika održive proizvodnje i potrošnje otežava očuvanje ekološke ravnoteže, što postavlja pitanja o dugoročnoj održivosti savremenih društava.

Današnje tržište karakteriše intenzivna konkurencija, brze promjene u preferencijama potrošača i rastuća svjesnost o ekološkim pitanjima.[6] Preduzeća teže eliminisanju ekoloških anomalija, očuvanje životnog ambijenta i koncipiranje održivog ekonomskog razvoja društva ali se i suočavaju sa izazovom da odgovore na zahtjeve tržišta, a istovremeno smanje negativan uticaj svojih proizvoda i procesa na okoliš. Tradicionalne strategije fokusirane su isključivo na ekonomsku dobit, sve više gube efektivnost, jer potrošači i šira javnost sve više cijene odgovorno poslovanje i ekološku održivost. [9]

Primjena zelenog marketinga uključuje dizajniranje ekološki prihvatljivih proizvoda, optimizaciju proizvodnih procesa, korištenje obnovljivih resursa i komunikaciju tih praksi prema potrošačima. [4] Pored ekoloških koristi, zeleni marketing doprinosi jačanju brenda, diferencijaciji od konkurenata, povećanju lojalnosti kupaca i stvaranju dodatne vrijednosti za poslovanje. Na taj način, ekološka

odgovornost postaje izvor strateške prednosti i ključni faktor konkurentnosti. [10]

U okviru ovog istraživanja, posebna pažnja posvećena je identifikaciji faktora koji omogućavaju da ekološki orijentisane strategije postanu efektivan instrument konkurentske prednost preduzeća, a to su: zelena ambalaža, zeleno oglašavanje, inovacija zelenih proizvoda i inovacija zelenih procesa. Analizom primjene ovih praksi istraživanje nastoji razmotriti kako preduzeća mogu balansirati između ekonomskih ciljeva i ekološke odgovornosti, te na koji način resursna efikasnost i inovacije u proizvodnji doprinose održivosti i tržišnoj prednosti.

Cilj ovog rada je istražiti primjere dobre prakse i pružiti smjernice za preduzeća koja žele unaprijediti svoje ekološke i poslovne performanse. Kroz ovu analizu, rad nastoji ukazati na značaj integrisanja ekoloških strategija u poslovnu politiku, naglašavajući da odgovorno i održivo poslovanje može istovremeno doprinositi očuvanju okoliša i jačanju tržišne pozicije. [18] Na taj način, zeleni marketing postaje ne samo ekološki, već i strateški imperativ savremenih preduzeća.

II.DRUŠTVENO ODGOVORNO POSLOVANJE I MARKETING

Društveno odgovorno poslovanje predstavlja savremeni pristup upravljanju u kojem preduzeća, pored ekonomskih ciljeva, svjesno integrišu brigu o društvu i životnoj sredini u svoje poslovne aktivnosti[1]. [13] To znači da organizacije, pored poštovanja zakonskih propisa, ulažu dodatne napore u razvoj ljudskog kapitala, zaštitu okoline i izgradnju kvalitetnih odnosa sa svim relevantnim interesnim grupama. Integracija društvene odgovornosti u poslovnu strategiju može doprinijeti stvaranju zajedničke vrijednosti za kompaniju i društvo [14].

U takvom konceptu poslovanja profit više nije jedini pokazatelj uspješnosti. Uspješnim se smatra ono preduzeće koje uravnoteženo upravlja svojim ekonomskim rezultatima, društvenim uticajem i ekološkim aspektima poslovanja. [16] Poseban značaj imaju ulaganja u ekološki prihvatljive tehnologije koje smanjuju zagađenje vode, vazduha i zemljišta, kao i kontinuirano unapređenje znanja i vještina zaposlenih. [8] Poboljšanje uslova rada, briga o zdravlju i bezbjednosti zaposlenih te njegovanje kvalitetnih međuljudskih odnosa doprinose većoj produktivnosti i jačanju konkurentske pozicije na tržištu[2]. [16]

Društveno odgovorno poslovanje ne ogleda se samo u internim aktivnostima preduzeća, već ima i širu, eksternu dimenziju. Ono podrazumijeva pozitivan uticaj na lokalnu zajednicu i odgovoran odnos prema dobavljačima, poslovnim partnerima, investitorima, potrošačima, javnim institucijama i drugim zainteresovanim stranama. Time se gradi povjerenje i dugoročna stabilnost poslovanja. [19]

U skladu sa ovim pristupom, marketing je doživio značajnu transformaciju. Tradicionalni marketing, koji je primarno bio usmjeren na povećanje prodaje i tržišnog udjela, proširen je vrijednostima koje uključuju društvenu i ekološku odgovornost. Savremeni marketing nastoji istovremeno zadovoljiti potrebe potrošača, ostvariti finansijsku održivost i doprinijeti zaštiti životne sredine i opštem dobru društva. [3] Na taj način, društveno odgovorno poslovanje i zeleni marketing postaju važni faktori izgradnje konkurentske prednosti u modernom tržišnom okruženju.

III.ZELENI MARKETING

Prve sistematske rasprave o ekološkom, odnosno zelenom marketingu pojavile su se tokom 1970-ih godina, u periodu kada je globalna konkurencija sve više rasla, a potrošači postajali obrazovaniji, kulturno i informatički osviješteniji. [2] U tom periodu kompanije su počele prepoznavati da smanjenje negativnog uticaja na životnu sredinu može postati važan element u izgradnji konkurentske prednosti[3].[1]

Zeleni marketing se danas definiše kao marketinški pristup koji u svim svojim segmentima — od planiranja do implementacije — uzima u obzir kako proizvodi i usluge, tako i širi uticaj marketinških aktivnosti na životnu sredinu i društvo u cjelini[4]. [7] Ovaj koncept je evoluirao od prvih definicija koje je Američka marketinška asocijacija (AMA) formulisala sredinom 1970-ih kao proučavanje ekoloških efekata marketinga[5] [2], a savremeni autori naglašavaju da on uključuje i strateško sagledavanje konkurentskih koristi i odnosa sa potrošačima kroz održive prakse[6]. [10] Iz različitih definicija jasno je da zeleni marketing ima dva osnovna cilja: s jedne strane, razvijati proizvode koji zadovoljavaju potrošačke potrebe za kvalitetom, praktičnošću, dobrom upotrebnom vrijednošću i prihvatljivom cijenom uz minimalan uticaj na životnu sredinu; s druge strane, graditi imidž preduzeća kao ekološki i društveno odgovorne organizacije, čime se jača njena pozicija na tržištu i odnosi sa dionicima[7]. [20]

Intenzivne promjene u društvenom, tehnološkom i ekonomskom okruženju doprinijele su promjenama u

[1] Kotler, Philip and Lee, Nancy (2005): Corporate Social Responsibility: Doing the Most Good for Your Company and Your Cause, Hoboken: John Wiley & Sons, p. 23.

[2] Porter, Michael E. and Kramer, Mark R. (2006): "Strategy and Society: The Link Between Competitive Advantage and Corporate Social Responsibility", Harvard Business Review, Vol. 84, No. 12, p. 82.

[3] Alkhatib, S., Kecskés, P. & Keller, V. (2023). *Green Marketing in the Digital Age: A Systematic Literature Review*. *Sustainability*, 15(16), 12369. Dostupno online: https://www.mdpi.com/2071-1050/15/16/12369

[4] Jovičić, D., Ilić, D. & Raletić Jotanović, S. (2022). *Zeleni marketing kao determinanta konkurentske prednosti na B2B tržištima*. *International Journal of Economic Practice and Policy*. Dostupno online: DOI: https://doi.org/10.5937/skolbiz2-41068

[5] American Marketing Association (AMA) (1975). *Proceedings on Ecological Marketing*.

[6] Pancić, M., Serdarušić, H. & Ćućić, D. (2023). *Green Marketing and Repurchase Intention: Stewardship of Green Advertisement, Brand Awareness, Brand Equity, Green Innovativeness, and Brand Innovativeness*. *Sustainability*, 15(16), 12534. Dostupno online: https://doi.org/10.3390/su15161234

[7] Risteska, L. (2021). *Green Marketing Mix and Promotion of Responsible Consumption*. *KNOWLEDGE – International Journal*. Dostupno online: https://ojs.ikm.mk/index.php/kij/article/view/5976

vrijednostima, stavovima i potrošačkim preferencijama, usljed čega se formirao segment tzv. zelenih ili ekološki odgovornih potrošača. Ovu grupu karakteriše povećana osjetljivost na uticaj proizvodnje i potrošnje na prirodne resurse, kao i sklonost ka izboru proizvoda koji su proizvedeni na održiv način i imaju minimalan negativan uticaj na životnu sredinu. [5] U takvom kontekstu, zeleni marketing dobija značajnu ulogu u procesu komunikacije između kompanija i potrošača, jer omogućava informisanje javnosti o ekološkim karakteristikama proizvoda, načinima proizvodnje i naporima preduzeća u pravcu očuvanja životne sredine. Istovremeno, kroz odgovarajuće promotivne aktivnosti i transparentnu komunikaciju, kompanije doprinose jačanju ekološke svijesti potrošača i podstiču donošenje odgovornijih odluka u procesu kupovine, čime zeleni marketing postaje važan instrument u ostvarivanju održivog razvoja savremenog tržišta. [22]

U praksi, osim elenenata tradicionalnog marketing miksa, zeleni marketing se provodi kroz nove specifične elemente i aktivnosti koji uključuju:

- *Zeleni proizvodi i usluge* — razvoj i plasman proizvoda koji su ekološki prihvatljivi, koriste reciklirane ili biorazgradive materijale i imaju smanjen uticaj na životnu sredinu;
- *Zelena ambalaža* — ambalaža koja se može reciklirati, ponovo upotrijebiti ili minimalno koristiti materijal, što smanjuje otpad i zagađenje;
- *Zelena cijena* — politika cijena koja uzima u obzir ekološke karakteristike proizvoda, pri čemu ekološke prednosti ne moraju automatski značiti najvišu cijenu, jer potrošači sve više očekuju vrijednost i održivost u paketu;
- *Zelena komunikacija* — iskrena i transparentna promocija ekoloških karakteristika proizvoda i praksi, bez obmana ili „zelenog ispiranja“, uz korištenje prepoznatljivih sertifikata koji potrošačima garantuju kvalitet i način proizvodnje. [6]

Temeljni okvir zelenog marketinga često se povezuje sa prihvaćenom logikom 3R — *reduce* (smanjiti), *reuse* (ponovo upotrijebiti) i *recycle* (reciklirati) — koji kroz tri ključna koraka doprinosi očuvanju životne sredine i racionalnijem korišćenju resursa[8]. [4]

- *Reduce (smanjiti)* — smanjivanje iskorišćavanja prirodnih resursa i energije u proizvodnim i drugim poslovnim procesima;
- *Reuse (ponovo upotrijebiti)* — višekratna upotreba ambalaže ili dijelova proizvoda umjesto jednokratne upotrebe;
- *Recycle (reciklirati)* — organizovano prikupljanje i prerada proizvoda i ambalaže nakon njihove upotrebe.

Kod kontinuiranog povrata ambalaže ili proizvoda, javlja se reverzibilna distribucija koja je jedno od obilježja zelenog marketinga. U ovom modelu distribucije tok proizvoda odvija se obrnutim smjerom u odnosu na tradicionalne kanale, odnosno proizvodi se nakon upotrebe vraćaju od potrošača nazad proizvođaču ili drugom subjektu zaduženom za njihovu obradu. [17] Time se uspostavlja povratni logistički sistem koji omogućava ponovno korišćenje, recikliranje ili adekvatno zbrinjavanje ambalaže i proizvoda. Prednosti ovakvog pristupa ogledaju se u efikasnijem upravljanju distribucijskim tokovima, smanjenju troškova vezanih za ambalažu te unapređenju imidža preduzeća kao ekološki odgovornog subjekta. [4] S druge strane, organizacija povratnih kanala podrazumijeva dodatne izdatke, uključujući troškove transporta, sortiranja, skladištenja i reciklaže, kao i prilagođavanje proizvodnih procesa. Zbog navedenih troškova, primjene specifičnih tehnologija i često nižih prinosa, posebno u oblasti organske poljoprivrede, ekološki proizvodi se na tržištu često formiraju po višim cijenama u odnosu na proizvode proizvedene konvencionalnim metodama.

IV. IMPLEMENTACIJA PRINCIPA ODRŽIVOSTI U POSLOVANJU

Kao ilustrativan primjer integracije principa održivosti u poslovne strategije globalnih kompanija može se izdvojiti kompanija Nike, koja u posljednjim godinama pozicionira održivost kao sastavni dio svoje korporativne i konkurentske strategije, a ne kao izolovanu filantropsku ili promotivnu aktivnost. [12] Njihov pristup obuhvata sve faze vrijednosnog lanca — od dizajna proizvoda i nabavke materijala do proizvodnje, distribucije i komunikacije sa potrošačima. Neprestano postavljanje mjerljivih ciljeva u smanjenju emisije stakleničkih gasova, povećanju upotrebe recikliranih materijala i prelasku na cirkularne modele proizvodnje čini Nike istaknutim primjerom inovativnog i odgovornog poslovanja, razlikujući ga od drugih globalnih kompanija. U okviru strateških dokumenata i godišnjih izvještaja o uticaju (Impact Report), ova politika održivosti utiče na inovacije proizvoda, upravljanje lancem snabdijevanja, investicione odluke i odnose sa dionicima, potvrđujući da ekološke i društveno odgovorne prakse doprinose dugoročnoj konkurentskoj prednosti. [15]

Kompanija implementira ključne elemente zelenog marketing miksa u svoje poslovne prakse, integrirajući ekološke principe u proizvode, ambalažu, politiku cijena i komunikaciju sa potrošačima.

Održivi proizvodi i usluge — Nike razvija proizvode koji su dizajnirani da budu ekološki prihvatljivi, koriste materijale koji su reciklirani ili biorazgradivi i smanjuju negativan uticaj na životnu sredinu.

Ekološka ambalaža — Ambalaža je osmišljena tako da se može reciklirati, koristiti više puta ili da koristi minimalnu količinu materijala, čime se smanjuje stvaranje otpada i zagadjenje.

[8] Emel Gelmez, Eren Özceylan & Beata Mrugalska (2024). *The Impact of Green Supply Chain Management on Green Innovation, Environmental Performance, and Competitive Advantage*. *Sustainability*, 16(22), 9757. Dostupno online: https://www.mdpi.com/2071-1050/16/22/9757

Cijena sa ekološkim pristupom — Politika odredjivanja cijena proizvoda uzima u obzir njihove ekološke karakteristike, pri čemu održivi proizvodi ne moraju nužno biti skuplji, već balansiraju vrijednost, kvalitet i održivost.

Transparentna ekološka komunikacija — Nike jasno i otvoreno informiše potrošače o ekološkim svojstvima proizvoda i svojim praksama, koristeći relevantne sertifikate i izbjegavajući bilo kakve netačne ili obmanjujuće tvrdnje.

U cilju sistematskog unapređenja održivog poslovanja i smanjenja ekološkog uticaja svojih operacija, kompanija Nike razvila je niz strateških inicijativa i programa održivosti koji obuhvataju različite segmente vrijednosnog lanca. [12]

Inicijativa „Move to Zero"

Centralni okvir ove transformacije predstavlja inicijativa „Move to Zero" [12], čiji je osnovni cilj postizanje nulte emisije ugljen-dioksida (net-zero) i nultog otpada u poslovanju kompanije. Projekat obuhvata sve faze vrijednosnog lanca – od dizajna i nabavke sirovina do distribucije i krajnje upotrebe proizvoda. Poseban fokus stavljen je na smanjenje emisija stakleničkih gasova (Scope 1, 2 i 3), povećanje udjela obnovljive energije u proizvodnim procesima, kao i unapređenje energetske efikasnosti logističkih sistema. Pored toga, inicijativa podrazumijeva i intenzivniju primjenu recikliranih materijala, razvoj cirkularnih modela proizvodnje i smanjenje količine otpada u svim fazama proizvodnog procesa. Na taj način kompanija integriše principe održivog razvoja i smanjuje ekološki uticaj poslovanja.

Tabela 1. nam prikazuje strukturu emisija stakleničkih gasova kompanije prema GHG Protocol metodologiji za fiskalnu 2024. godinu (FY24), uključujući apsolutne emisije po opsegu (Scope 1, 2 i 3), njihov udio u ukupnim emisijama te strateške oblasti na koje su usmjerene mjere smanjenja. [12]

Tabela 1. Struktura emisija po opsegu (scope)

Scope	FY24 (tCO_2e)	Udio u ukupnim emisijama (%)	Strateški fokus smanjenja
Scope 1	57.390	~0,7%	Energetska efikasnost
Scope 2	12.120	~0,1%	Obnovljiva energija
Scope 3	8.196.965	~99%	Materijali i proizvodnja

Izvor: https://about.nike.com/en/mission/focus-areas/sustainability

U poređenju sa baznom fiskalnom 2020. godinom (FY20), kompanija je do FY24 ostvarila smanjenje od 69% u Scope 1 i Scope 2 emisijama te 36% u Scope 3 emisijama, što potvrđuje snažan napredak u operativnoj energetskoj tranziciji, ali i činjenicu da najveći izazov ostaje transformacija lanca vrijednosti. Prema zvaničnim podacima iz izvještaja o održivosti, kompanija kontinuirano povećava upotrebu recikliranih materijala (posebno recikliranog poliestera), dok značajan procenat električne energije u operativnom poslovanju potiče iz obnovljivih izvora. Time se potvrđuje da inicijativa „Move to Zero" nije samo komunikaciona platforma, već operativno razrađen program sa mjerljivim ciljevima i indikatorima performansi[9]. [12]

Sa aspekta teorijskog okvira konkurentske prednosti, ova strategija se može povezati sa konceptom koji ističu Porter i Kramer (2006), prema kojem integracija društvene odgovornosti u korporativnu strategiju može generisati „zajedničku vrijednost" (shared value) za kompaniju i društvo[10]. [16] U tom kontekstu, „Move to Zero" omogućava Nike-u:

- smanjenje dugoročnih troškova kroz energetsku efikasnost i racionalnije upravljanje resursima,
- jačanje reputacionog kapitala na globalnom tržištu,
- diferencijaciju brenda kroz inovativne, održive proizvode,
- usklađenost sa regulatornim i investicionim zahtjevima vezanim za ESG standarde.

Zaključno, može se istaći da program „Move to Zero" predstavlja institucionalizovani oblik zelenog marketinga, u kojem se ekološke vrijednosti sistematski integrišu u strateško upravljanje, čime se potvrđuje teza da održivost može biti izvor dugoročne konkurentske prednosti [15], a ne isključivo etička obaveza savremenih kompanija.

Upravljanje resursima i ekološki uticaj

U okviru savremenih strategija održivog poslovanja posebna pažnja posvećuje se racionalnom upravljanju resursima i smanjenju negativnog uticaja na životnu sredinu. Kompanije sve češće nastoje da kroz inovacije u dizajnu proizvoda i izboru materijala smanje emisiju štetnih gasova i količinu otpada, te da postepeno prelaze na cirkularne modele proizvodnje. U tom kontekstu, Nike je strateški integrisao održivost u proces dizajna i proizvodnje materijala, sa ciljem smanjenja emisije štetnih gasova i otpada, kao i prelaska na cirkularni poslovni model. Prema podacima za fiskalnu 2024. godinu (FY24), oko 78% proizvoda u globalnoj kolekciji sadrži reciklirane materijale, uključujući recikliranu plastiku, poliester i gumu, što doprinosi smanjenju ugljeničnog otiska i podržava principe cirkularne ekonomije.

Inicijative poput Nike Grind i Reuse-A-Shoe omogućavaju prikupljanje starih patika i viškova materijala iz proizvodnje, koji se potom pretvaraju u nove proizvode ili materijale za sportsku infrastrukturu. Na taj način se zatvara materijalni ciklus i smanjuje količina otpada koja završava na deponijama. Ovi programi predstavljaju praktičnu primjenu cirkularne ekonomije u globalnoj proizvodnji sportske opreme, a istovremeno doprinose jačanju imidža kompanije [23] i kreiranju dodatne vrijednosti za potrošače. Pored toga, Circular Design Guide je industrijski alat koji Nike koristi za dizajn proizvoda sa minimalnim otpadom i

[9] Nike, Inc., *FY24 NIKE, Inc. Sustainability Data* (2024), dostupno na: https://about.nike.com/en/mission/focus-areas/sustainability (04.03.2026.)

[10] Porter, Michael E. and Kramer, Mark R. (2006): "Strategy and Society: The Link Between Competitive Advantage and Corporate Social Responsibility", Harvard Business Review, Vol. 84, No. 12, p. 78-92.

maksimalnom mogućnošću reciklaže na kraju životnog ciklusa. Integracija inovativnih materijala i dizajnerskih praksi omogućava kompaniji ne samo smanjenje ekološkog uticaja, već i jačanje konkurentske prednosti kroz diferencijaciju proizvoda i reputaciju lidera u održivosti.

Nike implementira sveobuhvatnu strategiju održivosti koja obuhvata upravljanje otpadom, energijom i potrošnjom vode u globalnim operacijama i dobavljačkom lancu. Prema podacima za fiskalnu 2024. godinu (FY24), 100% operativnog otpada strateških dobavljača preusmjereno je sa deponija, dok je više od 60% otpada reciklirano ili ponovo upotrijebljeno, što značajno doprinosi principima cirkularne ekonomije. Kompanija razvija i programe za smanjenje otpada u dobavljačkom lancu, optimizujući proizvodne procese i ambalažu kako bi smanjila ekološki otisak i stvorila dodatnu vrijednost u proizvodnji.

U pogledu energije, Nike je postigao da 96% električne energije u globalnim operacijama dolazi iz obnovljivih izvora, dok kontinuirano ulaže u energetski efikasne fabrike i operacije, smanjujući direktne emisije stakleničkih gasova (Scope 1 i 2). Takođe, kompanija aktivno radi na smanjenju potrošnje svježe vode kod dobavljača, ostvarivši smanjenje od preko 40% u odnosu na prethodne godine, što doprinosi održivoj proizvodnji i smanjenju ekološkog otiska proizvoda. Ovaj integrisani pristup upravljanju resursima pokazuje da Nike ne samo da minimalizuje negativni uticaj svojih operacija, već i stvara konkurentsku prednost kroz odgovorno i održivo poslovanje.

V.ZAKLJUČAK

Savremeni poslovni uslovi i rastuća ekološka svijest potrošača doveli su do toga da održivost postane važan element strategijskog upravljanja kompanija. Koncept zelenog marketinga predstavlja odgovor na promjene u preferencijama potrošača koji sve više vrednuju proizvode i brendove sa odgovornim odnosom prema životnoj sredini. U tom kontekstu, kompanije nastoje da integrišu ekološke principe u različite aspekte poslovanja, uključujući dizajn proizvoda, proizvodne procese, upravljanje resursima i komunikaciju sa potrošačima.

Analiza strategije održivosti kompanije Nike pokazuje da je održivost postala sastavni dio njenog dugoročnog poslovnog modela. Program „Move to Zero“ predstavlja centralni okvir ove strategije i usmjeren je na smanjenje emisija stakleničkih gasova, povećanje upotrebe obnovljive energije, primenu recikliranih materijala i razvoj cirkularnih proizvodnih modela. Podaci o emisijama prema GHG Protocol metodologiji ukazuju na značajan napredak u smanjenju operativnih emisija, ali i na činjenicu da najveći deo ekološkog otiska potiče iz dobavljačkog lanca, što dodatno naglašava značaj transformacije proizvodnih i materijalnih tokova. Pored smanjenja emisija, Nike implementira i brojne inicijative u oblasti upravljanja resursima, uključujući reciklažu materijala, smanjenje otpada, korišćenje obnovljivih izvora energije i racionalnije upravljanje vodnim resursima. Ovakav integrisani pristup doprinosi smanjenju negativnog uticaja na životnu sredinu, ali istovremeno jača konkurentsku poziciju kompanije na globalnom tržištu.

Zaključno, može se istaći da održivost u savremenom poslovanju predstavlja ne samo društvenu odgovornost, već i važan izvor dugoročne konkurentske prednosti. Integracija principa zelenog marketinga i održivog upravljanja resursima omogućava kompanijama da odgovore na zahteve tržišta, unaprede reputaciju brenda i doprinesu očuvanju životne sredine.

LITERATURA

[1] Alkhatib, S., Kecskés, P. & Keller, V., “Green Marketing in the Digital Age: A Systematic Literature Review,” *Sustainability*, vol. 15, no. 16, 12369, 2023. Dostupno na: https://www.mdpi.com/2071-1050/15/16/12369

[2] American Marketing Association (AMA), *Proceedings on Ecological Marketing*, 1975.

[3] Belz, F. & Peattie, K., *Sustainable Marketing: A Global Perspective*, Chichester: Wiley, 2012.

[4] Gelmez, E., Özceylan, E. & Mrugalska, B., “The Impact of Green Supply Chain Management on Green Innovation, Environmental Performance, and Competitive Advantage,” *Sustainability*, vol. 16, no. 22, 9757, 2024. Dostupno na: https://www.mdpi.com/2071-1050/16/22/9757

[5] Han, J., Zhang, Y., Xiao, H. & Zhao, Z., “Green marketing or demarketing? Temporal perspectives on tourists’ pro-environmental behavior,” *Journal of Hospitality and Tourism Management*, vol. 66, 101422, 2026. Dostupno na: https://doi.org/10.1016/j.jhtm.2026.101422

[6] Jevtić, A., Radić, A. & Riznić, D., “Zeleni marketing i aspekti razvoja zelenog marketinga u Republici Srbiji / Green marketing and development aspects of green marketing in Republic of Serbia,” *ECOLOGICA*, vol. 30, no. 112, pp. 576–582, 2023. Dostupno na: https://doi.org/10.18485/ecologica.2023.30.112.10

[7] Jovičić, D., Ilić, D. & Raletić Jotanović, S., “Zeleni marketing kao determinanta konkurentske prednosti na B2B tržištima,” *International Journal of Economic Practice and Policy*, 2022. Dostupno na: https://doi.org/10.5937/skolbiz2-41068

[8] Lehner, T., *Environmental Marketing and Corporate Sustainability*, Cham: Springer, 2022.

[9] Peattie, J. & Crane, A., *Green Marketing: Legend, Myth, Farce or Prophesy?*, London: Qualitative Market Research, 2005.

[10] Pancić, M., Serdarušić, H. & Ćućić, D., “Green Marketing and Repurchase Intention: Stewardship of Green Advertisement, Brand Awareness, Brand Equity, Green Innovativeness, and Brand Innovativeness,” *Sustainability*, vol. 15, no. 16, 12534, 2023. Dostupno na: https://doi.org/10.3390/su15161234

[11] Pupovac, D., “Održivi razvoj – Novo lice ekonomije,” *Socijalna ekologija*, 24, 2015.

[12] Nike, Inc., *FY24 NIKE, Inc. Sustainability Data*, 2024. Dostupno na: https://about.nike.com/en/mission/focus-areas/sustainability

[13] Kotler, P. & Lee, N., *Corporate Social Responsibility: Doing the Most Good for Your Company and Your Cause*, Hoboken: John Wiley & Sons, 2005, p. 23.

[14] Porter, M. E. & Kramer, M. R., “Strategy and Society: The Link Between Competitive Advantage and Corporate Social Responsibility,” *Harvard Business Review*, vol. 84, no. 12, p. 82, 2006.

[15] Porter, M. E. & Kramer, M. R., “Strategy and Society: The Link Between Competitive Advantage and Corporate Social Responsibility,” *Harvard Business Review*, vol. 84, no. 12, pp. 78–92, 2006.

[16] Porter, M. E. & Kramer, M. R., *Creating Shared Value: How to Reinvent Capitalism—and Unleash a Wave of Innovation and Growth*, Boston: Harvard Business Review Press, 2011.

[17] Nefat, A., *Zeleni marketing*, Pula: Sveučilište Jurja Dobrile u Puli, 2015.

[18] Lüdeke Freund, C., *Business Models for Sustainability*, 2nd ed., Routledge, 2021.

[19] Sinčić Ćorić, D., "Održivi marketing na tržištima poslovne (B2B) potrošnje," *International Journal of Multidisciplinarity in Business and Science*, vol. 7, no. 11, pp. 27–35, 2021. Dostupno na: https://hrcak.srce.hr/260173

[20] Risteska, L., "Green Marketing Mix and Promotion of Responsible Consumption," *KNOWLEDGE – International Journal*, 2021. Dostupno na: https://ojs.ikm.mk/index.php/kij/article/view/5976

[21] Tolušić, Z., Dumančić, E. & Bogdan, K., "Društveno odgovorno poslovanje i zeleni marketing," *Agroeconomia Croatica*, vol. 4, no. 1, pp. 25–31, 2014. Dostupno na: https://hrcak.srce.hr/125551

[22] Trandafilović, B. & Blagojević, A., *Zeleni marketing*, Zadužbina Andrejević, 2017.

[23] Smith, S. & Brower, D., *Long-Term Brand Equity through Sustainability Initiatives*, New York: Routledge, 2020.

UDK 316.772.4:[502.131.1:005.334
DOI 10.7251/ZRSNG2526029S

Uloga organizacijske kulture i podrške menadžmenta u procesu zelene tranzicije i održivosti

The role of organizational culture and management support in the process of green transition and sustainability

Snježana Stanišić, Aleksandar Sandro Cvetković, Univerzitet Sinergija, Bijeljina

***Sažetak* — Zelena tranzicija i održivi razvoj predstavljaju ključne izazove savremenog poslovanja. Uspješnost implementacije održivih praksi u velikoj mjeri zavisi od organizacijske kulture i podrške menadžmenta. Rad analizira odnos između organizacijske kulture, liderstva, društveno odgovornog poslovanja (DOP), poslovne etike i humane ekonomije u kontekstu zelene transformacije. Poseban akcenat stavljen je na mjerenje društvene odgovornosti putem indeksa i standarda, kao i na specifičnosti tranzicijskog konteksta Bosne i Hercegovine. Održiva transformacija zahtjeva sistemsku promjenu vrijednosti, stratešku integraciju održivosti i aktivnu institucionalnu podršku. Humana ekonomija može doprinijeti uspostavljanju temeljnih vrijednosti preduzeća koje su usmjerene na društveno odgovorno poslovanje i održivi rast.**

***Ključne riječi* – organizacijska kultura, zelena tranzicija, održivost, društveno odgovorno poslovanje, poslovna etika, humana ekonomija**

Abstract – Green transition and sustainable development represent key challenges of modern business. The success of implementing sustainable practices largely depends on organizational culture and management support. The paper analyzes the relationship between organizational culture, leadership, corporate social responsibility (CSR), business ethics and human economy in the context of green transformation. Special emphasis is placed on measuring social responsibility through indices and standards, as well as on the specifics of the transition context of Bosnia and Herzegovina. Sustainable transformation requires a systemic change in values, strategic integration of sustainability and active institutional support. Humane economy can contribute to the establishment of the fundamental values of companies that are focused on socially responsible business and sustainable growth.

***Keywords* – organizational culture, green transition, sustainability, corporate social responsibility, business ethics, humane economy**

I. UVOD

Uloga organizacijske kulture i podrške menadžmenta u procesu zelene tranzicije i održivosti predstavljaju osnovu na kojoj se zasniva uspjeh svake inicijative za održivost u poslovanju. Organizacijska kultura definiše vrijednosti, norme, uvjerenja i ponašanja unutar organizacije, dok menadžment postavlja smjer i pruža resurse potrebne za implementaciju tih vrijednosti. Udruženi, oni oblikuju okruženje u kom održive prakse mogu ostati marginalizovane i zanemarene ili se mogu podstaći i razviti. Jedan od mogućih načina na koji se organizacijska kultura može razvijati u smjeru održivosti je kroz kreiranje ekoloških timova unutar organizacije. Zelena tranzicija često zahtijeva značajna početna finansijska ulaganja, gdje međunarodne organizacije i vlade zemalja pružaju finansijsku podršku putem zelenih fondova, grantova i povoljnih kredita. Kada zaposleni ne razumiju dugoročne koristi održivih inicijativa, dolazi do otpora, posebno ako se promjene percipiraju kao nametnute spolja.

Društveno odgovorno poslovanje obuhvata aktivnosti kojima preduzeća, uz ostvarivanje ekonomske koristi, doprinose zaštiti okoline i poboljšanju kvaliteta života zaposlenih i potrošača kao i razvoju lokalne zajednice. Društveno odgovorno poslovanje (DOP), poznato i kao Corporate Social Responsibility (CSR), razvilo se kao praktična implementacija principa održivosti u poslovne procese. Ono podrazumijeva integraciju ekonomskih, socijalnih i ekoloških ciljeva u korporativnu strategiju.

Poslovna etika predstavlja normativni okvir donošenja odluka u organizacijama. Ona podrazumijeva moralno procjenjivanje poslovnih aktivnosti, uz poštovanje zakonskih, društvenih i ekoloških standarda. Bez etičkog temelja, zelena tranzicija ostaje formalna i deklarativna, bez stvarne transformacije poslovnih praksi.

Koncept humane ekonomije naglašava centralnu ulogu čovjeka u ekonomskim procesima. On integriše društvene i ekološke ciljeve u poslovne strategije i posmatra organizaciju kao dio šireg društvenog sistema.

Cilj ovog rada je prikazati način mjerenja DOP-a, način i prilagođavanja na pametna rješenja, u kom stadijumu se Bosna i Hercegovina nalazi u odnosu na druge zemlje i šta dobijamo primjenom humane ekonomije.

II. ZELENA TRANZICIJA U JAVNOM SEKTORU I URBANIM SISTEMIMA

Brza urbanizacija predstavlja i prepreke i potencijalne puteve ka održivom razvoju, posebno u pogledu upravljanja resursima i očuvanja okoline.[1] Uticaj klimatskih promjena na ljudsko društvo i ekonomiju postaje sve očigledniji, privlačeći značajnu globalnu pažnju.[2] Zelene tranzicije su takođe ključne za podršku principima kružne ekonomije.[3]

Kad je u pitanju zelena tranzicija tu organizacijska kultura može biti moćan pokretač, ali može predstavljati i prepreku ako nije usklađena s ciljevima održivosti. Kultura koja favorizuje inovacije, promjene i odgovornost prema okolini omogućava zaposlenima da lakše prihvate i sprovedu zelene inicijative. Organizacije koje već imaju kulturu koja podstiče transparentnost, etičnost i društvenu odgovornost, imaju veću vjerovatnoću da će uspješno implementirati održive prakse.[4] U tim organizacijama, zaposleni često osjećaju veći stepen odgovornosti prema ekološkim ciljevima, jer su te vrijednosti već integrisane u njihovo svakodnevno poslovanje. Decenijama su strategije razvoja i ekonomskog rasta naglašavale brzi porast finansijskog kapitala bez brige o stanju okoline i bez postavljanja pitanja o iscrpljivanju i degradaciji prirodnih resursa.[5]

Jedan od načina na koji se organizacijska kultura može razvijati u smjeru održivosti je kroz kreiranje ekoloških timova unutar organizacije, koji se zovu green teams. Ovi timovi omogućavaju zaposlenima da predlažu i sprovode inicijative za smanjenje ekološkog uticaja unutar organizacije, što ne samo da podstiče inovacije, već i jača osjećaj odgovornosti i angažovanja zaposlenih. Na taj način, zelene prakse postaju dio svakodnevne organizacijske kulture, a ne samo privremeni projekat ili marketinški trik.

U organizacijama gdje vlada rigidna, birokratska kultura koja ne podstiče inovacije i promjene, implementacija održivih praksi, može doći do otpora. U takvim slučajevima, zelena tranzicija može da se percipira kao spoljni pritisak, odnosno kao nametnuta promjena koja remeti uhodane poslovne procese. Zaposleni u ovim organizacijama mogu biti skeptični prema promjenama, posebno ako im nije jasno kako zelene inicijative doprinose dugoročnom poslovnom uspjehu. Prema istraživanju organizacijska kultura može biti glavna prepreka u promjenama kada je duboko ukorijenjena u tradicionalne vrijednosti i prakse koje su suprotstavljene inovacijama i promjenama.[6] Jedan od najvažnijih aspekata podrške menadžmenta je osiguranje potrebnih resursa za implementaciju održivih praksi. To uključuje finansijska sredstva za uvođenje novih tehnologija, vremenska ulaganja za edukaciju zaposlenih, kao i infrastrukturnu podršku za promjenu postojećih poslovnih modela u održivije alternative. Bez ovih resursa, zelene inicijative ostaju na nivou teorije i ne mogu se uspješno sprovesti u praksi.[7] Bez finansijskih sredstava, projekti su privremeni poduhvati ograničeni vremenom i budžetom, što ograničava i dostupne resurse.[8] Na primjer, sve veća efikasnost sistema energije vjetra učinili su ih atraktivnijom opcijom za smanjenje zavisnosti o neobnovljivim izvorima energije i doprinijeli su smanjenju emisija staklenih bašta. Odnosno, kako energija vjetra postaje pristupačnija, njena uloga u postizanju održivih energetskih rješenja nastavlja rasti, povećavajući njenu održivost kao obnovljivog izvora energije.

Tehnologije poput sistema obnovljivih izvora energije, infrastrukture koja efikasno koristi vodu i inovativna rješenja za upravljanje otpadom pomažu gradovima da minimiziraju svoj uticaj na okolinu, a istovremeno će zadovoljiti rastuće potrebe urbanog stanovništva.[9] Na primjer, mnogi gradovi postavljaju solarne panele na zgrade ili uvode pametne mreže (smart grids) koje pomažu u optimizaciji potrošnje električne energije. Ovaj prelazak na obnovljive izvore energije pomaže u smanjenju emisije gasova sa efektom staklene bašte[10] Modernizacija upravljanja otpadom kroz kružnu ekonomiju predstavlja ključni korak u zelenoj tranziciji. Javna komunalna preduzeća implementiraju napredne sisteme za razdvajanje otpada i reciklažu, dok mnogi gradovi usvajaju praksu energetski oporavak otpada (waste-to-energy), čime se smanjuje potreba za deponijama i emisija metana.[11] Obnovljivi izvori energije, uključujući solarnu i energiju vjetra, stvaraju dinamične energetske sisteme koji se koriste umjesto centraliziranih i pasivnih.[12]

Pametni gradovi (smart cities) postaju sve prisutniji kao model urbanog razvoja, a javna komunalna preduzeća igraju ključnu ulogu u ovoj transformaciji. Inicijative kao što su senzori za praćenje potrošnje resursa, digitalizacija upravljanja infrastrukturom i optimizacija usluga poput javne rasvjete i saobraćaja, značajno doprinose smanjenju energetske potrošnje.[13] Zelena tranzicija često zahtijeva značajna početna

[1]Balsalobre-Lorente D., J. Abbas, C. He, L. Pilař, S.A.R. Shah (2023) Tourism, urbanization and natural resources rents matter for environmental sustainability: the leading role of AI and ICT on sustainable development goals in the digital era, Resour. Policy., 82, Article 103445, 10.1016/

[2]Zhenhua Liu, Jialong Fu, Xinyang Zhang, Qiang Ji, (2026) Higher-order moment risk spillovers between the carbon and energy markets under climate policy uncertainty, Journal of Management Science and Engineering Volume 11, Issue 1, Pages 1-19

[3]Nieke Masruchiyah, Novita Damayanti, Prasetya Yoga Santoso, Asep Marfu (2025) Harnessing green human capital and circular economy in urbanization: Advancing water resilience through resource conservation and green technology, Environmental ChallengesVolume 20,101227

[4]Cameron, K.S. and Quinn, R.E. (2006) Diagnosing and Changing Organisational Culture Based on Competing Values Framework. Josey Bass, San Francisco.

[5]Bassem Kahouli, Basma Hamdi, Kamel Miled (2026) Exploring the interplay between renewable energy, agriculture, clean technologies, natural resources, and environmental sustainability, Energy Strategy Reviews Volume 64

[6]Schein, E. H. (2010). Organizational Culture and Leadership (4th ed.). San Francisco, CA: Jossey-Bass

[7]Rodrigo Lozano, 2015. A Holistic Perspective on Corporate Sustainability Drivers, Corporate Social Responsibility and Environmental Management: Volume 22, Issue 1

[8]Miller J. G., (2022) Stakeholder roles in artificial intelligence projects, Project Leadership and Society,Volume 3, 100068

[9]Jain H., (2024) From pollution to progress: groundbreaking advances in clean technology unveiled, Innovation and Green Development, 3 (2),Article 10014

[10](https://www.pwc.com/gx/en/global-annual-review/2023/pwc-global-annual-review-2023.pdf).

[11](https://www.worldbank.org/en/about/annual-report-2023)

[12]Gulfaraz Anis a, Naila Samar Naz a, Taher M. Ghazal b, Muhammad Sajid Farooq c, Muhammad Saleem a, Chan Yeob Yeun d, Munir Ahmad e, Khan Muhammad Adnan, (2026) Smart and transparent grid stability prediction for efficient energy management using explainable AI, Energy Strategy Reviews Volume 64, 102083

[13](https://globescan.com/2022/06/23/2022-sustainability-leaders-report/)

ulaganja, vlade i međunarodne organizacije pružaju finansijsku podršku putem zelenih fondova, grantova i povoljnih kredita. Javna komunalna preduzeća imaju pristup ovim sredstvima kako bi modernizovala svoju infrastrukturu u skladu sa klimatskim regulativama.[14] Uvođenje električnih autobusa i infrastrukture za punjenje električnih vozila u javnom transportu pomaže u smanjenju emisije štetnih gasova i poboljšanju kvaliteta vazduha u urbanim područjima. Uz to, gradovi sve više investiraju u biciklističke staze i pješačke zone kao održive alternative tradicionalnim vidovima transporta.[15]

Bosna i Hercegovina je zemlja koja je kroz razne reforme prošla samo u teoriji, ali ne i u praksi. Proces tranzicije na ovim prostorima traje od 90-ih godina. Energetska tranzicija, međutim, već neko vrijeme vrlo stidljivo kuca na vrata, a fosilni sat otkucava do 2050. Za zemlju koja uglavnom zavisi o uglju, ovo je velika prekretnica. Intenzitet transformacije sistema koja se trenutno odvija na globalnom nivou u smislu ublažavanja klimatske krize obrnuto je proporcionalan nivou svijesti i zabrinutosti domaćih vlasti o ovoj temi.

Nažalost, važeći zakoni u Bosni i Hercegovini potpuno isključuju mogućnosti za građansku energiju: proizvođače i potrošače ili zajednice obnovljivih izvora energije.

Zelena logistika sve više prelazi iz područja volontarizma u područje tržišne neophodnosti, jer kupci, investitori i regulatori zahtijevaju mjerljive pokazatelje održivosti.[16] što predstavlja jedan od načina jačanja dugoročnog ugleda preduzeća na tržištu.[17]

III. POSLOVNA ETIKA I NJENA PRIMJENA

Poslovna etika i društvena odgovornost predstavljaju važan segment savremenog poslovanja, a njihov naglasak je na načinima ponašanja svih učesnika uključenih u privredne procese, bilo da je riječ o pojedincima, poslovnim subjektima ili interesnim grupama. Osnovna svrha ovog područja je usmjeriti poslovne aktivnosti prema praksama koje ne samo da osiguravaju profitabilnost, već i doprinose širem društvenom, ekološkom i privrednom razvoju. Poslovna etika istražuje moralne vrijednosti, načela i standarde koji bi trebali biti vodič učesnicima u donošenju poslovnih odluka, dok društveno odgovorno poslovanje posmatra kako se te vrijednosti mogu primijeniti u praksi kroz održivost, poštivanje ljudskih prava, očuvanje okoline i doprinos opštem društvenom blagostanju.

Važno je da menadžment kontinuirano prati promjene u okruženju i aktivno se prilagođava novim uslovima. U savremenoj ekonomiji, prelaz s tradicionalnog na odgovorno poslovanje podrazumijeva da organizacije djeluju u skladu sa zakonima, ali i da moralno procjenjuju posljedice svojih odluka. Takav pristup doprinosi kvalitetu lokalnih zajednica i ostvarivanju javnog dobra, a istovremeno osigurava dugoročnu održivost poslovanja.

Odnos s kupcima je od presudne važnosti. Zadovoljni kupci su garancija za lojalnost, pozitivn imidž i stabilan tržišni položaj preduzeća. Organizacije koje osiguravaju kvalitetne proizvode i usluge po pravednim cijenama ostvaruju dugoročnu konkurentsku prednost. Istu važnost imaju i dobavljači. Pouzdani dobavljači omogućuju stabilno snadbjevanje resursima, dok eventualni problemi poput kašnjenja ili smanjenog kvaliteta mogu ozbiljno narušiti poslovne rezultate i reputaciju preduzeća. Stoga je za uspješno poslovanje ključno održavati partnerski i dugoročno održiv odnos s dobavljačima.

IV. PROMJENE ORGANIZACIJSKE KULTURE

Organizacijska promjena se kao pojam najjednostavnije može posmatrati polazeći od činjenice da je rezultat svake promjene razlika koja tokom vremena nastaje u jednoj ili više dimenzija subjekta. To je jedan od razloga zašto organizacijske promjene predstavljaju razlike u stanju organizacije između dva vremenska perioda, dok je proces organizacijskih promjena proces u kom ta razlika nastaje.

Svaka organizacija, nezavisno o sektoru kom pripada, veličini, broju zaposlenih ili bilo kom drugom parametru ima jednu specifičnost - organizacijsku kulturu koja određuje i predstavlja smjernicu za svaku poslovnu odluku i proces. Ali, iako se čini jednostavnom i lako objašnjivom komponentom organizacije, kultura je zbog svoje neopipljivosti vrlo složena što mogu potvrditi brojni zaposleni nekih organizacija jer se nisu osjećali njenim dijelom.

Organizacijsku kulturu ne treba zanemariti jer često predstavlja najosjetljiviju, ali i najnepopustljiviju prepreku digitalnoj i održivoj transformaciji. Otpor promjenama, bilo iz samog straha od nepoznatog, bilo iz navike ili opreza, može sabotirati i najbolje osmišljene strategije. Bez snažnog liderstva, interne komunikacije i promjene mentaliteta unutar preduzeća, tehnologija ostaje samo skup alata bez stvarnog efekta. Važno je istaći da preduzeća koje žele provesti zelenu tranziciju moraju uložiti u promjenu organizacijske kulture.[18] Jer se preduzeća više ne posmatraju isključivo kao privredni subjekti usmjereni na ostvarivanje profita, već i kao društveni akteri čije odluke i aktivnosti imaju značajan uticaj na zajednicu, okolinu i buduće generacije.

Društveno odgovorno poslovanje razvija se kao praktična implementacija načela održivosti u svakodnevne poslovne procese. Ono obuhvata aktivnosti kojima preduzeća, uz ostvarivanje ekonomske koristi, doprinose razvoju lokalne zajednice, zaštiti okoline i poboljšanju kvaliteta života zaposlenih i potrošača. Takav pristup zahtijeva promjenu perspektive u korporativnom upravljanju: od orijentacije na kratkoročnu dobit prema stvaranju dugoročne vrijednosti za sve učesnike. U tom kontekstu, društveno odgovorno poslovanje ne predstavlja trošak, nego investiciju u stabilnost, reputaciju i konkurentsku prednost preduzeća.

[14] https://commission.europa.eu/strategy-and-policy/state-union/state-union-2023 (pristupljeno 11.03.2026.)

[15] https://www.iea.org/reports/world-energy-outlook-2023 (pristupljeno 12.03.2026.)

16 Shekhar, S., & Daniel, M. (2025). Sustainable supply chains: Leveraging AI for green logistics. ResearchGate. https://www.researchgate.net/publication/

[17] Dienagha, E.C., Digitemie I.N., Egbumokei W.N. & Oladipo, O. T. (2025). Integrating sustainability into procurement and supply chain processes in the energy sector. Gulf Journal of Advance Business Research, 3(1)

[18] Teddy, S. M., & Kumar, B. R. (2024). The future of supply chain: Innovations, best practices and key trends, Chinesa Journal of Experimental Traditional Medical fomulae, Volume 30, Issue 5

Primjena koncepcije održivog razvoja u privredi podrazumijeva svjesno i etično ponašanje preduzeća prema svim učesnicima: zaposlenim, potrošačima, dobavljačima, lokalnoj zajednici i okolini. Riječ je o pristupu koji preduzećima donosi ne samo reputacijske koristi, već i dugoročnu stabilnost kao i otpornost na promjene u zakonodavstvu, tržištu i društvenim očekivanjima. Ideja održivog razvoja, iako u savremenom smislu prepoznata tek u novijoj istoriji, ima svoje duboke korijene još u ranim ljudskim civilizacijama. Iako se sam pojam „održivi razvoj" počeo koristiti tek u 20. vijeku, temeljne misli koje stoje iza tog koncepta, kao što su ravnoteža između čovjeka i prirode i odgovorno korištenje resursa, prisutne su godinama u nazad.

Ciljevi održivog razvoja predstavljaju sveobuhvatan plan za budućnost koji obuhvata borbu protiv siromaštva, jačanje zdravstvenog sistema, osiguranje kvalitetnog obrazovanja, promociju čiste energije, očuvanje okoline i podsticanje privredno - ekonomskog rasta. Danas su oni referentna tačka za nacionalne politike, strategije poslovnih sektora i djelovanje civilnog društva u cijelom svijetu.

Osvrćući se na istoriju održivog razvoja ukazuje se na to da ovaj koncept nije prolazni trend, već logičan nastavak ljudske potrebe za ravnotežom s prirodom. Od drevnih praksi poljoprivrednog očuvanja do savremenih međunarodnih inicijativa, održivost se profiliše kao ključan odgovor na izazove današnjice i kao nada za sigurniju i kvalitetniju budućnost svih stanovnika planete. Jedna od mjera koju organizacije mogu uvesti za unapređenje ekološki prihvatljive kulture na radnom mjestu je uključivanje inicijativa za ekološku održivost u svoje funkcije ili prakse ljudskih resursa.[19]

Društveno odgovorno poslovanje (DOP; eng. Corporate Social Responsibility – CSR) koncept je koji posljednjih decenija zauzima sve važnije mjesto u teoriji i praksi poslovnog upravljanja. Kao odgovor na sve veće izazove savremenog poslovnog okruženja, poput klimatskih promjena, socijalne nejednakosti, digitalizacije i promjena u očekivanjima potrošača, CSR se transformirao iz dodatne opcije u stratešku nužnost. Prema istraživanju[20] društveno odgovorno poslovanje ima značajan pozitivan uticaj na percepciju potrošača, konkurentnost preduzeća i dugoročnu finansijsku održivost. Preduzeća koja uspješno implementiraju CSR strategije bilježe bolju reputaciju na tržištu, veće zadovoljstvo zaposlenih kao i veću lojalnost kupaca.

Kompanije sa dosljednom praksom dijaloga sa zainteresovanim stranama bolje su pripremljene za predviđanje i reagovanje na ekonomske, društvene i ekološke promjene te društvena odgovornost preduzeća postaje alat koji pomaže kompanijama u prepoznavanju i prilagođavanju tržišnim trendovima, što potvrđuju istraživanja o ulozi CSR-a u održivosti i reputaciji organizacija.[21] CSR inicijative koje su povezane s korporativnim upravljanjem, transparentnošću i uključivanjem učesnika donose veće koristi za organizaciju nego one koje su usmjerene isključivo na reputacijske aktivnosti. U tom kontekstu, CSR postaje sastavni dio korporativne strategije, a ne zasebna funkcija unutar preduzeća.[22]

Jedan od izazova u provođenja CSR-a je mjerenje njegovog učinka. Iako postoji niz međunarodnih standarda i okvira, poput Global Reporting Initiative (GRI) ili ISO 26000, još uvijek ne postoji jedinstvena i univerzalna metoda kojom bi se mogli ocijeniti svi aspekti društveno odgovornog poslovanja. Ipak, sve veći broj preduzeća odlučuje se na redovno izvještavanje o CSR aktivnostima, čime jačaju svoju transparentnost i povjerenje javnosti.

V. NAČIN MJERENJA DOP-a

Koncept društvene odgovornosti definiše se istovremeno s njegovim spajanjem s konceptom održivosti, a i jedan i drugi dobijaju na snazi kada se počnu tretirati zajedno. Društvena odgovornost preduzeća smatra se ključnim alatom za unapređenje konkurentskih prednosti, kreativnosti i inovacija, kao i za poboljšanje ugleda preduzeća u zajednici s njegovim kupcima, zaposlenima, partnerima, vladinim agencijama i nevladinim organizacijama. Društvena odgovornost smatra se aktivnim izvorom konkurentske prednosti i može se koristiti kao proaktivna poslovna strategija i efikasan marketinški alat za uspostavljanje i održavanje konkurentske prednosti.

Mjerenje društveno odgovornog poslovanja uključuje niz različitih alata i metoda koje pomažu organizacijama da kvantifikuju i analiziraju svoje aktivnosti usmjerene na ostvarivanje društveno odgovornih ciljeva. Među najvažnijim instrumentima u ovom području ističe se Indeks DOP-a. Ovi indeksi omogućavaju organizacijama, ali i učesnicima poput investitora i potrošača, da ocijene i uporede svoje rezultate u području društvene odgovornosti i održivosti na različitim nivoima. Indeks DOP-a mjeri angažman preduzeća u područjima poput ekonomske efikasnosti, socijalne odgovornosti prema zaposlenima i zajednici, te ekološke održivosti, pružajući preduzećima konkretne pokazatelje za unaprjeđenje svojih praksi.

Primjena alata pomaže organizacijama da ne samo prate svoje DOP aktivnosti, već i da razvijaju strategije koje odgovaraju specifičnom društvenom i regulatornom kontekstu zemlje, uključujući lokalne zajednice, zakonodavstvo i očekivanja potrošača. Na taj način, preduzeća mogu stvarati održive vrijednosti, jačati povjerenje i ostvarivati konkurentsku prednost unutar domaćeg i međunarodnog okruženja. U nastavku će se detaljnije opisati kako se ovi indeksi koriste u praksi, koje prednosti pružaju kao i na koji način mogu doprinijeti boljem razumijevanju i unapređenju društveno odgovornih politika unutar kompanije.

[19]Segbenya M., Evans Appiah Kissi, John Oti Amoah (2024) Green human resource management and environmental sustainability in a developing economy: Examining the mediation and moderation effect of employee personal norms and sex, Social Sciences & Humanities Open Volume 10,

[20]Licandro, O., Vázquez-Burguete, J. L., Ortigueira, L., Correa, P. (2023) Definition of Corporate Social Responsibility as a Management Philosophy Oriented towards the Management of Externalities: Proposal and Argumentation Definition of Corporate Social Responsibility as a Management Philosophy Oriented towards the Management of Externalities: Proposal and Argumentation. Sustainability, 15(13)

[21]Touitu T., Ekeh C. M., Nagwoke O., Owolabi R., (2024), Corporate Social Responsibility as A Strategic Tool for Sustainable Organizational Image and Development 2024. International Journal of Religion, Volume 5, Number 12.

[22]Nimani,A., Zeqiraj, V., i Spahija, D. (2022.). The importance of corporate social responsibility for companies: The developing market study. Journal of Governance & Regulation, 11(4)

Indeks društveno odgovornog poslovanja je sistem koji procjenjuje koliko kompanije primjenjuju društveno odgovorne prakse u svom poslovanju. On predstavlja koristan alat za investitore, potrošače i ostale učesnike jer pokazuje na koji način preduzeća upravljaju društvenim i ekološkim pitanjima te koliko doprinose održivom razvoju. Metodologija ovog indeksa temelji se na procjeni poslovanja u sedam ključnih područja, a za svako područje postoje precizni parametri koji omogućuju detaljnu evaluaciju nivoa društvene odgovornosti:

TABELA 1

Redni broj	Ključni stubovi društveno odgovornog poslovanja	
1.	Ekonomska održivost	Ovdje se prati sposobnost kompanije da dugoročno posluje profitabilno, vodeći računa o transparentnosti, poštovanju zakonskih odredbi, borbi protiv korupcije i odgovornom upravljanju finansijama
2.	Integracija DOP-a u poslovnu strategiju	DOP ne smije biti samo dodatak, već sastavni dio strategije, što znači da kompanija definiše jasne i mjerljive ciljeve društvene odgovornosti usklađene s poslovnim planovima
3.	Radna okolina	Ovaj segment uključuje zaštitu prava zaposlenih, osiguravanje sigurnih i podsticajnih radnih uslova, jednaku zastupljenost i mogućnosti za razvoj svih zaposlenih, bez diskriminacije
4.	Zaštita okoline	Podrazumijeva primjenu politika i praksi koje smanjuju negativan uticaj na okolinu, poput efikasnog korištenja resursa i smanjenja emisija štetnih gasova
5.	Tržišni odnosi	Ovdje se vrednuju etički poslovni odnosi, transparentnost prema potrošačima, poštovanje konkurencije i odgovorno komuniciranje
6.	Odnosi sa zajednicom	Naglašava se aktivno učestvovanje u životu lokalne zajednice kroz podršku inicijativama, razvoj vještina i zapošljavanje lokalnog stanovništva
7.	Politike raznolikosti i zaštite ljudskih prava	Obuhvata poštovanje osnovnih ljudskih prava, borbu protiv diskriminacije i stvaranje sigurnog, zdravog radnog okruženja

Indeks DOP-a se sastoji od upitnika koji dolazi u dvije verzije: veći upitnik sa 137 pitanja koristi se za detaljnu procjenu u većim i složenijim organizacijama, dok je manji upitnik sa 67 pitanja namijenjen manjim preduzećima koja žele pratiti svoj društveni uticaj uz ograničene resurse. Ispunjavanje ovog upitnika pomaže kompanijama da samostalno procijene svoje jake i slabe strane u području društvene odgovornosti te da odrede smjer daljeg razvoja. Dodjela nagrada unutar ovog indeksa postala je važan događaj u poslovnoj zajednici jer promoviše kontinuirani napredak i podstiče kompanije na usvajanje sve zahtjevnijih standarda društvene odgovornosti. Tako se ističu preduzeća koja daju pozitivan primjer a rezultati indeksa često su dostupni i investitorima koji žele ulagati u održive i društveno odgovorne kompanije.

VI. HUMANA EKONOMIJA

Humana ekonomija je ona vrsta ekonomije koja daje prioritet onome što ljudi stvarno rade i misle, a istovremeno se bavi potrebama čovječanstva u cjelini.[23] Teorija pretpostavlja da ljudski kapital predstavlja nematerijalno bogatstvo ugrađeno u pojedince, koje obuhvata vrijeme i vrijednost uloženu u obrazovanje i obuku, kao i oportunitetne troškove izgubljene tokom procesa učenja.[24]

U savremenom kontekstu, koncept humane ekonomije proširen je kroz ideju humanog preduzetništva (engl. humane entrepreneurship), koja integrišu društvene i ekološke ciljeve u poslovne strategije. Važna je uloga zelene tržišne orijentacije kao posredničkog mehanizma. Humane preduzetničke prakse pozitivno utiču na održivost preduzeća, posebno u uslovima visoke tehnološke turbulencije u zelenim tehnologijama. Humana ekonomija nadilazi uobičajena istraživanja zaposlenih i preduzeća, što znači da nastoji dobiti uvid u to kako karakteristike i ponašanja učesnika na dubljem nivou utiču na društveni i ekonomski razvoj te njihov uticaj na društvo.

Humana ekonomija se posmatra kao neponovljiv i jedinstven resurs specifičan za preduzeće. Zbog toga, takav resurs može biti koristan samo u svom predviđenom kontekstu. Iz te perspektive, humana ekonomija može doprinijeti uspostavljanju temeljnih vrijednosti preduzeća koje su usmjerene na društveno odgovorno poslovanje i održivi rast. Na organizacijskom nivou, ovaj proces zatim može dovesti do postizanja održivog korporativnog učinka rješavanjem društvenih problema, čime se generiršu dugoročni ekonomski rezultati. Zbog toga je humana ekonomija ključni resurs koji može osigurati povoljne uslove poslovanja kako za samu organizaciju, tako i za druge uključene strane.[25]

VII. ZAKLJUČAK

Uticaj klimatskih promjena na ekonomiju i ljudsko društvo postaje sve očigledniji, privlačeći značajnu pažnju na globalnom nivou. Kultura koja na prvo mjesto stavlja inovacije, promjene i odgovornost prema okolini omogućava zaposlenima da lakše prihvate i sprovedu zelene inicijative. U organizacijama koje već imaju kulturu koja podstiče

[23] https://www.up.ac.za/human-economyprogramme/article/16511/about-human-economy (pristupljeno 10.03.2026.)

[24] Bo Shao, Hongqi Wang,(2025), Digital economy, industrial structure advancement and human capital accumulation, Finance Research Letters Volume 83, 107727

[25] Le, T. T.(2022) How humane entrepreneurship fosters sustainable supply chain management for a circular economy moving towards sustainable corporate performance, J. Cleaner. Production, Vol. 368, 133178

transparentnost, zaposleni često osjećaju veći stepen odgovornosti prema ekološkim ciljevima, jer su te vrijednosti već integrisane u njihovo svakodnevno poslovanje. Dok u organizacijama u kojima vlada rigidna implementacija održivih praksi može doći do otpora, zbog takve situacije zelena tranzicija može da se percipira kao spoljni pritisak, odnosno nametnuta je kao promjena koja remeti uhodane poslovne procese. Zaposleni u ovim organizacijama mogu biti skeptični prema promjenama, posebno ako im nije jasno kako zelene inicijative doprinose dugoročnom poslovnom uspjehu.

Tehnologije poput sistema obnovljivih izvora energije, infrastrukture koja efikasno koristi vodu i inovativna rješenja za upravljanje otpadom pomažu da se minimizira njihov uticaj na okolinu, a da istovremeno zadovolje rastuće potrebe urbanog stanovništva. Zelena tranzicija često zahtijeva značajna početna ulaganja, ali vlade i međunarodne organizacije pružaju finansijsku podršku putem zelenih fondova, grantova i povoljnih kredita.

Od drevnih praksi poljoprivrednog očuvanja do savremenih međunarodnih inicijativa, održivost se profiliše kao ključni odgovor na izazove današnjice i kao nada za sigurniju i kvalitetniju budućnost svih stanovnika planete. Jedna od mjera koju organizacije mogu uvesti za unapređenje ekološki prihvatljive kulture na radnom mjestu je uključivanje inicijativa za ekološku održivost u svoje funkcije ili prakse kad su u pitanju ljudski resursi. Organizacije koja uspješno implementiraju CSR strategije bilježe bolju reputaciju na tržištu, veće zadovoljstvo zaposlenih kao i veću lojalnost kupaca.

Društveno odgovorno poslovanje razvija se kao praktična implementacija načela održivosti u svakodnevne poslovne procese. Ono obuhvata aktivnosti kojima preduzeća, uz ostvarivanje ekonomske koristi, doprinose razvoju lokalne zajednice, zaštiti okoline i poboljšanju kvaliteta života zaposlenih i potrošača. Takav pristup zahtijeva promjenu perspektive u korporativnom upravljanju: od orijentacije na kratkoročnu dobit prema stvaranju dugoročne vrijednosti za sve učesnike. U tom kontekstu, društveno odgovorno poslovanje ne predstavlja trošak, nego investiciju u buduću stabilnost, reputaciju i konkurentsku prednost preduzeća. Mjerenje društveno odgovornog poslovanja uključuje niz različitih alata i metoda koje pomažu organizacijama da kvantifikuju i analiziraju svoje aktivnosti usmjerene na ostvarivanje društveno odgovornih ciljeva. Među najvažnijim instrumentima u ovom području ističe se Indeks DOP-a. Dodjela nagrada unutar ovog indeksa postala je važan događaj u poslovnoj zajednici jer promoviše kontinuirani napredak i podstiče kompanije na usvajanje sve zahtjevnijih standarda društvene odgovornosti.

Humana ekonomija nadilazi uobičajena istraživanja zaposlenih i preduzeća, što znači da nastoji dobiti uvid u to kako karakteristike i ponašanja učesnika na dubljem nivou utiču na društveni i ekonomski razvoj te njihov uticaj na društvo. Kao takva predstavlja ključni resurs koji može osigurati povoljne efekte za sve strane koje su uključene.

Možemo zaključiti da održiva transformacija zahtijeva sistemsku promjenu vrijednosti, stratešku integraciju održivosti i aktivnu institucionalnu podršku.

LITERATURA

[1] Balsalobre-Lorente D., J. Abbas, C. He, L. Pilař, S.A.R. Shah (2023) Tourism, urbanization and natural resources rents matter for environmental sustainability: the leading role of AI and ICT on sustainable development goals in the digital era, Resour. Policy., 82, Article 103445, 10.1016/

[2] Bassem Kahouli, Basma Hamdi, Kamel Miled (2026) Exploring the interplay between renewable energy, agriculture, clean technologies, natural resources, and environmental sustainability, Energy Strategy Reviews Volume 64, 102057

[3] Bo Shao, Hongqi Wang,(2025), Digital economy, industrial structure advancement and human capital accumulation, Finance Research Letters Volume 83, 107727

[4] Cameron, K.S. and Quinn, R.E. (2006) Diagnosing and Changing Organisational Culture Based on Competing Values Framework. Josey Bass, San Francisco.

[5] Dienagha, E.C., Digitemie I.N., Egbumokei W.N. & Oladipo, O. T. (2025). Integrating sustainability into procurement and supply chain processes in the energy sector. Gulf Journal of Advance Business Research, 3(1), 76-104.

[6] Gulfaraz Anis a, Naila Samar Naz a, Taher M. Ghazal b, Muhammad Sajid Farooq c, Muhammad Saleem a, Chan Yeob Yeun d, Munir Ahmad e, Khan Muhammad Adnan, (2026) Smart and transparent grid stability prediction for efficient energy management using explainable AI, Energy Strategy Reviews Volume 64, 102083

[7] Jain H. (2024) From pollution to progress: groundbreaking advances in clean technology unveiled, Innovation and Green Development, 3 (2), Article 100143, 10.1016/j.igd.2024.100143

[8] Le, T. T.(2022) How humane entrepreneurship fosters sustainable supply chain management for a circular economy moving towards sustainable corporate performance, J. Cleaner. Production, Vol. 368, 133178, 2022. str. 133178.

[9] Licandro, O., Vázquez-Burguete, J. L., Ortigueira, L., Correa, P. (2023) Definition of Corporate Social Responsibility as a Management Philosophy Oriented towards the Management of Externalities: Proposal and Argumentation Definition of Corporate Social Responsibility as a Management Philosophy Oriented towards the Management of Externalities: Proposal and Argumentation. Sustainability, 15(13), 10722.

[10] Miller G. J., (2022) Stakeholder roles in artificial intelligence projects, Project Leadership and Society,Volume 3, 100068

[11] Nieke Masruchiyah, Novita Damayanti, Prasetya Yoga Santoso, Asep Marfu (2025) Harnessing green human capital and circular economy in urbanization: Advancing water resilience through resource conservation and green technology, Environmental ChallengesVolume 20,101227

[12] Nimani,A., Zeqiraj, V., i Spahija, D. (2022.). The importance of corporate social responsibility for companies: The developing market study. Journal of Governance & Regulation, 11(4)

[13] Rodrigo Lozano, 2015. A Holistic Perspective on Corporate Sustainability Drivers, Corporate Social Responsibility and Environmental Management: Volume 22, Issue 1

[14] Schein, E. H. (2010). Organizational Culture and Leadership (4th ed.). San Francisco, CA: Jossey-BassKim S. Cameron Robert E. Quinn (2006) Diagnosing and Changing Organizational Culture, John Wiley & Sons, Inc.

[15] Segbenya M., Evans A. K., Oti J. A., (2024) Green human resource management and environmental sustainability in a developing economy: Examining the mediation and moderation effect of employee personal norms and sex, Social Sciences & Humanities Open Volume 10, 101016

[16] Shekhar, S., & Daniel, M. (2025). Sustainable supply chains: Leveraging AI for green logistics. Research Gate. https: //www. researchgate.net/publication/

[17] Teddy S. M., & Kumar, B. R. (2024). The future of supply chain: Innovations, best practices and key trends, Chinesa Journal of Experimental Traditional Medical fomulae, Volume 30, Issue 5

[18] Touitu T., Ekeh C. M., Nagwoke O., Owolabi R., (2024), Corporate Social Responsibility as A Strategic Tool for Sustainable Organizational Image and Development 2024. International Journal of Religion, Volume 5, Number 12.

[19] Zhenhua Liu, Jialong Fu, Xinyang Zhang, Qiang Ji, (2026) Higher-order moment risk spillovers between the carbon and energy markets under climate policy uncertainty, Journal of Management Science and Engineering Volume 11, Issue 1, Pages 1-19

[20] https://www.pwc.com/gx/en/global-annual-review/2023/pwc-global-annual-review-2023.pdf

[21] https://www.worldbank.org/en/about/annual-report-2023

[22] https://globescan.com/2022/06/23/2022-sustainability-leaders-report/

[23] https://commission.europa.eu/strategy-and-policy/state-union/state-union-2023

[24] https://www.iea.org/reports/world-energy-outlook-2023

[25] https://www.up.ac.za/human-economyprogramme/article/16511/about-human-economy

UDK 330.322:005.334(4-672EU)
DOI 10.7251/ZRSNG2526036J

Komparativna analiza modernih investicionih strategija diversifikacije rizika

Comparative analysis of modern risk diversification investment strategies

Zoran Jović, Univerzitet Sinergija, Bijeljina

Sažetak **- Ovaj rad je istraživao evoluciju investicionih strategija u post-kriznom ekonomskom ambijentu, fokusirajući se na kritiku tradicionalnog modela pasivnog investiranja ('Kupi i Drži'), kroz analizu pristupa Ray Dalio-a, osnivača *Bridgewater Associates*, i Thomasa Kee-a, autora i tržišnog stratega. Rad je suprotstavio dva fundamentalno različita odgovora na tržišnu volatilnost. Dok Dalio rešenje pronalazi u 'Svetom gralu investiranja' — preciznoj diversifikaciji kroz nekorelisanu imovinu unutar 'All Weather' tj. portfolija za sve prilike, Kee proklamuje neodrživost strategije pasivnog držanja portfolija i zagovara aktivno upravljanje gotovinom zasnovano na makroekonomskom zamahu odnosno momentumu. Rad je analizirao efikasnost oba modela tokom istorijskih tržišnih poremećaja (2008. i 2022. godine), nudeći sintezu koja bi mogla poslužiti kao okvir za modernu alokaciju kapitala u uslovima visoke inflacije i promene monetarnih ciklusa.**

Ključne reči **- Alokacija imovine; Moderna teorija portfolija; Ublažavanje rizika; Tržišni tajming; Nekorelacija; Analiza zamaha**

Abstract **- This paper investigated the evolution of investment strategies in the post-crisis economic environment, focusing on the criticism of the traditional model of passive investing ('Buy and Hold'), by analyzing the approaches of Ray Dalio, founder of Bridgewater Associates, and Thomas Kee, author and market strategist. The paper contrasts two fundamentally different responses to market volatility. While Dalio finds the solution in the 'Holy Grail of investing' — precise diversification through uncorrelated assets within 'All Weather' ie. a portfolio for all occasions, Kee proclaims the 'death' of passive asset holding and advocates active cash management based on macroeconomic momentum. The paper analyzed the effectiveness of both models during historical market disturbances (2008 and 2022), offering a synthesis that could serve as a framework for modern capital allocation in conditions of high inflation and changing monetary cycles.**

Keywords **- Asset Allocation; Modern Portfolio Theory; Risk Mitigation; Market Timing; Non-correlation; Momentum Analysis**

I. Uvod

Tradicionalni model pasivnog investiranja poznat kao “Buy and Hold” strategija koji je dominirao u drugoj polovini XX veka i početkom XXI veka, kada je davao najbolje rezultate u praksi, više nije dovoljan. Tradicionalna strategija “kupi i drži” npr. 60% akcije i 40% obveznice, savršeno je funkcionisala u pomenutom periodu od oko 40-tak godina, jer su kamatne stope uglavnom padale, dok je globalizacija cvetala. Dalio i drugi analitičari poput Kee-a tvrde da je taj period završen [1],[2]. Akcije su danas skupe tj. uglavnom precenjene, a obveznice više ne pružaju istu zaštitu kao ranije.

U prošlosti kada bi cene akcija padale, cene obveznica bi rasle. To je bila osnova “buy and hold” strategije. Međutim, u okruženju visoke inflacije, kakva je bila recimo 2022. godine, cene i akcija i obveznica padaju istovremeno. Zbog toga pasivno držanje ova dva finansijska instrumenta više ne smanjuje rizik, pa moderni investitori napuštaju ovu strategiju [3],[4]. Diversifikacija portfolia unutar jedne klase aktive ne daje zadovoljavajuće rezultate niti smanjuje rizik i predstavlja jednu od osnovnih zamki investicione diversifikacije rizika. Česta diversifikacija portfolia unutar iste klase aktive, recimo akcija, nosi sobom visoke transakcione troškove koji umanjuju ili čak poništavaju eventualnu zaradu, a takođe kumulira rizik koji sobom nosi svaka klasa aktive ponaosob, istovremeno stvarajući privid diversifikacije i upravljanja rizicima.

Dalio [1]sugeriše da investitori treba da prestanu da budu pasivni i da počnu da uključuju imovinu koja nije u korelaciji sa akcijama, odnosno da počnu vršiti diversifikaciju uključivanjem različitih klasa aktive u svoj investicioni portfolio. Aktiva koja nije korelirana sa akcijama podrazumeva:

- Robe (Commodities) i Zlato. Oni pružaju zaštitu od inflacije koju akcije ne mogu pružiti.
- Gotovna (Cash). Ona je postala atraktivna kao privremeno utočište dok se tržišta ne redefinišu.

- Geografska diversifikacija. Izlazak iz isključivo američkih akcija tj. S&P 500 Indexa, jer se globalni odnos snaga menja zbog uspona Kine i Indije.

Dakle, u vremenu niske inflacije strategija "buy and hold" ima smisla, ali u vreme nepredvidive inflacije, inflacija postaje ubica pasivnog investiranja jer realni prinosi pasivnih portfolija postaju negativni nakon oduzimanja stope inflacije. Zbog toga se preporučuje aktivno balansiranje portfolija prema ekonomskim ciklusima, umesto pukog čekanja. U obzir treba uzimati kretanje kamatnih stopa, stopu rasta i stopu inflacije i prilagođavati portfolio njihovom kretanju umesto da se slepo veruje da će tržište akcija uvek da raste na dugi rok jer se statični porfoliji danas mogu pokazati opasnima [2].

II. Ray Dalio i arhitektura diversifikacije

Većina investitora pada u zamku diversifikacije misleći da poseduju dovoljno diversifikovan portfolio koga čine recimo 20 različitih akcija sa NYSE. Često ne shvataju da je to privid diversifikacije jer se nalaze unutar iste vrste aktive, što nosi kumulaciju rizika.

Raj Dalio, osnivač najvećeg hedž fonda na svetu *Bridgewater Associates*, smatra da diversifikacija nije samo koncept poznat pod sloganom "ne stavljajte sva jaja u jednu korpu", već mnogo šire, on kreira koncept zasnovan na matematičkoj moći smanjenja rizika bez žrtvovanja prinosa poznat pod nazivom *"Sveti gral investiranja"* [1].

Ovaj koncept polazi od Daliovog zaključka da je tajna u pronalaženju 10 do 15 nezavisnih (nekorelisanih) izvora prinosa. Matematički gledano, ako se doda imovina koja se kreće drugačije od onoga što se već poseduje, onda će ukupni rizik (volatilnost) opasti drastično, dok će očekivani prinos ostati skoro isti. Rezultat toga je bolji odnos prinosa i rizika (Sharpe Ratio). Dalio tvrdi da je sa 15 nekorelisanih investicija moguće da se rizik smanji za 80% [1]. Takođe tvrdi da su mnogi investitori u zabludi da imaju dovoljno diversifikovan portfolio jer poseduju desetine različitih akcija. Ali sve te akcije zavise od istih faktora (npr. od rasta američke ekonomije), i one mogu pasti zajedno u krizu. Prava diversifikacija zahteva imovinu koja reaguje različito na različite ekonomske uslove.

U uslovima *rasta* koji je veći od očekivanog, poželjna aktiva su akcije, robe (commodities) i korporativne obveznice.

U uslovima *recesije* poželjna aktiva su državne obveznice.

U uslovima *inflacije* koja je veća od očekivane, poželjna aktiva su zlato, robe i obveznice zaštićene od inflacije (TIPS).

U uslovima *deflacije* poželjna aktiva su gotovina i tradicionalne obveznice.

Dalio [1] je predložio koncept namenjen običnim investitorima poznat pod imenom *"Portfolio za sve vremenske prilike"* (All Weather Portfolio). Strategija je dizajnirana tako da ovaj portfolio preživi bilo koji ekonomski scenario (tzv. "ekonomska godišnja doba").

Tipična struktura ovog portfolija može se prikazati na sledeći način (tabela 1):

TABELA 1 All Weather Portfolio

Procenat	**Imovina**	**Uloga**
30%	Akcije (Stocks)	Za periode ekonomskog rasta.
40%	Dugoročne državne obveznice	Za periode pada rasta i deflacije.
15%	Srednjoročne obveznice	Stabilnost i umeren prinos.
7,5%	Zlato	Zaštita od visoke inflacije i pada valute.
7,5%	Robe (Commodities)	Zaštita od inflacije i rasta potražnje.

Ovaj Daliov pristup se zasniva na poniznosti pred tržištem. On smatra da je predviđanje budućnosti izuzetno teško i skupo. Umesto da se investitor kladi na to šta će se desiti, on treba da pravi portfolio koji je *otporan na to što ne zna šta će se desiti*. S tim u vezi poznata je i Daliova misao da je diversifikacija jedini besplatan ručak u investiranju.

Dakle, prema Daliovoj arhitekturi diversifikacije ne treba kupovati samo akcije različitih korporacija već treba kupovati različite *klase imovine* koje se nalaze u različitim delovima sveta i reaguju na različite ekonomske sile [1].

III. Thomas Kee i kraj pasivnog Investiranja

Thomas H. Kee je postavio direktan izazov tradicionalnoj investicionoj mudrosti u svom delu "Buy and Hold Is Dead" u kome zastupa neodrživost strategije pasivnog držanja portfolija. Dok Dalio [1] fokus stavlja na strukturnu diversifikaciju portfolija, Kee [2] se fokusira na vreme (tajming) i makroekonomske cikluse. Ovu tezu potvrđuju i noviji podaci o kretanju tržišta tokom 2022. godine [4], dok institucionalni modeli poput onih iz Bridgewater-a [3] nude matematički okvir za balansiranje rizika.

Kee-ova argumentacija o neodrživosti pasivnog pristupa [2] dobija dodatnu težinu kada se posmatra kroz prizmu teorije

Nassima Taleba **o** „Crnim labudovima“ [5]. Taleb dokazuje da finansijska tržišta nisu podložna normalnoj raspodeli verovatnoće, već da ekstremni, nepredvidivi događaji imaju disproporcionalno veliki uticaj na dugoročne prinose. Dok tradicionalni zagovornici pasivnog investiranja, poput Johna Bogla [6], veruju da će tržište na duge staze uvek nagraditi strpljenje, Kee upozorava da „dugi rok“ može trajati decenijama (sekularni trendovi), tokom kojih investitor može izgubiti ne samo kapital, već i vreme potrebno za oporavak.

Kee [2] tvrdi da je Bogleova filozofija [6] bila idealna za period od 1980. do 2000. godine, ali da u novoj eri povećane volatilnosti pasivno držanje portfolija postaje oblik kockanja sa makroekonomskim neizvesnostima. Umesto slepog poverenja u statističke proseke, Kee predlaže aktivnu zaštitu, jer, kako Taleb sugeriše, jedan jedini negativni „Crni labud“ može poništiti decenije stabilnog rasta [5].

Glavna teza u negovoj knjizi je da pasivno investiranje u indeksne fondove (poput S&P 500) više ne garantuje bogatstvo. On podseća na rizik od “izgubljene decenije” kakvi su bili periodi 1929-1954. i 2000-2013. kada je investitorima trebalo više od decenije da se vrate na nulu. Otuda zaključuje da ako se na tržište uđe u pogrešno vreme sa “buy and hold” strategijom, investitori mogu izgubiti svoje najbolje životne godine za postizanje uspeha [2].

Umesto toga, Kee [2] zagovara strategiju zasnovanu na gotovini (Cash-Based Strategy), prema kojoj umesto da se uvek bude 100% investirano, treba pribeći aktivnom upravljanju baziranom na dva postulata: *kešu kao poziciji* gde gotovina nije samo sredstvo za kupovinu, već aktivna odbrambena pozicija i *rotaciji* koja podrazumeva da investitor mora znati kada da izađe sa tržišta i čeka u kešu dok se uslovi ne poprave. Pod gotovinom se ne podrazumevaju samo fizičke novčanice, već finansijski instrumenti koji omogućavaju očuvanje glavnice uz minimalni prinos. Tu se prvenstveno misli na Trezorske zapise (T-Bills) odnosno kratkoročni državne hartije od vrednosti sa rokom dospeća od 3 do 6 meseci i na Fondove tržišta novca tj. Many Market fondove koji ulažu u najlikvidnije i najsigurnije hartije od vrednosti. Nasuprot ovome, pojedini autori poput Malkiela [7] i Asnessa [8] upozoravaju na drugu stranu medalje aktivnog tajminga Kee-a koji može da bude veoma težak za prosečnog investitora. Malkiel tvrdi da su tržišta fundamentalno efikasna i da su pokušaji tajminga dugoročno osuđeni na neuspeh zbog transakcionih troškova i nepredvidivosti kratkoročnih fluktuacija. Iz Malkielove perspektive, Kee-ova strategija napuštanja tržišta mogla bi rezultirati propuštanjem najboljih dana oporavka, što dramatično umanjuje ukupni prinos. Asness priznaje da su godine poput 2022. bolne, ali argumentuje da je to statistička anomalija, a ne trajni kraj diversifikacije. On smatra da je Daliov „All Weather“ pristup i dalje superioran jer se oslanja na dugoročne ekonomske zakonitosti, a ne na pokušaje da se „nadmudri“ tržišni momentum, što Asness vidi kao visokorizičan poduhvat.

Kee [2] uvodi koncept koji naziva Ekonomski ciklus tržišta kapitala (The Economic Cycle of the Stock Market) koji u fokus stavlja fundamentalne makro pokretače. On smatra da investitori moraju pratiti *kretanje kamatnih stopa* (FED) jer su one primarni pokretač cena na tržištu kapitala i *zarade kompanija naspram procena* (Valuations) jer ako su akcije preskupe u odnosu na istorijske proseke, onda “buy and hold” strategija postaje recept za investicionu katastrofu.

1) Kee u svojoj strategiji investiranja ne koristi komplikovane algoritme, već se oslanja na makroekonomske indikatore koji signaliziraju promenu dugoročnog trenda. Cilj ove strategije je da se izbegnu veliki padovi koji uništavaju portfolije koji su kreirani na bazi strategije “buy and hold”.

2) On koristi četiri osnovna signala sa tržišta za donošenje investicionih odluka:

1. *Odnos cene i zarade* (P/E Ratio) u odnosu na istorijske vrednosti. Ako je tržište, oličeno kroz npr. Index S&P 500, istorijski skupo tj. ako je visok racio P/E onda je to signal za izlazak sa tržišta, odnosno ekstremno visoki nivoi racia P/E predstavljaju crvenu zastavicu za investitore, jer ukazuju na visoke cene akcija u odnosu na realne zarade kompanija i to je znak da je rizik “buy and hold “ strategije nadalje neprihvatljiv. Sa psihološkog aspekta, od investitora se zahteva mentalna snaga da ne kupuje na tržištu koje se nalazi na vrhu balona, iako postoji veliki pritisak javnog mnjenja na tržištu da će cene i dalje rasti.

2.*Politika FED-a* (kamatne stope). Kee prati likvidnost koju diktira centralna banka (FED). Ovaj parametar daje signale za izlazak i ulazak na tržište. *Signal za izlazak* sa tržišta nastaje kada FED počne agresivno da podiže kamatne stope kako bi obuzdao inflaciju. Kee tumači taj trenutak kao kraj “jeftinog novca” koji je dotle gurao cene akcija naviše. Signal za ulazak na tržište nastaje tek kada ciklus podizanja kamatnih stopa stane ili krene naniže, a tržište se “očisti” od nerealnih cena.

3.*Pratiti trend, ne prognozu* (Trend Following). Umesto da pogađa i prognozira kada će cene dosegnuti dno na tržištu, Kee koristi tehničke indikatore promene smera trenda na tržištu. Da bi potvrdio promenu smera tržišnog trenda on koristi pravilo 200-dnevnog proseka. Ako ce cena berzanskog indeksa spusti ispod svog proseka u poslednjih 200 dana i tu ostane, onda je to jasan signal da se prekine “buy and hold” strategija i da se prelazi u keš poziciju. Ponovni ulazak na tržište odnosno ponovna kupovina berzanskih efekata se dešava tek kada se trend ponovo uspostavi iznad ključnih proseka, čak iako to znači da se propušta 5-10% oporavka, odnosno rasta cena, jer je to neophodno zbog bezbednosti tj. savladavanja rizika kratkotrajne oscilacije trenda.

4.*Relativna snaga* (Relative Strenght). Kee traži ulaganje u sektore koji pokazuju snagu čak i kada je ostatak tržišta u problemu. Ako nijedan sektor ne pokazuje snagu, onda on zagovara tržišnu poziciju koja je 100% u gotovini. Praktičan

rezime strategije Tomasa Kee-a može se prikazati tabelarno (tabela 2):

TABELA 2 Strategija Thomasa Kee-a

Faza	Akcija prema Kee-u
Ekspanzija (Niske kamate, rast zarada)	Investiran u akcije (ETFs).
Pregrevanje (Visok P/E, FED počinje da steže)	Počinje postepeni izlazak u keš.
Pad (Medveđe tržište)	Čeka u kešu. Ne "dokupljuje dno" (averaging down).
Oporavak (Nove valuacije, stabilan trend)	Ponovni ulazak sa zaštitnim stop-loss nalozima.

U suštini Tomas Kee tvrdi da je vreme u kojem je bilo dovoljno samo kupiti i čekati da tržište uradi svoje, sada prošlost. Moderni investitor po njemu mora da bude taktičan, da prati makroekonomske pokazatelje i da bude spreman da se povuče sa tržišta kada su rizici previsoki.

Poređenjem Dalija i Kija može se konstatovati da se obojica slažu da je tradicionalni model 60/40 u problemu, ali se njihova rešenja razlikuju (tabela 3):

TABELA 3. Razlika između Dalija i Kija

Autor	Rešenje	Filozofija
Ray Dalio	Diversifikacija	"Ne znam šta će biti, zato posedujem sve što se kreće različito."
Thomas Kee	Tajming (Vreme)	"Znam da su ciklusi loši, zato ću biti u kešu dok se oluja ne završi."

IV. Analiza i diskusija

Da bi se proverile praktične performanse ove dve strategije investiranja interesantno je analizirati specifične podatke o prinosima ovih dvaju strategija tokom prošlih kriza 2008. i 2022. godine. Na osnovu istorijskih pokazatelja dolazi se do zaključka o prednostima i slabostima jedne i druge strategije.

1. *Globalna finansijska kriza 2008*. Pokazala je trijumf strategije diversifikacije. Tokom 2008. godine kada je berzanski Index S&P 500 pao za oko 37%, ove dve strategije su pokazale svoju moć na različite načine:

-Daliov "All Weather" pristup je u velikoj alokaciji u dugoročnim državnim obveznicama, (čije su cene rasle dok su cene akcija padale), i u zlatu, zahvaljijući čemu je ovaj portfolio zabeležio minimalan pad (procenjuje se na manje od 4%). Time je Dalio dokazao da nekorelisana imovina pruža dovoljan buffer u kriznim periodima povišenog rizika.

-Kee-ov "Momentum" pristup govori da bi Kee prema svojim pravilima dobio signal za izlazak čim je S&P 500 probio 200-dnevni prosek krajem 2007. ili početkom 2008 [2]. Pristalice njegove strategije bi veći deo krize proveli u kešu, tačnije u T-Bills (Trezorskim zapisima), zarađujući tadašnjih 2-3% kamate, dok su ostali gubili bogatstvo.

2.*Inflatorni šok 2022.* Ovo je primer kada diversifikacija zakaže. Ova godina je ključna za razotkrivanje mane tradicionalne diversifikacije, čime je dala vetar u leđa Kee-ovoj teoriji o neodrživosti strategije pasivnog držanja portfolija.

-Problem za Dalija: U 2022. godini zbog rasta kamatnih stopa i inflacije, cene i akcija i obveznica su padale istovremeno. Tradicionalni 60/40 portfolio je zabeležio jednu od najgorih godina u istoriji. Čak je "All Weather" koncept nekorelisane strukture portfolija trpeo lošije performanse jer obveznice koje čine 55% portfolija nisu služile kao zaštita.

-Trijumf za Kija: U ovoj godini Kee-ova strategija dobija potvrdu na finansijskom tržištu. Njegov model ne čeka da obveznice spasu akcije. On uviđa da oba trenda idu naniže i seli kapital 100% u keš. Tako, dok su diversifikovani investitori gubili 15-20%, Investitori koji su primenjivali Kee-ov koncept su bili na nuli ili u blagom plusu zbog rasta kamatnih stopa na keš.

Analiza kriznih perioda 2008. i 2022. godine otkriva suštinsku razliku ovih strategija. Dok je Daliov model superioran u deflatornim recesijama poput one 2008. godine, gde obveznice balansiraju pad cena akcija, on postaje ranjiv u ambijentu visoke inflacije kada korelacije postaju pozitivne. Nasuprot tome Kee-ova strategija nudi veću zaštitu u scenarijima "savršene oluje" poput one 2022. godine jer prepoznaje da je u određenim ciklusima jedina prava diversifikacija zapravo potpuni izlazak u gotovinu. Time Kee potvrđuje svoju tezu da pasivno držanje imovine, bez obzira na njenu raznovrsnost,

može biti fatalno ako investitor ignoriše makroekonomski momentum.

V. ZAKLJUČAK

Komparativnom analizom modernih investicionih strategija diversifikacije rizika u procesu upravljanja portfolijom Ray Dalio-a i Thomasa Kee-a, mogu se sumirati sve prednosti i mane obe strategije u jednom tabelarnom prikazu (tabela 4):

TABELA 4. Uporedni pregled: Dalio vs. Kee

Karakteristika	**Ray Dalio (All Weather)**	**Thomas Kee (Buy and Hold Is Dead)**
Osnovna filozofija	Pasivna diversifikacija: Uvek si na tržištu, ali u svemu.	Aktivni tajming: Na tržištu si samo kada je trend pozitivan.
Glavni alat	Nekorelisanost: Imovina koja se kreće u suprotnim smerovima.	Momentum: Praćenje 200-dnevnog proseka i FED politike.
Uloga gotovine (Cash)	"Cash is trash" (dugoročno gubi vrednost).	"Safe Haven": Legitimna investiciona pozicija za zaštitu.
Najbolji scenario	Deflatorna recesija (rast obveznica balansira pad akcija).	Tržišni krahovi i "medveđa" tržišta (izlazak u keš na vreme).
Najveći rizik	Inflatorni šok: Kada i akcije i obveznice padaju zajedno (npr. 2022).	"Whipsaw": Lažni signali gde izađeš, a tržište odmah skoči nazad.
Psihologija	Mirnoća kroz balansiranje (manja volatilnost).	Disciplina kroz pravila (spremnost na radikalne rezove).

Dok Dalio nudi arhitekturu portfolija koji je dizajniran da preživi sve ekonomske sezone, Kee nudi navigaciju kojom se izbegavaju najopasnije tržišne oluje. Istraživanje sprovedeno u ovom radu ukazuje na to da su tradicionalne investicione paradigme pred ozbiljnim izazovom. Doktrina „kupi i drži“ (Buy and Hold), koja je decenijama bila zlatni standard, pokazuje znake zamora u uslovima povišene inflacije i promene režima kamatnih stopa. Analizirajući pristupe Raya Dalia i Thomasa Kee-a, dolazimo do zaključka da stabilnost više ne leži u pasivnosti, već u adaptivnosti.

Daliov doprinos kroz koncept pariteta rizika [1] ostaje temelj svakog racionalnog portfolija. Njegova teza da je diversifikacija jedini „besplatan ručak“ na berzi naučno je potkrepljena i institucionalno dokazana [3]. Međutim, Kee-ova argumentacija o „smrti“ pasivnog modela [2] unosi neophodnu dozu pragmatizma. U svetu gde korelacije između različitih klasa imovine teže jedinici tokom kriza (kao što je viđeno 2022. godine [4]), puko posedovanje različite imovine nije dovoljno.

Za savremenog investitora, najefikasnije rešenje bi moglo ležati u *hibridnom modelu*: korišćenje Daliovih principa diversifikacije unutar portfolija koji može da izdrži različite ekonomske sezone, uz primenu Kee-ovih momentum signala za povremenu zaštitu kapitala u ekstremnim makroekonomskim uslovima, odnosno spremnost na privremeni prelazak u likvidna sredstva kada se prekrše ključni nivoi podrške tržišta.

Budućnost investiranja u 2026. godini i dalje zahteva prelazak sa statične na dinamičnu alokaciju. Cilj više nije samo „pobediti tržište“, već preživeti njegove najekstremnije periode bez trajnog gubitka kapitala. Spajanjem ova dva naizgled suprotstavljena pristupa, investitor dobija ono najbolje iz oba koncepta: robusnost strukture i fleksibilnost odgovora na tržišne promene.

LITERATURA

[1] R. Dalio, *Principles: Life and Work*. New York, NY, USA: Simon & Schuster, 2017.

[2] T. H. Kee, Jr., *Buy and Hold Is Dead: Profit Using Momentum Analysis*. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2011.

[3] Bridgewater Associates, "The All Weather Strategy," Bridgewater White Paper, Dec. 2019.

[4] M. Somerset Webb, "Why Buy and Hold Is Dead," *Bloomberg Wealth*, Nov. 23, 2022.

[5] N. N. Taleb, *The Black Swan: The Impact of the Highly Improbable*. New York, NY, USA: Random House, 2007.

[6] J. C. Bogle, *The Little Book of Common Sense Investing: The Only Way to Guarantee Your Fair Share of Stock Market Returns*. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2017.

[7] B. G. Malkiel, *A Random Walk Down Wall Street: The Time-Tested Strategy for Successful Investing*. New York, NY, USA: W. W. Norton & Company, 2023.

[8] C. S. Asness, "The 60/40 Portfolio Is Dead! Long Live the 60/40 Portfolio," *AQR Capital Management*, White Paper, Jan. 2024.

UDK 657.6:[339.13:336.763(497.6)
DOI 10.7251/ZRSNG2526042J

Implikacije kreativnog računovodstva na procjenu investicionog rizika i (ne)stabilnost finansijskog sistema

Implications of Creative Accounting on the Assessment of Investment Risk and the (In)Stability of the Financial System

Mladen Jovanović, Ekonomski fakultet Pale, Univerzitet u Istočnom Sarajevu

***Sažetak* — Kreativno računovodstvo predstavlja praksu kojom se, koristeći fleksibilnost računovodstvenih standarda i druge regulative, manipuliše finansijskim izvještajima kako bi se prikazao povoljniji imovinski, prinosni i finansijski položaj preduzeća nego što on zaista jeste. Primjenom takvih praksi menadžment preduzeća nastoji privući potencijalne investitore, koji se prilikom donošenja odluka oslanjaju na iskrivljene finansijske izvještaje. U radu su razmotrene implikacije kreativnog računovodstva na procjenu investicionog rizika i (ne)stabilnost finansijskog sistema putem kvalitativne analize. Rezultati analize pokazuju da kreativno računovodstvo, utičući na procjenu investicionog rizika, a samim tim i na povjerenje investitora, može dovesti do nestabilnosti cjelokupnog finansijskog sistema. Takođe, u radu su predstavljeni i regulatorni i etički aspekti kreativnog računovodstva kao manipulativne prakse.**

***Ključne riječi* — kreativno računovodstvo; finansijski izvještaji; investicioni rizik; (ne)stabilnost finansijskog sistema; profesionalna regulativa; etika.**

***Abstract* — Creative accounting is a practice that, using the flexibility of accounting standards and other regulations, manipulates financial statements in order to present a more favorable property, income, and financial position of the company than it really is. By applying such practices, company management tries to attract potential investors who rely on distorted financial statements when making decisions. The paper discusses the implications of creative accounting on the assessment of investment risk and the (in)stability of the financial system through qualitative analysis. The results of the analysis show that creative accounting, affecting the assessment of investment risk, and therefore the confidence of investors, can lead to the instability of the entire financial system. Also, the paper presents the regulatory and ethical aspects of creative accounting as a manipulative practice.**

***Keywords* — creative accounting; financial statements; investment risk; (in)stability of the financial system; professional regulation; ethics.**

I. UVOD

Finansijski izvještaji predstavljaju jedan od osnovnih izvora informacija za investitore i druge učesnike na finansijskim tržištima, jer omogućavaju procjenu imovinskog, prinosnog i finansijskog položaja preduzeća, što je od izuzetne važnosti za procjenu investicionog rizika pri donošenju racionalnih ekonomskih odluka. Pouzdanost i transparentnost finansijskih informacija od suštinskog je značaja za efikasno funkcionisanje finansijskog sistema, budući da je povjerenje učesnika osnovni faktor njegove (ne)stabilnosti. Primjena određenih računovodstvenih praksi, poput kreativnog računovodstva, može uticati na fer i istinito finansijsko izvještavanje, kao i na preciznost procjene investicionog rizika. Takve manipulacije ne utiču samo na pojedinačne investicione odluke, već mogu imati šire negativne implikacije na funkcionisanje finansijskih tržišta i (ne)stabilnost finansijskog sistema u cjelini.

Cilj ovog rada je da razmotri način na koji kreativno računovodstvo utiče na pouzdanost finansijskih izvještaja, procjenu investicionog rizika i (ne)stabilnost finansijskog sistema u cjelini, te da naglasi važnost profesionalne regulative i etike u minimiziranju potencijalnih negativnih posljedica takvih praksi. Rad je strukturiran u četiri međusobno povezana dijela. Prvi dio rada posvećen je pojmu kreativnog računovodstva, drugi analizira njegov uticaj na procjenu investicionog rizika, treći razmatra implikacije kreativnog računovodstva na (ne)stabilnost finansijskog sistema, dok četvrti dio ispituje regulatorne i etičke aspekte. Na kraju rada iznose se zaključna razmatranja.

II. POJAM KREATIVNOG RAČUNOVODSTVA

Kreativno računovodstvo predstavlja jedan od značajnijih fenomena savremenog finansijskog izvještavanja, a sam termin prvi put je upotrijebio Argenti još 1973. godine. Javlja

se kao rezultat fleksibilnosti računovodstvene regulative i mogućnosti izbora između različitih računovodstvenih metoda, ali i odluka menadžmenta o načinu njihove primjene u konkretnim poslovnim situacijama. U stručnoj literaturi kreativno računovodstvo se najčešće povezuje sa praksom u kojoj se finansijski izvještaji prilagođavaju kako bi prikazali povoljniju sliku poslovanja preduzeća. Takva praksa može uključivati različite metode vrednovanja imovine i obaveza, korigovanje računovodstvenih procjena i različite načine priznavanja prihoda i rashoda, a sve u cilju prezentovanja povoljnijeg imovinskog, prinosnog i finansijskog položaja preduzeća.

Pojam kreativnog računovodstva se u stručnoj literaturi definiše na više različitih načina, što ukazuje na izuzetnu važnost njegovog razumijevanja, naročito u kontekstu savremenog poslovnog okruženja. Tako, prema Abed i saradnicima [1], kreativno računovodstvo je praksa koja utiče na finansijske pokazatelje korišćenjem računovodstvenog znanja i pravila koja eksplicitno ne krše računovodstvene politike, pravila i zakone. Slično tome, Gudev [2] računovodstvene prakse koje prate određene propise i standarde, ali odstupaju od onoga što ti propisi i standardi teže da postignu, naziva kreativnim računovodstvom. Kako navode Fejzić i Halilčević [3], kreativno računovodstvo je granica između alternativnih pristupa koje dopušta zakonodavstvo i lažnog finansijskog izvještavanja. Nešto iscrpniju definiciju od prethodno navedenih dao je Floştoiu [4], navodeći da kreativno računovodstvo uključuje manipulaciju računovodstvenim brojkama u finansijskim izvještajima i njihovo transformisanje u skladu sa skrivenim interesima menadžmenta privrednog subjekta, koristeći postojanje praznina u pravilima, fleksibilnost pravila i neke zakonske i za posao specifične praznine.

Kreativno računovodstvo moguće je klasifikovati na različite načine, ali se posebno ističe klasifikacija koju su dali Đorđević i Mitić [5], prema kojoj se ono dijeli na kozmetičko (pozitivno, „bijelo“) i stvarno (negativno, „crno“) kreativno računovodstvo. Prvi tip odnosi se na situaciju u kojoj preduzeće, pridržavajući se računovodstvene regulative, manipuliše vremenskim ograničenjima bez uticaja na tokove gotovine, dok drugi uključuje manipulacije koje utiču i na tokove gotovine s ciljem upravljanja periodičnim rezultatom. Razumije se, stvarno kreativno računovodstvo nosi izraženije negativne efekte.

Kada je riječ o formama koje kreativno računovodstvo može poprimiti, Budić [6] navodi sljedeće: upravljanje zaradom, nasilno (agresivno) računovodstvo, izglađivanje zarade i lažiranje finansijskih izvještaja.

III. UTICAJ KREATIVNOG RAČUNOVODSTVA NA PROCJENU INVESTICIONOG RIZIKA

Procjena rizika investicije predstavlja ključni element u procesu donošenja investicionih odluka. Investitori prilikom donošenja odluka o ulaganju kapitala nastoje procijeniti koliko je određena investicija sigurna, odnosno kolika je vjerovatnoća ostvarivanja očekivanog prinosa u odnosu na moguće gubitke, pri čemu se u velikoj mjeri oslanjaju na informacije sadržane u finansijskim izvještajima preduzeća. Kompletan set finansijskih izvještaja predstavlja značajan izvor informacija o finansijskom položaju, rezultatima poslovanja, novčanim tokovima, promjenama na kapitalu preduzeća i slično, što omogućava investitorima da procijene isplativost i rizik potencijalnog ulaganja.

Finansijski izvještaji imaju ključnu ulogu u procjeni investicionog rizika jer omogućavaju analizu finansijskih pokazatelja kao što su profitabilnost, likvidnost, zaduženost, stabilnost novčanih tokova i efikasnost poslovanja. Investitori na osnovu tih pokazatelja formiraju prognoze o budućem poslovanju preduzeća i procjenjuju vjerovatnoću ostvarivanja očekivanih prinosa. U tom kontekstu, menadžment preduzeća nerijetko nastoji "uljepšati" informacije sadržane u finansijskim izvještajima, budući da na taj način može povećati privlačnost preduzeća za potencijalne investitore. Kako navodi Kareem [7], ekonomske jedinice nastoje da prikažu najbolju sliku finansijskog položaja kako bi izrazile stepen svoje ekonomske stabilnosti, jer to direktno utiče na njihovu vrijednost, što se jasno vidi u cijenama njihovih akcija na tržištu i količini rizika koju investitori i zajmodavci procjenjuju na osnovu informacija objavljenih u finansijskim izvještajima ekonomske jedinice.

Međutim, primjena kreativnog računovodstva može dovesti do nepouzdanih finansijskih izvještaja. Potencijalni investitori se oslanjaju na objavljene finansijske informacije kako bi procijenili finansijsko zdravlje i perspektivu poslovanja preduzeća, ali ukoliko se radi o iskrivljenim informacijama, procjena rizika investicije može biti pogrešna. U skladu sa tim, Horaicu i saradnici [8] ističu da kreativno računovodstvo smanjuje pouzdanost prijavljenih informacija i potkopava sposobnost zainteresovanih strana da donose informisane ekonomske odluke. Kada su informacije nepouzdane ili djelimično prikazane investitori mogu precijeniti stabilnost i profitabilnost preduzeća, što dovodi do pogrešne procjene rizika koji je presudan za donošenje konačne investicione odluke.

Jedan od najznačajnijih efekata kreativnog računovodstva jeste naglašena informaciona asimetrija između menadžmenta preduzeća i potencijalnih investitora. Menadžment preduzeća ima direktan uvid u stvarno stanje poslovanja, dok investitori uglavnom raspolažu samo javno dostupnim finansijskim izvještajima, na osnovu kojih i donose svoje investicione odluke. Kreativno računovodstvo dodatno produbljuje informacionu asimetriju jer omogućava menadžment timu da oblikuje finansijske informacije na način koji poslovanje konkretnog preduzeća predstavlja stabilnijim i profitabilnijim nego što ono zaista jeste. Kao rezultat toga, potencijalni investitori mogu "zagristi mamac", odnosno donijeti odluke koje ne odražavaju stvarni nivo rizika i koje se kasnije mogu pokazati kao pogrešne.

U uslovima primjene kreativnog računovodstva, procjena investicionog rizika postaje znatno složeniji proces koji zahtijeva širi analitički pristup i veću pažnju prilikom interpretacije informacija sadržanih u javno dostupnim finansijskim izvještajima. Ahmed [9] naglašava da takve prakse smanjuju kredibilitet finansijskih izvještaja i njihovu korisnost za informisano donošenje odluka. Investitori su

često primorani da, pored standardne analize finansijskih izvještaja, uzmu u obzir i druge relevantne pokazatelje, kao što su trendovi poslovanja kroz duži vremenski period, uporedni pokazatelji u odnosu na druga preduzeća u istoj djelatnosti, opšti uslovi poslovanja u određenom sektoru, ali i opšti ekonomski uslovi i slično. Takav pristup omogućava realniju procjenu rizika investicije od one koja bi bila zasnovana isključivo na (iskrivljenim) finansijskim izvještajima.

Iz svega navedenog proizilazi da primjena kreativnog računovodstva može imati značajan uticaj na procjenu investicionog rizika, budući da način prezentacije finansijskih informacija utiče na percepciju finansijske stabilnosti preduzeća i nivo rizika koji investitori pripisuju potencijalnom ulaganju. Stoga je razumijevanje uticaja kreativnog računovodstva od izuzetnog značaja za realnu procjenu investicionog rizika i donošenje racionalnih investicionih odluka.

IV. UTICAJ KREATIVNOG RAČUNOVODSTVA NA (NE)STABILNOST FINANSIJSKOG SISTEMA

Finansijski sistem podrazumijeva skup finansijskih tržišta i institucija, kao i regulative i tehnika kojima se usmjerava nivo kamatnih stopa i trgovanje finansijskim instrumentima. Kao takav, on predstavlja jedan od ključnih preduslova za održivo funkcionisanje savremene ekonomije. Stabilnost finansijskog sistema podrazumijeva sposobnost finansijskih tržišta i institucija da obavljaju svoje osnovne funkcije čak i u uslovima ekonomskih šokova, finansijskih poremećaja ili povećane naizvjesnosti, a u velikoj mjeri zavisi od dostupnosti pouzdanih finansijskih informacija, budući da počiva na povjerenju investitora kao učesnika.

Kao što se može vidjeti na Slici 1, posljedice primjene kreativnog računovodstva ne zadržavaju se samo na nivou pojedinačnih investitora i investicionih odluka, već mogu imati znatno šire implikacije. Kada se prakse kreativnog računovodstva pojavljuju u većem broju preduzeća, njihovi efekti mogu uticati na funkcionisanje finansijskih tržišta i (ne)stabilnost sistema u cjelini. Kako navode Bouzidi, Sadani i Merkhoufi [10], kreativne računovodstvene prakse mogu iskriviti informacije i dovesti do pogrešnih investicionih odluka, ugrožavajući stabilnost finansijskog sistema.

Kada investitori donose odluke zasnovane na informacijama koje su iskrivljene primjenom kreativnog računovodstva, procjena rizika postaje nepouzdana, a odluke često pogrešne. Takve odluke mogu uključivati prekomjerno ulaganje u preduzeća čija je finansijska snaga precijenjena, koja zbog manipulisanih finansijskih izvještaja djeluju kao privlačna investiciona prilika. Posljedica toga nisu samo finansijski gubici pojedinačnih investitora, već i postepeno narušavanje povjerenja u finansijsko izvještavanje kao osnove za donošenje racionalnih investicionih odluka. Povjerenje, kao ključni faktor ukupne (ne)stabilnosti finansijskog sistema, formira se tokom dugog perioda, kroz transparentne i pouzdane informacije, ali se vrlo lako gubi kada se otkriju manipulacije ili druge neetične računovodstvene prakse.

Slika 1. Uticaj kreativnog računovodstva na (ne)stabilnost finansijskog sistema

Izvor: obrada autora.

Povjerenje investitora predstavlja temelj efikasnog funkcionisanja finansijskih tržišta i kada je ono na zavidnom nivou, investitori su spremni da alociraju kapital, cijene finansijskih instrumenata odražavaju realne rizike, a tržište kapitala funkcioniše stabilno i predvidivo. Suprotno tome, gubitak povjerenja izaziva povećanu volatilnost tržišta i dovodi do lančanih efekata destabilizacije, čime se povećava sistemski rizik. Baisla i saradnici [11] navode da se takozvana erozija povjerenja pretvara u čvrste promjene ponašanja kao što su povraćaj investicija, diverzifikacija radi smanjenja rizika ili okretanje ka preduzećima koja se smatraju transparentnijim. U uslovima nesigurnosti i nepouzdanih finansijskih informacija, investitori se najčešće povlače ili preusmjeravaju sredstva u sigurnije investicije, što može dovesti do slabljenja likvidnosti finansijskog sistema.

U krajnjem ishodu, kontinuirani i masovni gubitak povjerenja ugrožava efikasnost kompletnog finansijskog sistema, jer on počiva na međusobnom povjerenju učesnika da su informacije istinite i pouzdane i da finansijske institucije funkcionišu predvidivo. Bez povjerenja, finansijski tokovi se usporavaju, rizici se pogrešno procjenjuju, a sposobnost finansijskog sistema da apsorbuje šokove i održi stabilnost značajno opada. Zbog toga je održavanje povjerenja investitora i fer i istinito finansijsko izvještavanje ključno za dugoročnu stabilnost i funkcionalnost finansijskih tržišta, a svaka praksa koja narušava pouzdanost informacija direktno povećava rizik od destabilizacije cjelokupnog finansijskog sistema.

V. REGULATORNI I ETIČKI ASPEKTI

Pojava kreativnog računovostva u velikoj mjeri je povezana sa načinom na koji su postavljeni regulatorni okviri finansijskog izvještavanja. Računovodstveni standardi definišu pravila za priznavanje i prezentaciju finansijskih informacija, ali u praksi često ostavljaju određeni prostor za profesionalnu procjenu. Upravo taj prostor može biti iskorišćen za različita tumačenja računovodstvenih pravila, što može dovesti do primjene kreativnog računovodstva. Zbog toga regulatorni okvir ima ključnu ulogu u uspostavljanju jasnih pravila i mehanizama nadzora koji treba da ograniče mogućnost manipulacije finansijskim izvještajima i osiguraju njihovu pouzdanost. U tom kontekstu, značajnu ulogu ima revizija finansijskih izvještaja. Revizori procjenjuju da li su finansijski izvještaji sastavljeni u skladu sa važećom računovodstvenom regulativom i da li pružaju fer i istinit prikaz imovinskog, prinosnog i finansijskog položaja preduzeća. Međutim, važno je naglasiti da revizija pruža razumno, a ne apsolutno uvjerenje o tačnosti finansijskih izvještaja, što znači da ni revizija ne može u potpunosti eliminisati mogućnost postojanja kreativnog računovodstva ili drugih nepravilnosti (neetičnih računovodstvenih praksi).

Pored regulatornog okvira, izuzetno važnu ulogu imaju etički principi koji uređuju ponašanje profesionalaca u računovodstvu. Zhang [12] ističe da je etičko ponašanje temelj računovodstvene profesije, jer poštovanje etičkih principa omogućava očuvanje javnog povjerenja i kredibiliteta finansijskih informacija, što je ključno za stabilnost i funkcionisanje finansijskog sistema. Ukoliko profesionalni integritet izostane, čak i formalno ispravna primjena računovodstvenih pravila može biti iskorišćena za prikrivanje stvarnog finansijskog stanja preduzeća. Zbog toga mnogi autori naglašavaju potrebu za snažnijim regulatornim mehanizmima i višim etičkim standardima u računovodstvenoj profesiji. Mailani i saradnici [13] ukazuju na to da su strožiji nadzor, jasna pravila i računovođe sa visokim etičkim standardima ključni kako bi se spriječila zloupotreba kreativnog računovodstva. Istovremeno, dodatni problem predstavlja činjenica da je u praksi često zahtjevno jasno razgraničiti legitimne računovodstvene postupke od manipulativnih praksi. Prema Kaaya [14], veoma je teško podvući granicu između prevara povezanih sa finansijskim izvještajima i kreativnog računovodstva, jer su gotovo nerazlučive.

Upravo zbog toga regulatorni i etički aspekti predstavljaju ključne elemente u ograničavanju negativnih efekata kreativnog računovodstva. Jasna pravila, efikasan nadzor i visoki etički standardi doprinose transparentnosti finansijskih izvještaja i smanjuju prostor za manipulaciju, čime se jača povjerenje u finansijske informacije i stabilnost finansijskog sistema u cjelini.

VI. ZAKLJUČAK

Kreativno računovodstvo predstavlja kompleksan fenomen savremenog finansijskog izvještavanja koji proizilazi iz fleksibilnosti i određenih nedorečenosti u računovodstvenoj regulativi. Iako se određeni oblici kreativnog računovodstva mogu smatrati legitimnim u okviru dozvoljene profesionalne procjene, njegova zloupotreba može dovesti do iskrivljenog prikaza imovinskog, prinosnog i finansijskog položaja preduzeća. Zbog toga je razumijevanje ovog fenomena od posebnog značaja za sve učesnike finansijskog sistema.

U radu je ukazano na to da finansijski izvještaji predstavljaju osnovni izvor informacija na osnovu kojeg potencijalni investitori procjenjuju rizik investicionih odluka. Kada se u finansijskim izvještajima primjenjuju prakse kreativnog računovodstva, dolazi do smanjenja pouzdanosti prezentovanih informacija, što može dovesti do pogrešne procjene rizika i donošenja neadekvatnih investicionih odluka. Takve prakse dodatno produbljuju informacionu asimetriju između menadžmenta preduzeća i eksternih korisnika finansijskih izvještaja, čime se narušava transparentnost poslovanja.

Negativni efekti kreativnog računovodstva ne zadržavaju se samo na nivou pojedinačnih investicionih odluka. Kada su takve prakse prisutne u većem broju preduzeća, negativne implikacije mogu se prenijeti na šire finansijsko tržište i uticati na stabilnost finansijskog sistema. Nepouzdane finansijske informacije mogu dovesti do pogrešne alokacije kapitala, povećanja neizvjesnosti na tržištu i gubitka povjerenja investitora, koje je osnovni faktor (ne)stabilnosti finansijskog sistema. Zbog toga je uloga profesionalne računovodstvene regulative i etičkih principa od posebnog značaja. Jasno definisana pravila finansijskog izvještavanja, efikasan nadzor i odgovorno profesionalno ponašanje računovođa doprinose povećanju transparentnosti finansijskih informacija i smanjenju mogućnosti zloupotrebe kreativnog računovodstva. Poseban značaj ima i revizija finansijskih izvještaja, koja kroz pružanje razumnog uvjerenja doprinosi povećanju kredibiliteta objavljenih finansijskih podataka.

Na osnovu svega navedenog može se zaključiti da kreativno računovodstvo, iako proističe iz fleksibilnosti računovodstvene regulative, može imati značajne negativne implikacije na procjenu investicionog rizika i (ne)stabilnost finansijskog sistema u cjelini. Stoga je kontinuirano unapređenje regulatornog okvira, jačanje profesionalne etike i povećanje transparentnosti finansijskog izvještavanja od ključnog značaja za očuvanje povjerenja u finansijske informacije, racionalno donošenje investicionih odluka i dugoročnu stabilnost i efikasnost finansijskog sistema.

LITERATURA

[1] I. A. Abed, N. Hussin, M. A. Ali, H. Haddad, M. Shehadeh, and E. F. Hasan, "Creative Accounting Determinants and Financial Reporting Quality: Systematic Literature Review," *Risks*, vol. 10, no. 4, p. 76, Apr. 2022, doi: 10.3390/risks10040076.

[2] I. Gudev, "Creative Accounting – Definition, Types, Purposes and Impact on United Nations' Sustainable Development Goals," *Economic Alternatives*, no. 2, pp. 328–341, Jun. 2020, doi: 10.37075/EA.2020.2.09.

[3] S. Fejzić and E. Halilčević, "Primjena kreativnog računovodstva u finansijskim prevarama," *9. mednarodna znanstvena študentska konferenca SKEI 2024: Trajnostni razvoj in umetna inteligenca*, pp. 122–129, Apr. 2024, Accessed: Mar. 1, 2026. [Online]. Available: https://unvi.edu.ba/Files/Skei_2024/SKEI_Zbornik.pdf

[4] S. Floştoiu, "Creative Accounting – Option or Necessity," *International conference KNOWLEDGE-BASED ORGANIZATION*, vol. 28, no. 2, pp. 21–25, Jun. 2022, doi: 10.2478/kbo-2022-0043.

[5] S. Đorđević and N. Mitić, "Alternative accounting procedures, creative accounting and false financial reporting," *Oditor*, vol. 6, no. 2, pp. 21–37, 2020, doi: 10.5937/Oditor2002021D.

[6] M. Budić, "MANIPULATION OF FINANCIAL REPORTS USING CREATIVE ACCOUNTING," *Revizor*, vol. 26, no. 104, pp. 85–95, Dec. 2023, doi: 10.56362/Rev23104085B.

[7] CZ. A. Kareem, "METHODS FOR DETECTING CREATIVE ACCOUNTING PRACTICES AND THEIR IMPACT ON INVESTMENT DECISIONS UNDER INTERNATIONAL FINANCIAL REPORTING STANDARDS (AN APPLIED STUDY IN A SAMPLE OF BANKS LISTED ON THE IRAQI STOCK EXCHANGE)," *World Economics and Finance Bulletin*, vol. 29, pp. 137–144, Dec. 2023, Accessed: Mar. 4, 2026. [Online]. Available: https://scholarexpress.net/index.php/wefb/article/view/3573

[8] A. Horaicu *et al.*, "Creative Accounting Practices and Their Perceived and Actual Impact on Financial Reporting: Evidence from Romanian Listed Companies," *International Journal of Financial Studies*, vol. 14, no. 2, p. 28, Feb. 2026, doi: 10.3390/ijfs14020028.

[9] F. H. Ahmed, "THE IMPACT OF APPLYING CREATIVE ACCOUNTING ON THE RELIABILITY OF ACCOUNTING INFORMATION IN THE FINANCIAL STATEMENTS," *World Economics and Finance Bulletin*, vol. 12, pp. 55–64, Jul. 2022, Accessed: Mar. 5, 2026. [Online]. Available: https://scholarexpress.net/index.php/wefb/article/view/1150

[10] A. Bouzidi, Z. Sadani, and M. Merkhoufi, "The Impact of Creative Accounting on the Quality of Financial Information in Financial Statements of Algerian Public Banks," *European Economic Letters (EEL)*, vol. 14, no. 4, pp. 948–963, Dec. 2024, Accessed: Mar. 7, 2026. [Online]. Available: https://eelet.org.uk/index.php/journal/article/view/2220

[11] A. Baisla, A. Kumar and A. Kumar, "Impact of creative accounting on investor confidence," *International Journal of Research Publication and Reviews*, vol. 6, no. 9, pp. 2432–2437, Sep. 2025, Accessed: Mar. 8, 2026. [Online]. Available: https://ijrpr.com/uploads/V6ISSUE9/IJRPR52782.pdf

[12] W. Zhang, "Ethical Dilemmas in Accounting: A Comprehensive Analysis of Professional Ethics," *Academic Journal Business & Management*, vol. 6, no. 2, 2024, doi: 10.25236/AJBM.2024.060220.

[13] A. Mailani, A. Septiani, A. E. Saputri, I. A. Setiawan, and Y. Bago, "Ethics in Accounting Practices Creative Accounting Practices and Their Impact on Financial Statement Transparency Enron Case Study Corporation," *International Journal of Asian Business and Development*, vol. 1, no. 2, pp. 95–102, Mar. 2025, doi: 10.55927/metropolis.v1i2.252.

[14] I. Daniel Kaaya, "Motives and Ethics of Creative Accounting: A Reflective Review and Views," *African Journal of Accounting and Social Science Studies*, vol. 4, no. 1, Nov. 2024, doi: 10.64717/ajass.v4i1.94.

UDK 007.52(497.6):[368.1:004.738.5
DOI 10.7251/ZRSNG2526047G

Sajber osiguranje i izazovi digitalnog doba

Danijela Glušac, Pravni fakultet, Univerzitet u Kragujevcu

***Sažetak* — Rad se bavi sajber osiguranjem kao savremenim instrumentom zaštite od posledica digitalnih pretnji u uslovima sve izraženije digitalizacije poslovanja i upravljanja podacima. Polazi se od činjenice da sajber rizike odlikuju visoka neizvesnost, nedostatak stabilnih empirijskih podataka, međusobna povezanost informacionih sistema i mogućnost nastanka velikog broja istovremenih šteta, što otežava njihovu procenu i ugovorno oblikovanje osiguravajućeg pokrića. U radu se analiziraju osnovne kategorije sajber rizika, razlika između pokrića za direktne štete i odgovornosti prema trećim licima, kao i specifičnosti sajber osiguranja u pogledu obima pokrića, ugovornih isključenja i značaja pravilne procene rizika. U radu se razmatra i stanje u Republici Srbiji, gde je ponuda ovog proizvoda još uvek ograničena, ali se istovremeno ukazuje da postojeći domaći pravni okvir omogućava da se sajber osiguranje posmatra kao vrsta imovinskog osiguranja, bez potrebe za njegovim posebnim zakonskim regulisanjem.**

***Ključne riječi* – sajber osiguranje, sajber rizik, imovinsko osiguranje, odgovornost prema trećim licima, procena rizika.**

Abstract – This paper examines cyber insurance as a modern instrument for protection against the consequences of digital threats in the context of the increasingly intensive digitalisation of business operations and data management. It proceeds from the premise that cyber risks are characterised by a high degree of uncertainty, a lack of stable empirical data, the interconnectedness of information systems, and the possibility of a large number of simultaneous losses, all of which make their assessment and the contractual design of insurance coverage more complex. The paper analyses the main categories of cyber risk, the distinction between first-party coverage and third-party liability coverage, as well as the specific features of cyber insurance with regard to the scope of coverage, policy exclusions, and the importance of proper risk assessment. The paper also considers the situation in the Republic of Serbia, where the availability of this insurance product remains limited, while at the same time indicating that the existing domestic legal framework allows cyber insurance to be treated as a form of property insurance, without the need for separate statutory regulation.

***Keywords* – cyber insurance, cyber risk, property insurance, third-party liability, risk assessment**

I. UVOD

Digitalizacija poslovanja, upravljanja podacima i komunikacije dovela je do toga da sajber rizici postanu jedno od ključnih pitanja savremene ekonomije i prava osiguranja. Sve veća zavisnost privrednih subjekata od informacionih sistema, cloud infrastrukture i digitalnih mreža povećava izloženost incidentima kao što su povreda podataka, prekid poslovanja, sajber iznuda i neovlašćen pristup sistemima, što istovremeno stvara potrebu za novim oblicima ugovorne i ekonomske zaštite. U literaturi se zato naglašava da je sajber-osiguranje nastalo kao odgovor na ograničenja tradicionalnih polisa, koje često nisu bile prilagođene štetama nastalim usled sajber incidenata, kao i da ono danas predstavlja važan element šireg sistema upravljanja digitalnim rizicima [1] , [2].

Posebnost sajber-osiguranja proizlazi iz same prirode sajber rizika. Za razliku od klasičnih osiguravajućih rizika, sajber rizike odlikuju visoka neizvesnost, nedostatak stabilnih i potpunih podataka, izražena međusobna povezanost sistema i mogućnost istovremenog nastanka velikog broja šteta, što otežava procenu rizika i održivo oblikovanje pokrića [1]. Organizacija za ekonomsku saradnju i razvoj (OECD) dodatno ukazuje da razvoj tržišta sajber-osiguranja zavisi od veće jasnoće obima pokrića, preciznijeg ugovornog jezika i boljeg razumevanja potreba osiguranika, budući da nejasne formulacije polisa povećavaju rizik sporova i slabe poverenje u ovaj proizvod [5]. Agencija Evropske unije za sajber bezbednost (ENISA) u tom smislu posebno naglašava da neujednačen jezik procene rizika i terminologije u sajber-osiguranju predstavlja jednu od prepreka njegovom daljem razvoju [3].

Polazeći od toga, predmet ovog rada jeste analiza sajber-osiguranja kao pravnog instrumenta zaštite od posledica digitalnih pretnji, sa posebnim osvrtom na njegove osnovne karakteristike i izazove u savremenim uslovima. Posebna pažnja biće posvećena specifičnostima sajber rizika, složenosti ugovornih klauzula, pitanju pokrića i isključenja, kao i značaju pravilne procene rizika i predugovornih informacija koje osiguranik dostavlja osiguravaču. U tom okviru, sajber-osiguranje se posmatra ne samo kao sredstvo naknade štete, već i kao deo šireg mehanizma upravljanja rizicima i jačanja otpornosti poslovanja u digitalnom dobu [4] , [2].

II. SAJBER RIZICI KAO NOVI IZAZOV SAVREMENOG DRUŠTVA

Iako je sajber rizik postao široko rasprostranjen termin, njegova definicija je i dalje predmet stalnog istraživanja i promena. U najširem smislu, sajber rizik se definiše kao rizik od obavljanja posla u sajber okruženju (*risk of doing business in the cyber environment)* [6]. Budući da je usko povezan sa primenom novih tehnologija, spada u grupu rizika na čije ostvarenje prevashodno utiče ljudski faktor.

U nastavku su predstavljeni najčešći sajber rizici, svrstani u različite kategorije.

1) Kategorija zaštite podataka i sajber odgovornosti

Ova kategorija namenjena je pokriću osiguranika, njegovih povezanih lica, zaposlenih i ostalih fizičkih lica koje osiguranik razumno smatra svojim zaposlenima. Ključni pokriveni rizici: tužbeni zahtevi trećih lica usled povrede poverljivih informacija (uključujući podatke o ličnosti) ili

bezbednosnog propusta kompjuterskog sistema osiguranika; tužbeni zahtevi trećih lica usled nepoštovanja merodavnih zakona o zaštiti podataka o ličnosti kao i drugih politika o zaštiti podataka o ličnosti i okolnosti koje mogu dati povoda podizanju tužbenih zahteva i istrazi organa javnih vlasti, kao i troškovi takvih postupaka takođe su pokriveni ako osiguranik odluči da izvesti osiguravača o istima [7].

2) Kategorija gubitka bezbednosti računarske mreže i podataka nakon unutrašnje greške-ovde dolazi do prekida poslovanja zbog tehničkog zastoja samog računarskog sistema kao nenemarnog sajber događaja, a nekad i zbog ljudskog promašaja [8]. Osiguranik može podneti zahtev za naknadu štete po osnovu pokrića iz ove kategorije sajber osiguranja najčešće samo u slučaju kada materijalni prekidi prelaze unapred određen broj sati (npr. prekid u trajanju većem od 12 sati) i u tom slučaju osiguranik ostvaruje pravo naknade iz osiguranja za celokupan period trajanja materijalnog prekida [7].

3) Kategorija upravljanja nastalim rizikom-jedna od obaveza kompanije koja se suoči sa sajber incidentom je i reagovanje na povredu privatnosti, odnosno obaveštavanje korisnika i upravljanje kriznom situacijom. No, te situacije ne prolaze bez daljih troškova angažovanja eksperata, bilo unutar ili van kompanije, kao i ulaganje u medijske objave i obaveštenja [9].

4) Kategorija sajber iznude-izmiruju se zahtevi za naknadu troškova proisteklih iz borbe protiv ucenjivačkog programa koji ograničava pristup računarskom sistemu ili pohranjenim podacima i traži otkupninu. Ključni pokriveni rizici: iznosi plaćeni radi sprečavanja i okončanja sajber iznude; troškovi angažovanja savetnika za rešavanje i otkrivanje uzroka sajber iznude; pretnje iznude, u zavisnosti od načina njihovog definisanja, koje pogađaju osiguranikove kompjuterske sisteme i koji mogu uzrokovati finansijsku i reputacionu štetu [8].

U zavisnosti od toga da li se sajber osiguranje pribavlja sa ciljem zaštite sopstvene imovine i podataka od sajber rizika ili sa ciljem pokrivanja sopstvene odgovornosti za propuste koji su kod trećih lica doveli do sajber rizika, razlikujemo osiguranje od sajber odgovornosti za direktne štete (engl. *First party cyber insurance*) i osiguranje od sajber odgovornosti prema trećim licima (engl. *Third party cyber insurance*) [7].

Osiguranje od sajber odgovornosti može se podeliti na dva osnovna vida. Prvi se odnosi na direktne štete, odnosno na gubitke koje trpi sam osiguranik usled sajber incidenta. Drugi se odnosi na odgovornost prema trećim licima, kada zbog sajber događaja štetu pretrpe druga lica, pa osiguranje pokriva obavezu osiguranika prema njima.

Osiguranje za direktne štete obuhvata situacije kao što su krađa ili otkrivanje poverljivih podataka, zlonamerno ili slučajno uništenje podataka, otkaz IT sistema, sajber iznuda, kao i napadi virusima i zlonamernim softverom. Njegova svrha je da nadoknadi gubitke koji neposredno pogađaju samog osiguranika nakon sajber napada. U tu grupu spadaju, na primer, troškovi digitalne forenzike, prekida poslovanja, obnove podataka, gubici nastali sajber kriminalom, izdaci povodom sajber iznude, troškovi odnosa s javnošću radi očuvanja reputacije, pravni troškovi, kao i troškovi obaveštavanja pogođenih lica, kol centra i kreditnog praćenja.

S druge strane, osiguranje od sajber odgovornosti prema trećim licima štiti osiguranika u slučajevima kada zbog povrede podataka ili bezbednosnog propusta štetu pretrpe druga lica. To je posebno značajno u poslovnim odnosima, jer u slučaju većih incidenata tužbom često budu obuhvaćene sve strane koje su na bilo koji način učestvovale u radu na kompromitovanom sistemu, uključujući i spoljne saradnike ili dobavljače. Ovo osiguranje, stoga, pokriva troškove sudske odbrane, iznose poravnanja, presude i druge odluke, kao i kazne i naknade koje mogu proisteći iz takvih sporova.

III. SPECIFIČNOST SAJBER OSIGURANJA

Sudska praksa pokazuje da su sporna pitanja sajber-osiguranja najčešće vezana za tumačenje isključenja, obim pokrića i prirodu nastale štete. U predmetu *Merck & Co., Inc. v. ACE American Insurance Co.* sud je zauzeo stav da klasično isključenje za „*hostile or warlike action*“ ne isključuje automatski pokriće za štetu nastalu usled *NotPetya* sajber-napada, jer polisa nije dovoljno jasno predviđala primenu takvog isključenja na napad usmeren protiv civilnog privrednog subjekta [10]. Nasuprot tome, u predmetu *National Ink & Stitch, LLC v. State Auto Property & Casualty Insurance Co.* sud je prihvatio da *ransomware* napad može dovesti do „direktnog fizičkog gubitka ili oštećenja“ računarskog sistema, što je bilo od značaja za priznavanje pokrića po imovinskoj polisi subjekta [11]. Posebno je značajan i predmet *Travelers Indemnity Co. of America v. Portal Healthcare Solutions, LLC*, u kome je utvrđeno da osiguravač ima obavezu da snosi troškove pravne odbrane osiguranika, jer je objavljivanje osetljivih medicinskih podataka na internetu potencijalno spadalo u pokriveni rizik po polisi odgovornosti subjekta [12]. Ovi sporovi pokazuju da je u sajber-osiguranju ishod često uslovljen preciznošću ugovornog jezika, a ne samo prirodom samog incidenta. Upravo zato sudska praksa sve jasnije potvrđuje da su jasno formulisana isključenja, definicije i uslovi za aktiviranje osiguravajućeg pokrića od presudnog značaja za pravnu sigurnost strana u ugovoru.

U Republici Srbiji relativno mali broj osiguravača uopšte nudi ovaj proizvod osiguranja. Tradicionalne vrste osiguranja imovine ne pokrivaju ove vrste rizika, iako je moguće da se i po takvim polisama osiguranja pruža pokriće prilično ograničenog obima [13]. Sajber osiguranje je jedna od mogućnosti koje stoje na raspolaganju u cilju izgradnje bezbednosti i zaštite od ovakvih pretnji, te sposobnosti brzog oporavka ako se ona ipak dogode.

Uprkos specifičnostima sajber rizika, postojeće odredbe srpskog ugovornog prava osiguranja i dalje mogu primenjivati na sajber osiguranje. Posebno ukazuje na to da se u našem pravu pokazala korisnom opšta podela na osiguranje lica i osiguranje imovine iz Zakona o obligacionim odnosima iz 1978. godine, jer omogućava svrstavanje sajber osiguranja u već postojeći sistem. U literaturi se navodi da pristup srpskog

prava omogućava da se sajber osiguranje posmatra kao vrsta imovinskog osiguranja, pa zato nije potrebno posebno zakonski uređivati ugovor o sajber osiguranju. Drugim rečima, postojeći domaći pravni okvir je dovoljno širok da obuhvati i ovu novu vrstu rizika [14].

IV. ZAKLJUČAK

Sajber osiguranje predstavlja važan pravni i ekonomski instrument zaštite u uslovima intenzivne digitalizacije poslovanja, upravljanja podacima i komunikacije. Razvoj informacionih tehnologija, uz istovremeni porast učestalosti i složenosti sajber incidenata, pokazao je da tradicionalni modeli osiguranja često nisu dovoljni za adekvatno pokriće šteta koje nastaju u digitalnom okruženju. Zbog toga se sajber osiguranje sve jasnije izdvaja kao poseban odgovor tržišta osiguranja na savremene oblike rizika.

Analiza je pokazala da posebnost sajber osiguranja proizlazi pre svega iz prirode sajber rizika, koje odlikuju visoka neizvesnost, dinamičnost, međusobna povezanost sistema i mogućnost nastanka velikog broja istovremenih šteta. Upravo te karakteristike otežavaju procenu rizika, određivanje premije, kao i precizno ugovorno definisanje pokrića i isključenja. Istovremeno, praksa potvrđuje da su jasne ugovorne klauzule, precizan jezik polise i pravilna procena rizika od presudnog značaja za pravnu sigurnost ugovornih strana i efikasno ostvarivanje osiguravajuće zaštite.

Poseban značaj ima razlikovanje između pokrića za direktne štete i pokrića odgovornosti prema trećim licima. Dok prvo pruža zaštitu samom osiguraniku od posledica sajber incidenta, drugo obezbeđuje pokriće odgovornosti prema licima koja trpe štetu usled povrede podataka ili bezbednosnih propusta. Time sajber osiguranje potvrđuje svoju dvostruku funkciju: ono nije samo sredstvo naknade štete, već i mehanizam šireg upravljanja rizicima, očuvanja kontinuiteta poslovanja i zaštite reputacije privrednih subjekata.

Kada je reč o Republici Srbiji, može se zaključiti da je tržište sajber osiguranja još uvek nedovoljno razvijeno, budući da relativno mali broj osiguravača nudi ovu vrstu proizvoda. Ipak, uprkos ograničenoj ponudi i nedovoljnoj zastupljenosti u domaćoj praksi, postojeći pravni okvir omogućava da se sajber osiguranje sagleda kao vrsta imovinskog osiguranja, bez potrebe za njegovim posebnim zakonskim regulisanjem. To ukazuje da je dalji razvoj ove oblasti pre svega uslovljen razvojem tržišta, unapređenjem ugovornih uslova i jačanjem svesti o značaju zaštite od digitalnih pretnji.

Na osnovu svega navedenog, može se zaključiti da će značaj sajber osiguranja u budućnosti nesumnjivo rasti. Sa razvojem digitalne ekonomije raste i potreba za efikasnim, jasnim i pravno sigurnim modelima osiguravajuće zaštite. Upravo zato sajber osiguranje treba posmatrati kao neizostavan deo savremenog sistema upravljanja rizicima i kao oblast koja će u narednom periodu zahtevati dodatno teorijsko, zakonodavno i praktično usavršavanje.

LITERATURA

[1] C. Biener, M. Eling, J.H. Wirfs, "Insurability of cyber risk: An empirical analysis," The Geneva Papers on Risk and Insurance – Issues and Practice, vol. 40 (1), pp. 131-158, 2015.

[2] OECD (2017). Enhancing the role of insurance in cyber risk management. OECD Publishing. Preuzeto sa https://www.oecd.org/en/publications/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en.html

[3] ENISA. (2017). Commonality of risk assessment language in cyber insurance. European Union Agency for Cybersecurity. Preuzeto sa https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-3-2%201%20Recommendations%20on%20Cyber%20Insurance.pdf

[4] International Association of Insurance Supervisors (IAIS). (2020). Cyber risk underwriting: Identified challenges and supervisory considerations for sustainable market development. Preuzeto sa https://www.iais.org/uploads/2022/01/201229-Cyber-Risk-Underwriting_-Identified-Challenges-and-Supervisory-Considerations-for-Sustainable-Market-Development.pdf

[5] OECD. (2020). Encouraging clarity in cyber insurance coverage. OECD Publishing. Preuzeto sa https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/02/encouraging-clarity-in-cyber-insurance-coverage_c2dea16f/40beab07-en.pdf

[6] Cyber Resilience – The cyber risk challenge and the role of insurance, Cro Forum , 2014.

[7] S. Petrović, „Sajber osiguranje," Pravo i privreda, vol. 58 (1), str. 206-217, 2020.

[8] N. Žarković, G. Puzić, Sajber osiguranje kao vrsta neživotnih osiguranja, Novi Sad: Institut za energetiku, održivi razvoj i zaštitu životne sredine, 2020.

[9] VIB-posredovanje u osiguranju. Sajber osiguranje. Preuzeto sa https://vib.rs/sajber-osiguranje/

[10] Merck & Co., Inc., et al. vs. Ace American Insurance Company, et al., Docket Numbers: A-1879-21, A-1882-21, May 1, 2023. https://law.justia.com/cases/new-jersey/appellate-division-published/2023/a-1879-21.html

[11] National Ink And Stitch, LLC v. State Auto Insurance Companies, Docket Number: 1:2018cv02138, January 23, 2020. https://law.justia.com/cases/federal/district-courts/maryland/mddce/1:2018cv02138/427038/39/

[12] The Travelers Indemnity Company of America v. Portal Healthcare Solutions, LLC, Docket Number: 1:2013cv00917, August 7, 2014. https://law.justia.com/cases/federal/district-courts/virginia/vaedce/1:2013cv00917/297932/33/

[13] D. Glušac, „Osiguranje od sajber odgovornosti," Usluge i vladavina prava: zbornik referata sa Međunarodnog naučnog skupa održanog 28. maja 2021. godine, na Pravnom fakultetu u Kragujevcu, Kragujevac: Pravni fakultet, Institut za pravne i društvene nauke, 2021, str. 299-306.

[14] M. Glintić, „Sajber osiguranje kao nova vrsta osiguranja - postoji li potreba za novom klasifikacijom osiguranja," Zbornik radova „Međuanrodni pravni odnosi i pravda" Kopaoničke škole prirodnog prava - Slobodan Perović, Beograd: Kopaonička škola prirodnog prava – Slobodan Perović, 2023, str. 465-482.

UDK 338.486.1.02(497.6RS):005.334
DOI 10.7251/ZRSNG2526050L

Održivi modeli destinacijskog menadžmenta: Digitalna transformacija i gastronomsko nasleđe Semberije

Sustainable models of destination management: Digital transformation and gastronomic heritage of Semberija

Darija Lunić, Nikica Radović, Univerzitet Sinergija, Bijeljina, Republika Srpska, BiH

Sažetak – U radu se istražuje uloga digitalne transformacije u očuvanju i promociji lokalnog gastronomskog nasleđa, vodeći se principima Slow Food pokreta. Težište istraživanja je na afirmaciji gastronomskog turizma kao posebnog oblika održivog razvoja i alternative masovnom turizmu putem načela ekološke ekološke odgovornosti i očuvanja biodiverziteta. Primenom meto de analize sadržaja SlowFood projekata, mobilnih aplikacija i dr uštvenih mreža, ispitani su mehanizmi promocije lokalne gastro-nomije. Rezultati ukazuju na to da je digitalizacija ključna za održivost destinacije. Studija slučaja područja Semberije i grada Bijeljine pokazuje da, uprkos bogatoj ponudi, digitalna vidljivost resursa ostaje nedovoljno razvijena, te se predlaže projekat digitalizacije kao ključna smernica za budući turistički razvoj.

Ključne riječi – digitalna transformacija, gastronomsko nasleđe, Slow Food, održivi turizam, Bijeljina, Održivost destinacije

Abstract – The paper explores the role of digital transformation in the preservation and promotion of local gastronomic heritage, guided by the principles of the Slow Food movement. The focus of the research is on the affirmation of gastronomic tourism as a special form of sustainable development and an alternative to mass tourism through the principle of ecological ecological responsibility and preservation of biodiversity. By applying the method of content analysis of Slow Food projects, mobile applications and social networks, the mechanisms of promotion of local gastronomy were examined. The results indicate that digitization is key to the sustainability of the destination. The case study of the area of Semberija and the city of Bijeljina shows that, despite the rich offer, the digital visibility of resources remains underdeveloped, and a digitization project is proposed as a key guideline for future tourism development.

***Keywords* – digital transformation, gastronomic heritage, Slow Food, sustainable tourism, Bijeljina, sustainability of the destination**

I. UVOD

Održivost destinacije u savremenom turizmu više nije stvar izbora, već preduslov opstanka na globalnom tržištu. Ona podrazumeva uspostavljanje dugoročnog balansa između ekonomskog profita, zaštite životne sredine i očuvanja autentičnog načina života lokalne zajednice. U tom kontekstu, gastronomsko nasleđe se ne posmatra samo kao resurs, već kao ključni element otpornosti destinacije na negativne uticaje masovnog turizma. Gastronomski turizam se definiše kao poseta turista primarnim ili sekundarnim proizvođačima hrane, festivalima i ugostiteljskim objektima gde je hrana primarni motiv putovanja [1]. Implementacija održivih modela menadžmenta omogućava da se prirodni i kulturni kapital sačuva za buduće generacije, generišući prihode koji ostaju unutar lokalne ekonomije.

Lokalni identitet i autohtona kuhinja predstavljaju neraskidivu celinu. Konceptualizovana kroz autentične proizvode, lokalna hrana nije samo sredstvo prehrane, već primarni simbol kulture i mesta određene destinacije [2]. Tradicija i gastronomija su pojmovi koji nas upućuju na trajne vrednosti i kvalitet koji savremeni turisti sve više zahtevaju. Upravo na ovim idejama zasniva se filozofija Slow Food-a. Osnovna ideja pokreta Slow Food jeste da podstakne ljude da preuzmu veću kontrolu nad svojim načinom života i ishrane, kao i da hranu doživljavaju svim čulima, a ne samo kao nešto što se konzumira iz potrebe.

Pored same proizvodnje hrane, ovaj pokret se bavi i očuvanjem tradicionalnih recepata koji su se prenosili kroz generacije, ali ih istovremeno prilagođava savremenim uslovima života. Cilj je promovisanje ishrane koja je zdrava, zasnovana na lokalnim i autentičnim namirnicama, i duboko povezana sa tradicijom i kulturnim nasleđem.

Digitalni alati imaju sve značajniju ulogu u razvoju savremenog turizma, posebno u oblasti kulturnog turizma. Njihova primena omogućava turistima lakši pristup informacijama, interaktivnije iskustvo i bolje upoznavanje

kulturne baštine određene destinacije. Istovremeno, digitalne tehnologije doprinose održivom razvoju turizma kroz efikasnije upravljanje turističkim tokovima, promociju manje poznatih destinacija i smanjenje negativnih uticaja na životnu sredinu. Sagledavajući potrebe i interesovanja turista danas, digitalni alati predstavljaju važan faktor u razvoju održivog kulturnog turizma. Njihova uloga u budućnosti biće još značajnija, naročito sa promenama trendova i percepcija korisnika turističkih usluga. Ideja da se široko rasprostranjene tehnologije, omiljene među mladima, ali i starima, koriste u edukativne svrhe čini se spasonosnom za očuvanje civilizacijskih dobara, istorijskih činjenica, kao i lokalnog kulturno-umetničkog nasleđa i praksi [3].

Cilj ovog rada je da analizira mogućnosti primene održivih modela destinacijskog menadžmenta u Semberiji, sa posebnim fokusom na ulogu digitalne transformacije i valorizaciju gastronomskog nasleđa. Rad teži da da prikaz primera koji integriše ove elemente u cilju unapređenja konkurentnosti i održivog razvoja destinacije.

II. EKONOMSKI I SOCIJALNI POTENCIJAL GASTRONOMIJE

Gastronomsko nasleđe predstavlja značajan segment nematerijalne kulturne baštine i sve važniji motiv turističkih putovanja. Lokalna kuhinja odražava istoriju, tradiciju i način života jedne zajednice, čime doprinosi autentičnosti turističkog doživljaja. Gastronomija je evoluirala u jedan od najvažnijih faktora za razvoj društvenog i ekonomskog potencijala regije. U turističkoj ponudi sve se više pažnje poklanja promociji i potrošnji domaćih prehrambenih proizvoda [4].

Putem očuvanja i valorizacije autentičnih proizvoda, svaka oblast može postati značajna turistička destinacija. Kulinarsko iskustvo direktno oblikuje percepciju posetioca i utiče na nameru da turista planira da poseti destinacija. Atraktivnost destinacije u velikoj meri je određena kvalitetom regionalnih proizvoda, a hrana služi kao simbol nacionalnog identiteta. Prema istraživanjima Duarte-a (2013) [5], gastronomska iskustva pružaju razne mogućnosti:

- lokalni restorani omogućavaju autentično kušanje tipičnih jela koje mora biti čvršće ukorenjeno u ponudi destinacije;
- lokalne pijace koje su istorijski simboli kulture, a koje danas postaju "gastronomski pečati" za turiste u potrazi za kreacijom i iskustvom;
- istorijske lokacije kao spoj kulture, anegdota i tradicije vezane za lokalno jelo ili piće;
- poljoprivredna domaćinstva koja utiču na rastući trend poseta mestima primarne proizvodnje (agro-turizam).

Paralelno sa procesima digitalizacije, gastronomsko nasleđe se sve više afirmiše kao važan segment turističke ponude, naročito u ruralnim i nedovoljno razvijenim regionima. Tradicionalna hrana, lokalni recepti i običaji predstavljaju autentične resurse koji doprinose diferencijaciji destinacije na globalnom tržištu. Njihova valorizacija kroz turizam ne samo da doprinosi ekonomskom razvoju, već i očuvanju kulturnog identiteta i lokalne tradicije.

III. POJAM KONCEPTA "SLOW FOOD" I IMPLEMENTACIJA NA PROSTORU SEMBERIJE

Slow Food pokret nastao je kao odgovor na globalizaciju i širenje fast food trenda, sa ciljem očuvanja tradicije i "sporog tempa života" [6]. Osnovna ideja osnivača Karla Petrinija [7] počiva na tri stuba: hrana mora da bude dobra (ukusna i zdrava), čista (ekološki održiva) i socijalno pravedna za proizvođače i pristupačna za potrošače.

Ovaj pokret je usmeren na rešavanje brojnih izazova u savremenom prehrambenom sistemu, među kojima se posebno izdvajaju podrška lokalnim proizvođačima hrane i očuvanje autohtonih vrsta i tradicionalnih proizvoda. Na taj način, ovaj pokret nastoji da zaštiti male poljoprivrednike i proizvođače od pritisaka industrijske proizvodnje, istovremeno čuvajući raznovrsnost i autentičnost lokalne gastronomije. Međutim, njegov pristup prevazilazi samu pripremu i konzumaciju hrane. U središtu koncepta nalazi se edukacija potrošača, koja podrazumeva razvijanje svesti o poreklu hrane i načinima njene proizvodnje. Potrošači se podstiču da postavljaju pitanja o tome odakle hrana dolazi, da li je uzgajana na održiv način, u kojoj meri su korišćeni pesticidi i kakav je njen uticaj na zdravlje i životnu sredinu. Filozofija Slow Food-a promoviše odgovorniji odnos prema ishrani, ali i šire, prema prirodnim resursima, lokalnoj ekonomiji i nematerjalnom kulturnom nasleđu. Ovakav pristup doprinosi stvaranju održivog sistema proizvodnje i potrošnje hrane, u kojem se vrednuju kvalitet, transparentnost i etički principi.

Udruženje Slow Food danas deluje u više od 160 država kroz kroz nekoliko projekata. *Riznica ukusa (Arca del Gusto)* je projekat koji objedinjuje proizvode kojima preti nestanak usled poljoprivredne industrijalizacije i klimatskih promena. Do danas je registrovano preko 1.000 proizvoda, uključujući i one iz Srbije i BiH [8]. *Mercati della Terra (Pijace zemlje)* Međunarodna mreža pijaca koja omogućava direktan susret proizvođača i potrošača, promovišući sezonske namirnice i održive tehnike uzgoja, sa fokusom na autentične, lokalne, sezonske i održivo proizvedene namirnice.

Slow Food turizam je jedan od najmlađih oblika turizma koji kao motiv putovanja podrazumeva susrete sa poljoprivrednim proizvođačima, pastirima i vinarima, gde svaki učesnik postaje povezan za svoju teritoriju. U cilju upoznavanja turista, ali i širenja i negovanja ove ideje značajnu ulogu imaju aktivnosti edukacije. Edukacija obuhvata rad i sa turistima, ali i sa lokalnim stanovništvom. Cilj je da lokalno stanovništvo prepozna sve benefite ovog oblika turizma sa aspekta održivog razvoja destinacije, zbog ekonomskog, ekološkog i socio-kulturnog doprinosa.

Koncept pokreta Slow Food ističe ključnu ulogu očuvanja lokalne gastronomske tradicije, promocije održive proizvodnje i kreiranja autentičnih turističkih iskustava. Upravo zbog toga, ovaj pristup je izuzetno značajan za razvoj održivih modela destinacijskog menadžmenta, posebno u ruralnim regionima poput Semberije, gde turizam može biti snažan pokretač ekonomskog i kulturnog razvoja.

Svaka regija u svetu, pa tako i prostor Semberijske regije izdvaja se po autentičnim prehrambenim proizvodima koji zaslužuju da budu evidentirani i predstavljeni i šire. Naime, *„Riznica ukusa“* (*Arca del Gusto*) označava kolekciju i očuvanje autohtonih, tradicionalnih i često zaboravljenih namirnica i recepata koji su deo kulturnog i gastronomskog nasleđa određene regije. Namirnice u *„Riznici ukusa“* su karakteristične po svom prirodnom ukusu, koji često izostaje kod masovno proizvedene hrane. Projekat *„Riznice ukusa“* uključuje stare sorte voća i povrća, autohtone vrste žitarica, sireva, mesa i drugih proizvoda koje su karakteristične za određenu lokalnu zajednicu. Zadatak *„Riznice ukusa“* je da direktno podržava gastronomski turizam i Slow food turizam**,** jer turisti mogu probati autentične lokalne proizvode i na originalan način uživati u njima i boravku na destinaciji.

Semberija, poznata po bogatstvu prirodnih i kulturnih resursa, ima veliki potencijal za razvoj turizma zasnovanog na gastronomiji. Region obiluje tradicionalnim jelima i lokalnim proizvodima koji odražavaju autentičnost i kulturni identitet zajednice. Ovaj prostor je poznat po brojnim prehrambenim proizvodima koji su autentični i prepoznatljivi za Semberiju (Tabela 1), a koji bi atraktivni za projekta “*Riznice ukusa*”.

Tabela 1. Potencijalni proizvodi Semberije za upis u “*Riznicu ukusa*”

Naziv proizvoda	**Kategorija**	**Značaj za nasleđe**	**Predloženi digitalni alat**
Semberski kupus	Povrće	Autohtona sorta, ključ na za lokalni identitet i tradiciju.	QR kod sa "storytelli ng" pričom o gazdinstvu. Blockchain tehnologija
Semberka (rakija)	Destilat	Tradicionalna receptur a od starih sorti šljiva (npr. Požegača).	Interaktivna mapa puteva pića na web p ortalu.
Majevički sir Zarac	Mlečni proizvod	Receptura koja se prenosi generacijama, bez aditiva	Video marketing (proces proizvodnje) na mrežama
Meso mangulice	Mesni proizvod	Receptura koja se prenosi generacijama, bez aditiva	Video marketing (proces proizvodnje) na mrežama
Ulje od bundeve	Ulje	Tradicionalno pripremanje autentičnog ulja	QR kod sa "storytelli ng" pričom o gazdinstvu. Blockchain tehnologija

Izvor: Autori samostalno

Ipak, da bi se taj potencijal u potpunosti iskoristio, neophodno je uvesti savremene modele upravljanja destinacijom i intenzivnije koristiti digitalne tehnologije. Trenutno, iako gastronomska ponuda Semberije ima izuzetnu vrednost, njen digitalni prikaz i dostupnost turistima su ograničeni, što smanjuje vidljivost i mogućnosti za razvoj.

U ruralnim regionima poput Semberije, koncept *Mercati della Terra* utiče na razvoj ovakvih tržišta i može imati višestruke koristi. Razvoj ovog koncepta u okviru Slow Food-a omogućava direktnu prodaju lokalnih proizvoda, povećava vidljivost tradicionalnih jela i autohtonih namirnica, podržava lokalnu ekonomiju i doprinosi stvaranju autentičnog turističkog iskustva. Primena digitalnih alata za promociju i organizaciju ovih tržišta dodatno povećava njihov efekat, omogućavajući turistima lakši pristup informacijama i planiranje poseta, dok lokalnoj zajednici donosi nove mogućnosti razvoja i očuvanja kulturnog nasleđa.

IV. DIGIITALNA TRANSFORMACIJA I SLOW FOOD

Istraživanja pokazuju da bi primena digitalnih platformi u okviru Slow Food koncepta omogućila značajno unapređenje turističke ponude. Digitalne mape gastronomskih ruta, online promocija lokalnih proizvoda i virtuelne ture mogle bi direktno doprineti povećanju turističkog prometa, podršci lokalnim proizvođačima i očuvanju autohtonog nasleđa. Na taj način, Semberija bi mogla da postane prepoznatljiva destinacija koja kombinuje tradicionalnu gastronomiju, održivost i moderne tehnologije, stvarajući dugoročne koristi za ekonomiju, lokalnu zajednicu i kulturni identitet regiona.

Digitalizacija doprinosi i očuvanju tradicionalnih kuhinja, kao i prenošenju autentičnih veština i znanja. Naime, bilo bi atraktivno formirati online kurseve i platforme za učenje o gastronomiji Semberije, a na društvenim mrežama na blogovima i podkastima promovisati slow food filozofiju i autentične proizvode Semberijske regije.

Integracija digitalnih platformi u organizaciju i promociju *Mercati della Terra* dodatno povećava njihov efekat. Turisti mogu planirati posete, dobiti informacije o ponudama i proizvođačima, a lokalna zajednica dobija mogućnost šire promocije svojih proizvoda i usluga. Na taj način, razvoj ovakvih tržišta u Semberiji ne samo da bi doprineo ekonomskom razvoju, već i očuvanju kulturnog i gastronomskog identiteta regiona, čineći ga konkurentnijim na tržištu održivog turizma.

Prateći potrebe savremenih turista implementacija digitalnih rešenja u formi QR code menija, jelovnika, karti pića, informacija o sastavu i poreklu namirnica, vizuelizacija gotovih jela. Kao segment digitalizacije u održivom poslovanju značajna je implementacija blockchain tehnologije koja po principu „od njive do trpeze“ prati namirnice i utiče na osećaj sigurnosti i bezbednosti konzumenta, gosta restorana.

Primeri primene blockchaina su uspešne vinarije u Italiji[1], Australiji[2], kao protagonsti Slow Food namirnica koji u cilju sticanja poverenja od strane svojih korisnika usluga implementiraju ovu vrstu tehnologije koja garantuje bezbednost informacija. S tim u vezi, bila bi interesantna implementacija blockchain tehnologije u poslovanju lokalnih proizvođača autentičnih proizvoda iz Semberijske regije u okviru koje bi konzument mogao da isprati sve adekvatne informacije o namirnicama za koje su zainteresovani. Bila bi interesantna implementacija na primeru porodičnog gazdinstva koje proizvodi i prerađuje kupus. Implementacijom blockchain tehnologije mogla bi da se isprati namirnica, kupus, od sadnje, nege u toku odgajanja, berbe, veličine i klasifikacije plodova, kao i daljih koraka u proizvodnji. U okviru blockchain lanca jednom unete informacije se ne mogu menjati tako da bi sve aktuelno evidentirane o uzgoju i berbi kupusa u jednoj godini, kao i daljim koracima pripremanja istog bile dostupne konzumentu nepromenjene putem QR coda. Na taj način Slow Food filozofija poprima inovaciju, u cilju unapređenja usluga, sadržaja za goste, kao i zadovoljenja njihovih potreba. Slow Food turista bi imao potpunu informaciju „od njive do trpeze“ koja bi mu garantovala bezbednu konzumaciju tradicionalnog jela od kupusa jer bi bio upoznat sa celokupnim lancem od sadnje, uzgoja, proizvodnje, pripremanja jela i sl.

Turisti danas postaju svesniji vrednosti autentičnosti i kvaliteta tokom putovanja. Proizvođačima koji prate trendove i potrebe na turističkom tržištu nude se mogućnosti za napredak u okviru ruralnih područja, što istovremeno stvara novi horizont za razvoj održivog ruralnog turizma usmerenog na otkrivanje tradicionalne kuhinje i ruralnih zajednica kroz koncept implementacije Slow Food filozofije [9].

Održivost destinacije Bijeljina direktno zavisi od sposobnosti lokalnih aktera da integrišu tradicionalna znanja sa inovativnm digitalnim alatima. Digitalna transformacija je za analiziranu regiju značajna kao katalizator održivosti, jer omogućava preciznije upravljanje resursima, smanjenje otpada u lancima snabdevanja, kao i direktnu edukaciju turista o značaju očuvanja biodiverziteta. Kreiranje platform i aplikacija koje se u svetu koriste u cilju ekološki održivog poslovanja. Naime, pojedine platforme[3] pomažu kompanijama da smanje troškove odlaganja otpada, dopru do ekološki osveštenih kupaca i kolektivno spreče bacanje miliona tona hrane na godišnjem nivou. U cilju održivog razvoja turizma implementacija ovakvih rešenja je veoma značajna.

V. ZAKLJUČAK

Uključivanje Bijeljine, kao grada u regiji Semberije, u Slow Food mrežu uz adekvatnu digitalnu podršku donosi višestruke benefite kroz ekonomsko osnaživanje i direktnu prodaju putem digitalnih kanala, a *Mercati della Terra* utiče na rast prihoda malih nezavisnih poljoprivrednih proizvođača.

Globalna vidljivost je prisutna putem integracije na *Slow Food World Map* što Semberiju čini vidljivom za strane turiste koji su u potrazi za autentičnošću.

Zaštita biodiverziteta je prisutna kroz aktivnosti digitalne evidencije, praćenja i promocije autohtonih sorti jedne destinacije. Ovaj način brige o očuvanju autentičnih vrednosti za jednu destinaciju motiviše mlade da ostanu na selu i nastave tradiciju.

Održivost destinacije Bijeljina direktno zavisi od sposobnosti lokalnih aktera da integrišu tradicionalna znanja sa inovativni m digitalnim alatima. Digitalna transformacija ovde služi kao katalizator održivosti, jer omogućava preciznije upravljanje re-sursima, smanjenje otpada u lancima snabdevanja i direktnu edukaciju turista o značaju očuvanja biodiverziteta.

Usvajanjem Slow Food postulate, destinacijski menadžment prestaje da bude puko oglašavanje i postaje process strateškog očuvanja identiteta. Krajnji cilj nije samo veći broj posetilaca, već stvaranje “pametne” i odgovorne destinacije koja nudi vrhunski kvalitet života lokalnom stanovništvu, ali i nezaboravno, etički ispravno iskustvo svojim gostima. Realizacija projekta digitalizacije gastronomske ponude Semberije i grada Bijeljine predstavlja ključnu smernicu za buduća istraživanja i turistički razvoj regije, kao održive i prepoznatljive destinacije na turističkom tržištu.

[1] https://www.ezlab.it/en/sectors/wine-and-beverage/

[2] https://blockbar.com/how-it-works?srsltid=AfmBOooIve00ATxxAZHHsQ8fmVHkuTzcpUkomBg-k-_c5eJislexankF

[3] https://www.toogoodtogo.com/en-us

LITERATURA

[1] Vujko, A. , Cvijanović D. & Berjan S. (2024). *Gastronomija kao indikator održivog razvoja ruralnog turizma*, Fakultet za turizam i hotelijerstvo u Vrnjačkoj banji, Univerzitet u Kragujevcu.

[2] Frew, E., & White, L. (2011). *Tourism and National Identities: An International Perspective*. London: Routledge

[3] Čigoja D,. & Radović N. (2014). Uloga digitalnog marketinga u očuvanju kulturno-istorijske baštine Srbije, Međunarodni naučni skup SINTEZA 2014, Univerzitet Singidunum, Beograd https://portal.sinteza.singidunum.ac.rs/Media/files/2014/292-294.pdf

[4] Radović N.&Vujko A. (2025). *Kulturna baština i turizam*, Univerzitet Singidunum, Beograd

[5] Duarte, P., O'Neill, M., Liu, Y., & O'Shea, M. (2013). Factors driving consumer restaurant choice: An exploratory study from the Southeastern United States, *Journal of Hospitality Marketing & Management* 22 (5), 547-567 https://doi.org/10.1080/19368623.2012.671562

[6] Corvo, P. (2015). *Food Culture, Consumption and Society*. Palgrave Macmillan.

[7] Petrini, C. (2007). *Slow Food Nation: Why Our Food Should Be Good, Clean, and Fair*. New York : Rizzoli Ex Libris

[8] Fondazione Slow Food per la Biodiversità Onlus (2024). *Arca del Gusto & Mercati della Terra*. Preuzeto sa: fondazioneslowfood.com.

[9] Lunić D., Surla T., Pivac T., Micera R. (2024). TENETS OF THE SLOW FOOD MOVEMENT AS MOTIVATION FOR TOURISTS TO VISIT RURAL TOURIST HOUSEHOLDS IN SERBIA, TEME Vol. XLVIII, No 1 https://doi.org/10.22190/TEME230619011L

UDK 330.322:[336.77/.78:005.334
DOI 10.7251/ZRSNG2526054C

A Comparative Analysis of Static Feature Extraction Techniques for PE File Malware Detection using LightGBM and Gradient Boosting Variants

Aleksandar Sandro Cvetković [1*], Snježana Stanišić [2], Saša Adamović [1]
[1] Faculty of Computing and Informatics, Sinergija University, Bijeljina, Bosnia and Herzegovina
[2] Faculty of Business Economics, Sinergija University, Bijeljina, Bosnia and Herzegovina
[*]ascvetkovic@sinergija.edu.ba

Abstract **–** Efficiency of traditional signature-based detection has been severely diminished due to the exponential growth of sophisticated malware. For this reason, the cybersecurity industry has pivoted toward Machine Learning (ML) solutions. This paper presents a comprehensive comparative analysis of machine learning models for static malware detection using Windows Portable Executable (PE) files. By evaluating the efficiency of feature extraction methodologies, specifically targeting structural metadata, byte histograms, and import tables, we demonstrate the limitations of deep learning architectures, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), which often suffer from high computational overhead and the curse of dimensionality. In contrast, Gradient Boosted Decision Trees (GBDTs) such as XGBoost, CatBoost, and LightGBM establish a definitive performance upper bound for tabular PE metadata. Our findings emphasize that, when combined with optimized feature engineering, LightGBM achieves a superior speed-to-accuracy ratio, making it an ideal candidate for real-time, resource-constrained endpoint deployment.

Keywords – PE Malware, Static Analysis, Feature Extraction, LightGBM, Python, Gradient Boosting, EMBER 2024.

Introduction

The exponential spread of malware has rendered manual reverse engineering and traditional signature-based detection obsolete [1]. As attackers rapidly automate the generation of polymorphic and packed malware, the 'breakout time' for attackers has significantly decreased, making human-driven analysis impossible and leading the cybersecurity community to strive toward automated, predictive solutions. In order to counter these accelerated threat lifecycles, the industry is increasingly turning to Machine Learning (ML) models trained on static analysis data [2].

By extracting structural metadata (such as headers, section properties, Import Address Tables (IAT), and byte-level entropy) from Windows Portable Executable (PE) files prior to execution, static ML models provide a critical, zero-day capable first line of defense. This approach bypasses the high computational costs and runtime risks typically associated with dynamic execution in sandbox environments, [3].

While deep learning architectures such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been thoroughly researched for this task, they often behave as 'black boxes' and struggle with the curse of dimensionality. Furthermore, these models impose high computational demands and latency constraints that are largely impractical for real-time endpoint security [3], [4]. Recent literature points to a distinct gap in feature engineering, when structural PE features are engineered and compressed efficiently, tree-based models offer a demonstrably superior speed-to-accuracy ratio for tabular PE files [1].

Accordingly, research has shifted toward Gradient Boosted Decision Trees (GBDTs), specifically LightGBM, XGBoost, and CatBoost as the state-of-the-art for tabular malware data [1]. This study evaluates feature extraction efficiency, focusing primarily on Python libraries (such as pefile) to avoid version-induced feature drift, and systematically benchmarks LightGBM against its GBDT counterparts to establish optimal deployment strategies for resource-constrained environments.

I. Literature Review

For static malware analysis, simple string matching just doesn't cut it anymore. Instead, researchers have moved toward extracting complex, multidimensional structural features. Standardized benchmarks like the EMBER dataset changed the game by introducing a 2,381-dimensional vector. This vector covers general file info, Common Object File Format (COFF) optional headers, and section entropy [5].

Table 1. Summary of existing literature on PE malware detection

Specific Static Features Extracted	Machine Learning Model Used	Performance Results	Sources
PE Header, COFF headers, import/export tables, section properties, section entropy	LightGBM, XGBoost, CatBoost, Random Forest, Extra Trees, MLP	LightGBM: 0.9852 AUC, 0.9421 F1-Score	[1]

API call frequency, Windows-based APIs, file system interactions, registry manipulation	Random Forest, XGBoost, Logistic Regression, SVM, NB, KNN	Random Forest: 96% Accuracy, 0.96 F1-Score, 0.99 Precision	[2]
47 diagnostic features: static properties, process/file/registry activity, network telemetry	CatBoost, LightGBM, XGBoost, Random Forest, TabNet, FT-Transformer	CatBoost: 99.0% Accuracy; LightGBM: 98.7% Accuracy	[3]
EMBER feature set (format-agnostic byte/entropy histograms, string info, parsed headers)	MalConv (CNN), LightGBM (via GBDT-EMBER baseline)	GBDT: 0.75 TPR @ 0.0028 FPR	[4]
2,381 EMBER features: Byte distribution, entropy, headers, imports (excluding timestamps)	Residual Neural Network (ResNet), LightGBM (Baseline)	Improved ResNet: 92.58% Accuracy, 0.9175 F1-Score	[5]
965 features: Opcodes (93), Registers (26), Windows API (794), Section attributes, File size	GIN (Graph Isomorphism Network), MLP, SVM, ResNet-50	GIN (Adv): 99.5% Accuracy; MLP: 97.9% Accuracy	[6]
Fuzzy-import hashing, permissions, opcodes, API calls, grayscale image matrices	CNN, RNN, LSTM, DNN, Transformers	Various; Fischer et al.: 99.2% ROC-AUC	[7]
Binary code, assembly instructions (.text), source code (decompiled), API call traces	LightGBM (Baseline), CodeBERT, GPT-2, stacked BiLSTM	LightGBM: Highly competitive baseline	[8]
EMBER metadata (COFF headers, data directories, imports unrolled into flat arrays)	XGBoost, Deep Learning (Binary/Multi-class), Autoencoders	XGBoost: 97.76% Accuracy, 0.9776 F1-Score	[9]
Linear/Logical opcode sequences, weighted undirected graphs, PageRank, node degree	LightGBM, XGBoost, CatBoost, Graph Neural Networks (OSGNN)	Consensus Voting: 98.29% Accuracy, 0.9746 MDR	[10]
AST-JS nodes, node combinations, lexical/host-based features, Doc2Vec	LightGBM, XGBoost, RandomForest, FastText, LSTM	XGBoost: 0.9989 Recall, 0.9909 F1-Score	[11]
470 dynamically observed behaviors (API frequencies), static sensitive APIs, permissions	LightGBM, XGBoost, Random Forest	LightGBM: 93.95% Accuracy, 94.1% Precision	[12]
79 PE metadata features: ImageBase, Subsystem, CheckSum, MajorSubsystemVersion	Random Forest, Decision Tree, XGBoost, MLP, Conv1D, LSTM	Random Forest: 95.95% Accuracy; XGBoost: 95.69% Accuracy	[13]
"Radian" features (statistical dispersion), traffic patterns, flow-based features	TabLoRA (TabNet + LoRA), Random Forest, Decision Tree, KNN	TabLoRA: 99.97% Accuracy, 99.98 F1-Score	[14]
2,381 raw static features, byte histograms (hex values like 0x7D, 0x44), string entropy	LightGBM (Target), MalConv, GAMMA (Evolutionary black-box)	Adversarial evasion: >70% success against GBDTs	[15]
EMBER 2024 histogram-based static features (float32 compression)	Stacking ensemble: LightGBM, CatBoost, XGBoost (meta-learner: LightGBM)	Ensemble: 86.99% Accuracy, 0.87 F1-Score, 0.9473 AUC	[16]
PE Optional Header Fields (PEOHF), 1323 features (Balanced) / 1877 (Unbalanced)	SMO (SVM), J48 (Decision Tree), Simple Logistic, Random Forest	DFS/MI + SMO: 98.677% Accuracy (BD), 99.308% (UBD)	[17]
Semantically extracted raw bytes: Header, Code, Data, and integrated File	CNN (MalConv-based architecture for multi-classification)	Header-only: 99.54% Accuracy; File: 98.06% Accuracy	[18]
EMBER feature vector (2,381 features), SHA digest metadata, descubrimiento timestamp	LightGBM (calibrated via Isotonic Regression)	Calibrated LightGBM: 0.99712 F1-Score	[19]
Ordering concatenation: PE header, opcode sequence, and API import features	Stacking ensemble: SVM + Random Forest (meta-learner: Logistic Regression)	Hybrid Ensemble: 98.91% Accuracy, 98.91% F1-Score	[20]
Static Joint analysis of API calls and Dynamic Link Library (DLL) data	XGBoost, CNN-GRU-3, Random Forest, KNN, Extra Trees Classifier	XGBoost: 99.81% Accuracy; CNN-GRU-3: 99.37% Accuracy	[21]

Feature Extraction Challenges

Since malware authors are constantly switching up their code to tank model accuracy over time, concept drift remains a massive headache [5]. Static analysis is also wide open to problem space attacks. These tricks involve adding padding bytes or messing with non-critical header regions (like the DOS header) just to flip the classification results [15], [4]. Reproducibility is another issue. Version gaps in LIEF libraries often cause feature drift, so it's usually better to stick with clean Python alternatives like pefile [16].

The Transition to Gradient Boosting

Early approaches leaned heavily on the Random Forest algorithm, hitting accuracy levels up to 95.95% using limited PE metadata [13]. But as datasets ballooned into the millions, the focus shifted toward Gradient Boosted Decision Trees (GBDT) type models. A prime example of this scale is the EMBER 2024 dataset. While XGBoost has proven to have a high recall for analyzing opcode sequences [10], LightGBM has emerged as the state-of-the-art choice for tabular static data. It's simply more efficient, using significantly less memory and offering faster training times [8]. Comparative benchmarks show LightGBM hitting an AUC-ROC of 0.9852, outperforming both Random Forest and Extra Trees when it comes to inference speed [1].

Deep Learning and Hybrid Methodologies

The researchers in [7] conducted a deep dive into using deep learning for malware detection. They explored how models like CNNs, LSTMs, and Transformers handle features like fuzzy-import hashing, permissions, and opcodes. Their results show that specific architectures hit an impressive 99.2% AUC-ROC across various environments. Building on the use of neural networks, the authors of [18] introduced a semantic classification approach using a MalConv-based CNN. By pulling raw bytes strictly from specific semantic locations (like header, code, and data sections) they proved that analyzing the header alone can reach an accuracy of 99.54%.

Unified Feature Evaluation and Hashing

Addressing the need to for standardized feature assessment, the study in [9] presents a unified evaluation of learning-based similarity techniques. Authors did this by parsing EMBER metadata (specifically COFF headers and data directories) into flattened arrays. The research confirms that XGBoost is highly effective for this task, hitting an accuracy of 97.76% and an equivalent F1-Score.

Network, Web-based, and IoT Attack Detection

Beyond traditional PE binaries, machine learning is also making waves in the broader landscape of cyber defense. As shown in [14], a framework called TabLoRA, which pairs TabNet with Low-Rank Adaptation (LoRA) was used to analyze "Radian" features. These features focus on statistical dispersion and traffic patterns, and the combination hit a near-perfect accuracy of 99.97% in detecting network anomalies. In a similar vein, the research in [11] proved how effective XGBoost can be for spotting web-based attacks. By looking at AST-JS nodes and Doc2Vec features, that study recorded a 0.9989 recall and a 0.9909 F1-Score. More recently, a 2026 study [3] focused on Industry 6.0 by evaluating 47 different static and network telemetry features for IoT malware detection. The findings revealed that CatBoost and LightGBM are still the ones to beat, outperforming other models with accuracies of 99.0% and 98.7%, respectively.

Ensemble and Calibrated Approaches

To combat concept drift, recent studies highlight the superiority of complex, calibrated ensembles and the improvement of classification margins. The authors of [19] utilized Isotonic Regression to calibrate a LightGBM model using EMBER and SHA digest metadata, achieving an F1-score of 0.99712 in their fight against data drift. In a parallel advancement, a 2025 study [20] proposed a hybrid Support Vector Machine - Random Forest (SVM-RF) stacking ensemble that fused PE headers, opcode sequences, and API imports. Supervised by a Logistic Regression meta-learner, this hybrid approach reached an impressive 98.91% accuracy and F1-score.

II. METHODOLOGY AND FEATURE EXTRACTION

Data Collection

The primary data source for this research is the EMBER 2024 dataset. While the original EMBER release focused on 1.1 million files, the 2024 update has expanded significantly, now featuring over 3.2 million samples across six different file formats [5], [16]. To ensure the study covers a diverse range of current threats, additional samples were pulled from MalwareBazaar and VirusShare, focusing on recent families like Ransomware, Trojans, and Botnets [2]. These datasets provide the high-confidence labels needed to build robust classifiers that can stand up to modern obfuscation techniques [9].

The Extraction Pipeline

The pipeline uses a pure Python implementation to keep things stable in research environments. While the LIEF library handles the heavy lifting for advanced binary instrumentation [16], the pefile library is the go-to tool for pulling structural metadata. This choice specifically avoids the version-heavy "feature drift" that usually plagues C++ based parsers [16]. Raw files are then crunched into flattened numerical arrays, which keeps byte-level histograms and structural flags intact without the massive overhead of a full disassembly.

Feature Categories

The feature engineering process focuses on specific domains of the PE structure:

General File Info and Structural Metadata

This layer includes basic metrics like file size, global entropy, and digital signature status. High global entropy is a classic red flag, often pointing to packed or encrypted payloads designed to hide malicious code [15].

The extraction also deep-dives into the IMAGE_FILE_HEADER (tracking machine types and section counts) and the IMAGE_OPTIONAL_HEADER (capturing the AddressOfEntryPoint, ImageBase, and Subsystem). Key fields like CheckSum and MajorSubsystemVersion are prioritized because they have high "discriminative power", meaning they are very effective at helping the model tell a legitimate file from a fake one [13].

Content and Organization (Section Data and IAT)

This involves digging into the internal sections of the file, how many there are, their permissions (Read, Write, Execute), and their individual entropy levels. Malicious files frequently use odd section names or show high entropy in the .rsrc (resource) or .reloc (relocation) sections to hide data [16]. The pipeline also pulls the list of DLLs and Windows API calls from the Import Address Table (IAT). The frequency of sensitive APIs, especially those used for registry manipulation or network communication, is a major tell for malicious intent [2].

Statistical and Format-Agnostic Data

Finally, the system extracts fixed-length vectors, such as 256-byte histograms and sliding-window byte-entropy histograms, along with string statistics like the count of URLs and IP addresses. These features provide a strong statistical baseline that works regardless of the specific file format. Best of all, they allow the model to make highly accurate decisions without the heavy processing power needed for a full code disassembly [5], [4].

Table **2**. Proposed static PE feature set for LightGBM classification

Category	Specific Features	Justification	Sources
Structural Metadata (Headers)	DOS Header (e_lfanew), COFF/File Header (NumberOfSections, Characteristics), Optional Header (ImageBase, AddressOfEntryPoint, Subsystem).	GBDT ensembles are statistically efficient on tabular metadata; they excel at modeling high-order, non-additive feature interactions through hierarchical partitioning (e.g., specific linker flags combined with entry point anomalies) that traditional linear models miss.	[1], [13], [17]
Content and Organization	Section Headers (.text, .data names/sizes), Data Directories (DataDirectories 8), Opcode sequences, Import/Export tables (DLL names, Windows API calls like NtAllocateVirtualMemory).	Tree-based models naturally handle heterogeneous feature groups (numeric counts vs. categorical API names) without extensive preprocessing; they are robust to code changes because they learn decision paths where the predictive meaning of a feature is highly conditional on others.	[10], [2]
Statistical and Format-Agnostic	256-Byte Histograms, Byte-Entropy Histograms (sliding window), String information (counts of URLs/IPs), String Entropy.	These models excel at modeling non-linear thresholds in high-dimensional tabular data (e.g., thresholding global entropy to identify packing) and can achieve inference speeds up to 64 times faster than deep learning models while capturing sparse, high-entropy signals.	[5], [15], [4], [9]

LightGBM Algorithm Specification

To manage high-dimensional vectors (like the 2,381 features found in EMBER), we rely on LightGBM. This model stands out because it uses two specific techniques to keep things running fast without sacrificing precision. Its leaf-wise tree growth naturally prioritizes features with the highest variance. This makes it incredibly efficient at thresholding high-dimensional, format-agnostic data, such as byte histograms. Plus, its built-in categorical handling processes structural header flags seamlessly, avoiding the massive memory drain usually caused by one-hot encoding [14], [1].

Key LightGBM Optimizations

Gradient-based One-Side Sampling (GOSS)

Instead of chewing through every single data point to calculate information gain, GOSS focuses on instances with large gradients, essentially the "under-trained" data. It then takes a random sample of the instances with small gradients. This massively cuts down on the computational heavy lifting while keeping the model's accuracy sharp [5], [8].

Exclusive Feature Bundling (EFB)

Since PE feature sets are often "sparse", meaning many features are mutually exclusive and rarely active at the same time, EFB bundles these features into a single column. This reduces the total feature count and speeds up the training process without losing any critical information [8].

III. COMPARATIVE ANALYSIS

Overview of the Benchmarking Landscape

Evaluation of modern malware classifiers requires a multi-dataset approach to account for the growing number of complex threats. Established benchmarks such as EMBER 2018 [1], BODMAS [5], and the Kaggle PE dataset [13] have provided the foundational corpus for static analysis, focusing primarily on structural metadata and byte-level histograms.

Table 3. Benchmark results of gradient boosting and neural models for PE malware detection

Dataset	Algorithm	Accuracy (%)	Precision	Recall	PR AUC / F1	Ref.
EMBER 2018	LightGBM	—	—	—	0.9421	[1]
EMBER 2024	Stacking Ensemble (LGBM/XGB/CB)	86.99	0.87	0.87	0.87	[16]
BODMAS	Improved ResNet (DRBCE)	91.28	—	—	0.9056	[5]
EMBER (Binary)	XGBoost	97.76	0.9776	0.9776	0.9776	[9]
OSG Academic	LightGBM	96.48	—	0.9803	—	[10]
C-Prot PE	XGBoost	99.81	99.62	100.00	99.81	[21]
IoT Malware (Any.Run)	CatBoost	99.00	0.990	0.979	0.989	[3]
Big-15	MLP (Warm)	97.90	—	—	—	[6]
Kaggle PE	Random Forest	98.91	—	99.02	98.91	[13]
AST-JS	XGBoost	—	0.9698	0.9981	0.9838	[11]

Table 3 shows that transitioning to the high-complexity EMBER 2024 version 3 framework [16] introduces a rigorous environment characterized by adversarial samples designed to mimic benign software. Robust model evaluation extends across various architectures, including Internet of Things (IoT) specific malware samples from the Any.Run [3] environment to large-scale binary classifications [9], [10]. Specialized datasets focusing on specific feature domains, such as the opcode-sequence based Big-15 [21] and Abstract Syntax Tree (AST-JS) representations [10], are essential to ensure that models maintain resilience against obfuscation across both Windows PE and web-based attack vectors.

Performance Metrics and the EMBER v3 Challenge Gap

A critical review of the metrics in Table 3 reveals a significant performance gap when transitioning from legacy distributions to modern, evasive datasets. While earlier iterations of the EMBER dataset allowed models like LightGBM to achieve a PR AUC of 0.9421 [1] and XGBoost to reach an accuracy of 97.67% in binary tasks [9], these figures drop sharply when faced with current threats.

The Stacking Ensemble evaluated on EMBER 2024 achieved an accuracy of only 86.99% [16]. This degradation highlights the impact of concept drift, where the statistical properties of malware features change over time.

Concept drift makes older models less efficient. The F1-Score of 0.87 [16] serves as a realistic baseline for hardened static detectors, which stands in sharp contrast to the F1-Score of 0.9776 seen in simpler binary variants [9]. This gap underscores the difficulty of detecting samples that are specifically hardened to bypass traditional byte-histogram features.

Algorithmic Comparison: GBDT vs. Neural Architectures

The data consistently support the effectiveness of Gradient Boosted Decision Trees (GBDT) over Deep Learning architectures for tabular PE metadata. In Table 3, the XGBoost and CatBoost variants achieve excellent results across multiple tests. XGBoost reached an accuracy of 99.81% on the C-Prot PE dataset [21] and an accuracy of 99.00% on the IoT Malware dataset [3]. The AST-JS feature learning approach using XGBoost yielded an F1-Score of 0.9838 [11].

In contrast, neural network implementations show lower relative performance on these feature sets, an improved ResNet model on BODMAS recorded an accuracy of 91.28% [5], while Warm MLP on Big-15 achieved 97.90% [6]. These results indicate that GBDT variants are superior in handling the high-dimensional, non-linear, and heterogeneous feature sets typical of PE headers and metadata, without the massive computational overhead that neural architectures require.

Feature Extraction Complexity and Evasion

The deciding factor in maintaining high detection rates amidst adversarial evolution is the sophistication of the feature engineering process. The high accuracy of LightGBM on the OSG Academic dataset (96.48%) [10] and the Random Forest model on Kaggle PE (98.91% F1-Score) [13] demonstrate that moving beyond raw byte histograms is crucial.

Sophisticated extraction techniques allow models to maintain exceptional sensitivity, as evidenced by the 100.00% recall achieved by XGBoost on the C-Prot PE dataset [21] and the 0.9981 recall on AST-JS features [11]. These high recall values prove that advanced static feature extraction, incorporating graph-based opcode sequences or semantic code structures, remains the primary defense against adversarial evasion. By providing the classifier with a nuanced representation of the file's intent, these methodologies bridge the gap between static efficiency and dynamic-level detection depth.

IV. Discussion and Results

Synthesis of Comparative Findings

Empirical evidence from comparative analysis highlights a key reality in static malware detection, algorithmic complexity cannot compensate for inadequate feature engineering when dealing with adversarial evolution. As demonstrated by the performance degradation between the legacy EMBER 2018 dataset [1] and the evasive payloads in the EMBER 2024

framework [16], static metadata is highly susceptible to concept drift [5].

Despite this aggressive evolution, Gradient Boosted Decision Trees (GBDTs) consistently establish the upper performance bound for tabular PE metadata. Models such as XGBoost [9], [21] and CatBoost [3] dramatically outperform deep neural architectures like Multilayer Perceptrons (MLP) [6] because tree-based ensembles natively isolate non-linear structural anomalies without the massive computational overhead required to map sparse, heterogeneous data in a neural network.

Algorithmic Efficiency: Leaf-wise vs. Level-wise Growth

A key observation from the comparative data is the superior speed-to-accuracy ratio of LightGBM, which enables it to maintain highly competitive metrics (e.g., an accuracy of 96.48% on the OSG Academic dataset [10]) while achieving a drastic reduction in training and inference time compared to other tree-based models.

This processing superiority is fundamentally rooted in its tree growth strategy. Traditional algorithms, such as Random Forest [13] and standard XGBoost implementations, typically utilize level-wise (depth-first) tree growth. Level-wise growth expands all nodes at the same depth indiscriminately, calculating unnecessary splits for low-variance leaves, which wastes computational resources on uninformative data.

In contrast, LightGBM employs leaf-wise (best-first) tree growth. It strictly expands the specific leaf that yields the maximum delta loss (variance reduction), regardless of its depth. By focusing exclusively on the most informative splits, LightGBM converges toward optimal decision boundaries much faster. When this leaf-wise expansion is paired with Gradient-based One-Side Sampling (GOSS), which filters out well-trained instances, and Exclusive Feature Bundling (EFB) for compressing sparse PE metrics, LightGBM effectively bypasses the memory and latency bottlenecks that hinder both traditional GBDTs and Deep Learning models.

Feature Interpretation: Benign vs. Malicious Profiles

The true strength of GBDT architectures lies in their ability to dynamically determine the threshold of structural anomalies generated by modern feature extraction pipelines. To illustrate why sophisticated extraction techniques reliably flag evasive malware (yielding recall rates as high as 0.9981 [11] and 100.00% [21]), it is useful to examine a conceptual snippet comparing a benign PE header with a malicious one:

Standard Benign PE Profile

A legitimate executable typically exhibits conventional section names (such as .text, .data, .rsrc), average global entropy in the range of 4.5 to 5.5, and .rsrc (resource) section entropy around 3.0. Its Import Address Table (IAT) is usually densely populated with standard user-interface and system execution APIs (such as user32.dll and advapi32.dll).

Evasive Malicious PE Profile

A packed or encrypted malware variant often displays anomalous, randomized, or missing section names (such as .upx0 and .xgf1). Its global entropy frequently approaches 7.8 (nearing the theoretical maximum of 8.0 for compressed/encrypted data), with suspiciously high entropy localized specifically within the .rsrc or .reloc sections to conceal the true payload. The IAT is often artificially thinned, utilizing only a few dynamic loading APIs (such as LoadLibraryA and GetProcAddress) to reconstruct the malicious payload in memory post-execution.

Models like LightGBM and XGBoost excel precisely because their leaf-wise decision paths naturally form logical gates around these specific anomalies (such as branching when .rsrc entropy > 7.2 and total IAT imports < 5). By bridging the gap between raw statistical data and structural intent, advanced static feature extraction remains the most robust defense against adversarial evasion.

V. Conclusion and Future Work

Conclusion

The rapid escalation of polymorphic and packed malware has necessitated a transition from traditional signature-based detection to machine learning models based on static analysis. This research presented a comprehensive evaluation of feature extraction techniques for Windows Portable Executable (PE) files, comparing the performance of Gradient Boosted Decision Trees (GBDT), specifically LightGBM, XGBoost, and CatBoost against Deep Learning architectures.

Comparative analysis definitively shows that for high-dimensional, structured tabular metadata (such as EMBER feature sets), tree-based ensembles significantly outperform neural networks in both predictive accuracy and computational efficiency. Models like XGBoost and LightGBM consistently achieved near-ceiling accuracy across multiple benchmarks. LightGBM proved exceptionally suitable for real-time endpoint implementation. Its use of leaf-wise tree growth, Gradient-based One-Side Sampling (GOSS), and Exclusive Feature Bundling (EFB) enables rapid processing of sparse, heterogeneous data, such as byte histograms, header flags, and section entropy without the massive memory overhead required by deep learning counterparts.

The evaluation highlighted the critical challenges of concept drift and adversarial evasion. The observed performance degradation between legacy datasets (such as EMBER 2018) and modern, evasion-heavy environments (such as EMBER 2024) proves that raw algorithmic power cannot compensate for outdated feature representations. Sophisticated, semantically aware static feature extraction remains the most robust defense against attackers who manipulate non-critical headers or inject padding to bypass detection.

Future Work

While optimized GBDT models operating on static PE features offer an excellent speed-to-accuracy ratio for pre-execution filtering, highly obfuscated or packed payloads can still conceal their true malicious intent from static parsers. To address this limitation, future research must pivot toward hybrid detection frameworks.

The logical next step is combining highly efficient static structured features (such as COFF headers and global entropy) with dynamic behavioral features extracted during sandbox detonation or emulation. The integration of dynamic telemetry, such as API call frequencies, file system interactions, and registry manipulations can provide the classifier with a definitive blueprint of the malware's execution logic.

Future architectures should explore advanced stacking ensembles or TabNet-based models that merge LightGBM's rapid static triage capabilities with Recurrent Neural Networks (RNNs) or Random Forests trained on sequential dynamic behaviors. This hybrid approach would maximize both the rapid pre-execution efficiency of static analysis and the post-execution depth of behavioral profiling. Ultimately, this would provide a more resilient defense against zero-day attacks and adversarial concept drift.

REFERENCES

[1] D.-C. Horvath and I. Zsigmond, "A Comparative Benchmark of Machine Learning Models for Static Malware Analysis: From EMBER 2018 to the Challenges of 2024:," in *Proceedings of the 18th International Conference on Agents and Artificial Intelligence*, Marbella, Spain: SCITEPRESS - Science and Technology Publications, 2026, pp. 2284–2291. doi: 10.5220/0014218700004052.

[2] D. Z. Syeda and M. N. Asghar, "Dynamic Malware Classification and API Categorisation of Windows Portable Executable Files Using Machine Learning," *Appl. Sci.*, vol. 14, no. 3, p. 1015, Jan. 2024, doi: 10.3390/app14031015.

[3] M. Maghanaki, S. Keramati, F. F. Chen, and M. Shahin, "Systematic Evaluation of Machine Learning and Deep Learning Models for IoT Malware Detection Across Ransomware, Rootkit, Spyware, Trojan, Botnet, Worm, Virus, and Keylogger," *Sensors*, vol. 26, no. 6, p. 1750, Mar. 2026, doi: 10.3390/s26061750.

[4] A. Ponte, D. Trizna, L. Demetrio, B. Biggio, I. T. Ogbu, and F. Roli, "SLIFER: Investigating performance and robustness of malware detection pipelines," *Comput. Secur.*, vol. 150, p. 104264, Mar. 2025, doi: 10.1016/j.cose.2024.104264.

[5] W. Maillet and B. Marais, "Optimized Deep Learning Models for Malware Detection under Concept Drift".

[6] A. S. Li, A. Iyengar, A. Kundu, E. Bertino, and A. Iyengar, "Revisiting Concept Drift in Windows Malware Detection: Adaptation to Real Drifted Malware with Minimal Samples," in *Proceedings 2025 Network and Distributed System Security Symposium*, San Diego, CA, USA: Internet Society, 2025. doi: 10.14722/ndss.2025.240830.

[7] A. Bensaoud, J. Kalita, and M. Bensaoud, "A Survey of Malware Detection Using Deep Learning".

[8] H. Jelodar, M. Meymani, S. Bai, R. Razavi-Far, and A. A. Ghorbani, "SBAN: A Framework & Multi-Dimensional Dataset for Large Language Model Pre-Training and Software Code Mining," 2025, *arXiv*. doi: 10.48550/ARXIV.2510.18936.

[9] U. Prasad and A. Chawla, "A Unified Evaluation of Learning-Based Similarity Techniques for Malware Detection," 2026, *arXiv*. doi: 10.48550/ARXIV.2602.15376.

[10] A. Mello, V. G. Lemos, F. Barbosa, and E. Simoni, "Malware identification on Portable Executable files using Opcodes Sequence," in *Anais do XVI Congresso Brasileiro de Inteligência Computacional*, SBIC, Dec. 2023, pp. 1–8. doi: 10.21528/CBIC2023-006.

[11] S. N. Wangari, "A Machine Learning Approach to Web-based CyberAttack Detection," Kobe University (Graduate School of Engineering), 2021. [Online]. Available: https://da.lib.kobe-u.ac.jp/da/kernel/D1008170/D1008170.pdf

[12] E. G. Villarroel Enriquez and J. Gutiérrez-Cárdenas, "Dynamic Malware Analysis Using Machine Learning-Based Detection Algorithms," *Interfases*, no. 019, pp. 119–138, Jul. 2024, doi: 10.26439/interfases2024.n19.7097.

[13] G. Mutlu, "Comparative Evaluation of Machine and Deep Learning Models for PE File Malware Detection".

[14] J. Banerjee, "Feature Selection and Transfer Learning in Network Data: Enhancing Anomaly Detection with Zero-Shot and Few-Shot Learning".

[15] L. De Rose, G. Andresini, A. Appice, and D. Malerba, "OLIVANDER: a counterfactual-based method to generate adversarial Windows PE malware," *Data Min. Knowl. Discov.*, vol. 39, no. 5, p. 46, Sep. 2025, doi: 10.1007/s10618-025-01127-1.

[16] A. Alotaibi, "Enhancing Malware Detection Using Machine Learning Models on Static Features," *Int. J. Adv. Comput. Sci. Appl.*, vol. 17, no. 2, 2026.

[17] S. L. Shiva Darshan and C. D. Jaidhar, "Performance Evaluation of Filter-based Feature Selection Techniques in Classifying Portable Executable Files," *Procedia Comput. Sci.*, vol. 125, pp. 346–356, 2018, doi: 10.1016/j.procs.2017.12.046.

[18] E. Martins, R. Sant'Ana, J. R. B. Higuera, J. A. S. Montalvo, J. B. Higuera, and D. P. Castillo, "Semantic Malware Classification Using Artificial Intelligence Techniques," *Comput. Model. Eng. Sci.*, vol. 142, no. 3, pp. 3031–3067, 2025, doi: 10.32604/cmes.2025.061080.

[19] A. Manikandaraja, P. Aaby, and N. Pitropakis, "Rapidrift: Elementary Techniques to Improve Machine Learning-Based Malware Detection," *Computers*, vol. 12, no. 10, p. 195, Sep. 2023, doi: 10.3390/computers12100195.

[20] Dr. W. Rose Varuna, Naveen S, Shruthi K, "Hybrid SVM–Random Forest Ensemble Superiority for Static Malware Detection: A Comparative Study," *Int. J. Recent Trends Multidiscip. Res.*, doi: https://doi.org/10.59256/ijrtmr.20260602001.

[21] N. Vuran Sarı and M. Acı, "A hybrid CNN-GRU model with XAI-Driven interpretability using LIME and SHAP for static analysis in malware detection," *PeerJ Comput. Sci.*, vol. 11, p. e3258, Oct. 2025, doi: 10.7717/peerj-cs.3258.

UDK 004.738.5:[004.85:005.334
DOI 10.7251/ZRSNG2526061M

Zero-trust arhitektura i održivost digitalnih sistema

Zero-trust architecture and sustainability of digital systems

Srđan Mičić, Federalna uprava policije Sarajevo/Directorate of Federal Police Sarajevo

Sažetak **– Razvojem informacionih tehnologija, arhitektura korporativnih digitalnih sistema također prolazi kroz duboke promjene, a granice unutar sistema između mrežnih nivoa postaju nedefinisane izazvane pojavom "cloud" tehnologija, mobilnih uređaja i rada na daljinu. Sve više kompanija zbog ekonomičnosti i bržoj dostupnosti svojim podacima, implementira cloud servere, što povećava rizik od kompromitacije podataka između "cloud" servera i interne mreže. Tradicionalni model sigurnosti zasnovan na mrežnom perimetru pokazao se nedovoljnim u navedenom okruženju. Kao odgovor na ove izazove razvijen je koncept Zero-Trust arhitekture (ZTA), koji zasniva na principu „nikada ne vjeruj, uvijek provjeri", što bi značilo da nijedan korisnik ili uređaj ne treba automatski smatrati pouzdanim. Cilj ovog rada je analizirati osnovne principe Zero-Trust arhitekture i razmotriti njen doprinos održivosti i otpornosti digitalnih sistema. Posebna pažnja posvećena je ulozi kontinuirane autentifikacije, upravljanja korisničkim računima i mikrosegmentacije u očuvanju sigurnosti digitalne infrastrukture.**

Ključne riječi **– Zero Trust arhitektura, održivost digitalnih Sistema**

Abstract **- With the development of information technologies, the architecture of corporate digital systems has undergone significant changes, and the boundaries within systems between network layers have become increasingly blurred due to the emergence of cloud technologies, mobile devices, and remote work. An increasing number of companies, driven by cost efficiency and faster access to their data, are implementing cloud servers, which increases the risk of data compromise between cloud servers and internal networks. The traditional security model based on the network perimeter has proven insufficient in such an environment. In response to these challenges, the concept of Zero Trust Architecture (ZTA) has been developed, based on the principle "never trust, always verify," meaning that no user or device should be automatically considered trustworthy.**
The aim of this paper is to analyze the fundamental principles of Zero Trust architecture and examine its contribution to the sustainability and resilience of digital systems. Special attention is given to the role of continuous authentication, user account management, and micro-segmentation in maintaining the security of digital infrastructure.

Keywords **– Zero Trust Architecture, sustainability of digital systems**

I. UVOD

Digitalni sistemi savremenog doba karakterišu kompleksne mrežne strukture, mobilni korisnici, "cloud" servisi i "remote" pristup (pristup sa udaljene lokacije). Ovakvo okruženje generiše nove bezbjednosne izazove, uključujući lateralno kretanje napadača, napade na privilegovane korisničkih računa i njihovu kompromitaciju.

Današnje aplikacije, sistemi i računarska mreža kao dio infrastrukture, moraju zadovoljiti funkciju zahtjeva krajnjih korisnika i pružiti svu potrebnu podršku radu sistema, što na prvom mjestu uključuje informacionu bezbjednost. U jednoj od definicja NIST-a (National Institute of Standards and Technology), ona predstavlja skup tehnika i metoda kojima se vrši prevencija oštećenja, informacionih, sistema i usluga uključujući i informacije sadržane u njima kako bi se osigurao njihov integritet, dostupnost i povjerljivost.

Prema izvještajima European Union Agency for Cybersecurity (ENISA), veliki procenat cyber incidenata povezan je s ljudskim faktorom, posebno kroz napade cryptolockera, phishinga i napade socijalnog inženjeringa (što direktno potvrđuje da ljudski faktor ostaje jedan od vodećih uzroka sigurnosnih povreda), cyber napadi sve češće zaobilaze tradicionalne perimetarske sigurnosne kontrole, gdje se ističe "Phishing" kao dominantan vektor upada u system (60%) i razvija se kroz tehnike koje se koriste u kampanjama velikih razmjera[1].

Koncept digitalne otpornosti razvijen je kao odgovor na potrebu organizacija da osiguraju nesmetan kontinuitet poslovanja i funkcionalnost sistema uprkos sigurnosnim incidentima. Zero-Trust pristup ima posebno važnu ulogu u kontekstu održivosti digitalnih sistema, jer omogućava

dugoročnu stabilnost i otpornost infrastrukture na cyber napade, tehničke greške i sistemske ranjivosti.

U radu će se analizirati naučna i stručna literaturea iz oblasti cyber sigurnosti, digitalne otpornosti i upravljanja informacionim sistemima. Analizirani su relevantni međunarodni standardi, istraživački radovi i izvještaji međunarodnih organizacija, uključujući dokumente koje objavljuje National Institute of Standards and Technology u vezi sa Zero-Trust arhitekturom. Pored toga, primijenjena je komparativna analiza tradicionalnog sigurnosnog modela zasnovanog na mrežnom perimetru i savremenog Zero-Trust pristupa. Analiza obuhvata ključne komponente sigurnosne arhitekture kao što su autentifikacija korisnika, upravljanje identitetom, kontrola pristupa i segmentacija mreže.

II. KONCEPT ZERO-TRUST ARHITEKTURE

Zero-Trust arhitektura predstavlja sigurnosni model koji se temelji na principu kontinuirane provjere identiteta i pristupa resursima. Za razliku od tradicionalnih modela Savremeni digitalni sistemi suočavaju se sa sve složenijim sigurnosnim izazovima koji proizlaze iz ubrzanog razvoja informacionih tehnologija, širenja cloud infrastrukture, mobilnih uređaja i rada na daljinu. U takvom okruženju tradicionalni sigurnosni modeli zasnovani na zaštiti mrežnog perimetra više ne pružaju dovoljan nivo zaštite. Zbog toga se sve veća pažnja posvećuje implementaciji koncepta Zero Trust Architecture, koji polazi od pretpostavke da nijedan korisnik, uređaj ili aplikacija ne smije biti automatski smatran pouzdanim bez prethodne provjere.

Analiza osnovnih principa Zero-Trust arhitekture pokazuje da kontinuirana autentifikacija, stroga kontrola pristupa, princip minimalnih privilegija i mikrosegmentacija mreže značajno doprinose smanjenju rizika od neovlaštenog pristupa i kompromitacije podataka. Primjenom ovih mehanizama organizacije mogu efikasnije kontrolisati pristup digitalnim resursima i pravovremeno otkriti potencijalne sigurnosne incidente.

Takođe, implementacija Zero-Trust modela ima važnu ulogu u jačanju održivosti i otpornosti digitalnih sistema. Kada gledamo na digitalnu otpornost ona podrazumijeva sposobnost sistema da:

1. Spriječi napad
2. Detektuje prijetnju
3. Odgovori na incident
4. Obnovi funkcionalnost
5. Prilagodi se budućim rizicima[2]

ZTA kroz stalni nadzor, verifikaciju identiteta i segmentaciju mrežnih resursa, organizacije postaju sposobnije da spriječe širenje napada, zaštite kritične podatke i osiguraju kontinuitet poslovanja čak i u uslovima povećanih cyber prijetnji.

Može se zaključiti da Zero-Trust arhitektura predstavlja jedan od ključnih pravaca razvoja savremene cyber sigurnosti. Njena primjena ne samo da povećava nivo zaštite digitalne infrastrukture, već doprinosi i dugoročnoj stabilnosti, pouzdanosti i održivosti digitalnih sistema u savremenom tehnološkom okruženju koji pretpostavljaju da su korisnici unutar mreže pouzdani, Zero-Trust pristup pretpostavlja da potencijalna prijetnja može postojati bilo gdje u sistemu.

Zero-Trust nije isključivo tehnički model i njegova efikasnost zavisi od pravilne klasifikacije podataka, upravljanja identitetima, multifaktorske autentifikacije, ponašajnog nadzora korisnika, kulture odgovornosti zaposlenih. Bez razvijene sigurnosne kulture, zaposlenici mogu zaobići MFA, dijeliti lozinke ili koristiti nesigurne kanale komunikacije, čime se narušava integritet ZTA.

Prema modelu definisanom od strane National Institute of Standards and Technology, Zero-Trust arhitektura podrazumijeva sigurnosni pristup u kojem nijedan korisnik ili uređaj ne dobija implicitno povjerenje, već se svaki zahtjev za pristup resursima mora autentificirati i autorizirati[3]. Glavni principi Zero-Trust modela uključuju:

1. Verifikaciju identiteta korisnika i uređaja
2. Princip najmanjih privilegija (least privilege)
3. Kontinuirani nadzor i analizu pristupa
4. Mikrosegmentaciju mreže
5. Korištenje višefaktorske autentifikacije

Ovi principi omogućavaju kompanijama da značajno smanje prostor za napad i ograniče potencijalnu štetu u slučaju kompromitacije sistema.

III. KOMPONENTE ZERO-TRUST SISTEMA

Zero-Trust predstavlja bezbjednosni model zasnovan na principu da se povjerenje ne dodjeljuje unaprijed nijednom entitetu u mreži, već se svaki zahtjev za pristup resursima mora kontinuirano verifikovati na osnovu identiteta i konteksta. U okviru Zero-Trust modela poseban naglasak stavlja se na granularniju kontrolu pristupa, autentifikaciju i autorizacijusvakog zahtjeva i transakcije, princip najmanjih privilegija i kontinuiran monitoring sistema.

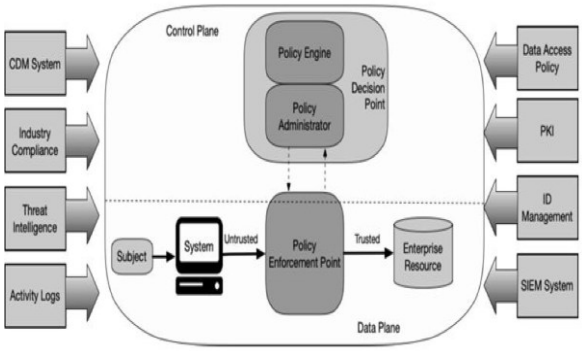
Zero-Trust arhitektura sastoji se od više ključnih komponenti koje zajedno osiguravaju kontrolu pristupa i sigurnost digitalnih resursa. Najvažnije komponente uključuju logički model[4]:

1. Generator politika “Policy Engine” (komponenta koja donosi odluku o pristupu određenom resursu. Ona analizira različite informacije kao što su identitet korisnika, sigurnosne politike organizacije, stanje uređaja i druge sigurnosne signale kako bi odlučila da li će pristup biti odobren ili odbijen);

2. Administrator politika “Policy Administrator” (provodi odluku koju je donio Policy Engine.

Njegova funkcija je da uspostavi ili prekine komunikaciju između korisnika i resursa, te generiše autentifikacione tokene ili kredencijale potrebne za pristup sistemu);

3. Tačka upisivanja politika "Policy Enforcement Point" (komponenta koja tehnički sprovodi sigurnosne odluke. Ona omogućava, nadgleda i po potrebi prekida vezu između korisnika i digitalnih resursa kako bi se osiguralo da se pristup odvija u skladu sa sigurnosnim pravilima).



Slika 1. Logički model ZTA [5].

Takva arhitektura omogućava fleksibilnu i skalabilnu zaštitu digitalne infrastrukture, posebno u cloud okruženjima i distribuiranim mrežama.

IV. ZERO-TRUST I ODRŽIVOST DIGITALNIH SISTEMA

Zero-Trust i održivost digitalnih sistema je savremeni koncept u oblasti cyber sigurnosti i upravljanja digitalnom infrastrukturom. Kombinuje sigurnosni model „nultog povjerenja" sa ciljem dugoročne stabilnosti i otpornosti digitalnih sistema. Digitalna otpornost podrazumijeva sposobnost sistema da spriječi napad, detektuje prijetnju, odgovori na incident, obnovi funkcionalnost sistema. Održivi digitalni sistemi moraju biti sposobni da funkcionišu čak i u uslovima cyber napada ili tehničkih kvarova. Zero-Trust arhitektura doprinosi digitalnoj otpornosti kroz smanjenje mogućnosti neovlaštenog pristupa, ograničavanje širenja napada unutar mreže i bržu detekciju sigurnosnih incidenata .[6]

Implementacija Zero-Trust principa ima značajan doprinos i održivosti digitalnih sistema, jer omogućava veću otpornost na sigurnosne incidente, bržu detekciju prijetnji i efikasniji oporavak nakon napada. Time Zero-Trust arhitektura postaje jedan od ključnih koncepata savremene cyber sigurnosti i važan element u izgradnji stabilnih i dugoročno održivih digitalnih infrastruktura.

Istraživanja pokazuju da implementacija Zero-Trust modela može značajno smanjiti troškove sigurnosnih incidenata i poboljšati sposobnost organizacija da odgovore na cyber prijetnje. [7]

Regulatorni okvir Evropske unije dodatno naglašava značaj otpornosti kroz Digital Operational Resilience Act (DORA), koji zahtijeva kontinuirano upravljanje ICT rizicima i testiranje operativne otpornosti.[8] Digitalna infrastruktura danas sve više zavisi od "cloud" tehnologija i distribuiranih servisa. U takvom okruženju tradicionalna sigurnosna rješenja postaju neefikasna jer se mrežni perimetar praktično gubi.

V. ODRŽIVOST DIGITALNIH SISTEMA KROZ ZERO-TRUST PRISTUP

Primjena Zero-Trust modela doprinosi održivosti sistema kroz modularnu i adaptivnu arhitekturu koja omogućava lakšu integraciju novih tehnologija i servisa. Za razliku od tradicionalnih sigurnosnih modela zasnovanih na zaštiti mrežnog perimetra, Zero-Trust pristup podrazumijeva kontinuiranu verifikaciju korisnika, uređaja i aplikacija prije odobravanja pristupa digitalnim resursima. Ovakav pristup smanjuje mogućnost neovlaštenog pristupa i povećava otpornost sistema na savremene cyber prijetnje. Prema preporukama koje je objavio National Institute of Standards and Technology, Zero-Trust arhitektura pomjera fokus zaštite sa mrežnog perimetra na identitet korisnika, uređaje i digitalne resurse, uz pretpostavku da mreža može biti kompromitovana u bilo kojem trenutku. [9]

Održivost digitalnih sistema ne zavisi isključivo od tehnoloških rješenja, već i od organizacionih i regulatornih faktora. Integracija Zero-Trust pristupa sa međunarodnim sigurnosnim standardima, kao što je ISO/IEC 27001, omogućava sistematsko upravljanje sigurnošću informacija i kontinuirano unapređenje sigurnosnih kontrola.[10] Takođe, usklađenost sa savremenim regulatornim okvirima, poput Digital Operational Resilience Act (DORA), doprinosi jačanju digitalne otpornosti organizacija i smanjenju sistemskih rizika u digitalnom okruženju[11].

Pored tehnoloških i regulatornih aspekata, važnu ulogu u implementaciji Zero-Trust modela imaju organizacione mjere kao što su upravljanje identitetima i pristupom, kontinuirana procjena rizika i edukacija zaposlenih. Kombinacija ovih elemenata omogućava organizacijama da izgrade sigurnu i održivu digitalnu infrastrukturu koja je sposobna da odgovori na savremene sigurnosne izazove i osigura dugoročnu stabilnost informacionih sistema.

VI. ZAKLJUČAK

Savremeni digitalni sistemi suočavaju se sa sve složenijim sigurnosnim izazovima koji proizlaze iz ubrzanog razvoja informacionih tehnologija, širenja cloud infrastrukture, mobilnih uređaja i rada na daljinu. U takvom okruženju tradicionalni sigurnosni modeli zasnovani na zaštiti mrežnog perimetra više ne pružaju dovoljan nivo zaštite. Zbog toga se sve veća pažnja posvećuje implementaciji koncepta Zero Trust Architecture, koji polazi od pretpostavke da nijedan

korisnik, uređaj ili aplikacija ne smije biti automatski smatran pouzdanim bez prethodne provjere.

Analiza osnovnih principa Zero-Trust arhitekture pokazuje da kontinuirana autentifikacija, stroga kontrola pristupa, princip minimalnih privilegija i mikrosegmentacija mreže značajno doprinose smanjenju rizika od neovlaštenog pristupa i kompromitacije podataka. Primjenom ovih mehanizama organizacije mogu efikasnije kontrolisati pristup digitalnim resursima i pravovremeno otkriti potencijalne sigurnosne incidente.

Takođe, implementacija Zero-Trust modela ima važnu ulogu u jačanju održivosti i otpornosti digitalnih sistema. Kroz stalni nadzor, verifikaciju identiteta i segmentaciju mrežnih resursa, organizacije postaju sposobnije da spriječe širenje napada, zaštite kritične podatke i osiguraju kontinuitet poslovanja čak i u uslovima povećanih cyber prijetnji.

Može se zaključiti da Zero-Trust arhitektura predstavlja jedan od ključnih pravaca razvoja savremene cyber sigurnosti. Njena primjena ne samo da povećava nivo zaštite digitalne infrastrukture, već doprinosi i dugoročnoj stabilnosti, pouzdanosti i održivosti digitalnih sistema u savremenom tehnološkom okruženju.

LITERATURA

[1] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[2] ISO/IEC 27001:2022 – Information security management systems Requirements https://km.thainsw.net/kmdcs/images/File/ISO%2027001-2022%20rm.pdf

[3] Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, NIST Special Publication 800-160, Volume 2, National Institute of Standards and Technology, Gaithersburg, 2021, https://www.solvitursystems.com/post/understanding-nist-special-publication-800-207-the-roadmap-to-zero-trust-architecture?utm

[4] National Institute of Standards and Technology, Implementing a Zero Trust Architecture. (NIST Computer Security Resource Center), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-35.pdf

[5] S. Rose, S. Mitchell, S. Connelly, „Zero Trust Architecture“, NIST SP 800-207, 2020.

[6] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (NIST Special Publication 800-207)*.National Institute of Standards and Technology.

[7] Yusuf, A. M. i dr., Zero Trust Architecture as a New Paradigm in Cyber Security, Journal of Embedded Systems, Security and Intelligent Systems(https://www.researchgate.net/publication/395708909_Zero_Trust_Architecture_as_a_New_Paradigm_in_Cyber_Security)

[8] Regulation (EU) 2022/2554 – Digital Operational Resilience Act (DORA), https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

[9] Rose, S., Borchert, O., Mitchell, S., Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and TechnologyZero Trust Architecture – Principles and Implementation.

[10] International Organization for Standardization (2022). ISO/IEC 27001: Information Security Management Systems. https://km.thainsw.net/kmdcs/images/File/ISO%2027001-2022%20rm.pdf

[11] European Union (2022). Regulation (EU) 2022/2554 – Digital Operational Resilience Act (DORA). https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

UDK 004.85:[005.334:338.583
DOI 10.7251/ZRSNG2526065S

Li-Fi Communication in the Context of Zero Trust Security Models

Ljubinko Stojanović, Vesna Radojčić, Petar Spalević, University Sinergija, Bijeljina

***Abstract* — Greater decentralization of modern IT environments, driven by distributed infrastructure, IoT devices, etc., has highlighted the limitations of traditional perimeter-based security models, which are based on the assumption that the internal network is trusted, while threats exist exclusively outside of it. Implicit trust and broad internal access that perimeter environments have can create – and do create – favorable conditions for lateral movement, insider misuse, and unauthorized access. This paper examines Zero Trust Architecture (ZTA) as a security paradigm designed to address these weaknesses. In parallel, the paper analyzes Li-Fi (Light Fidelity) communication as an alternative wireless technology whose physical properties, including spatial signal limitation and reduced penetration through walls, offer significant cybersecurity advantages compared to conventional radio-frequency systems, but since the physical environment alone does not guarantee protection, cryptographic protection mechanisms in Li-Fi environments are emphasized. By combining the Zero Trust model with Li-Fi communication and secure key management mechanisms, a layered approach is provided for securing sensitive internal wireless communication against eavesdropping, message manipulation, and unauthorized access.**

Keywords – ZTA (Zero Trust Security Models), Li-Fi (Light Fidelity), Perimeter, Unauthorized Access, Encryption

I. INTRODUCTION

The digitalization of infrastructure has fundamentally weakened the boundaries of the traditional network. Enterprises, currently, increasingly operate through cloud platforms, distributed infrastructure with employees located in different locations; therefore, security models are structurally no longer adequate. The paper from 2020 confirms this, stating that "this complexity has outstripped legacy methods of perimeter-based network security as there is no single, easily identified perimeter for the enterprise" [1] and also that "zero trust security models assume that an attacker is present in the environment and that an enterprise-owned environment is no different – or no more trustworthy – than any nonenterprise-owned environment" [1]. Zero Trust Architecture (ZTA), a term first introduced by John Kindervag [2], [3], emerged as a structural response, built on the principle of "verify and never trust" [3]. Security paradigms have historically developed reactively – as a response to new threats and attacks. According to the paper from "The concept of cybersecurity emerged alongside the development of computer networks and digital communication systems," with early security focused on physical access control of ARPANET mainframe systems [4].

The drawback of perimeter-based models, fundamentally, is their binary trust model. Entities within the network boundaries receive implicit permanent trust (if the user is outside the network → considered untrusted; if the user is inside the network → automatically considered trusted) without additional verification of identity or access context. In practice, a compromised computer within the network can freely access other systems. Once it breaches the perimeter, it can move through the network, and so-called lateral movement becomes relatively simple. As a result, "unauthorized lateral movement within the environment has been one of the biggest challenges" [1]. The CCDCOE Insider Threat Study [5] confirms the previous statement based on the analysis of the Snowden and Manning cases, where it is seen that the greatest damage was caused precisely by users with legitimate access (implicit, permanent trust) granted by the perimeter.

The evolution and change of threats in decentralized IT systems have created a completely different set of attack vectors and adversarial methodologies that differ fundamentally from the threats that formed the basis for the structure of traditional, perimeter-oriented security architectures. [6] In traditional enterprise security models, the perimeter refers to the conceptual and technical boundary that separates the organizational internal network – assumed to be trusted – from external, untrusted networks such as the public internet; the perimeter model envisions the network as a fortress where the interior is secure, and all entrances are controlled and filtered. [7] Perimeter protection is achieved through technical mechanisms such as Firewalls, Gateway proxies, Intrusion detection/prevention systems (IDS/IPS), and virtual private networks (VPN). [8] Therefore, perimeter-oriented security architectures were built on the principle of strong external defense and relatively permissive internal access. [9] Once a user authenticates and passes the perimeter boundary, they are often granted broad lateral movement privileges within the internal network. The perimeter model emerged in an era when business infrastructure was physically centralized, applications were hosted locally, employees worked within enterprise facilities, and the network topology was relatively static, making defense of a clearly identifiable boundary technically feasible and operationally rational. [10]

At its core, Li-Fi is a wireless optical network created as an extension of visible light communication (VLC) that transforms lighting fixtures into access points and integrates with the existing network ecosystem. [11] It has proven to be „an efficient solution for wireless communication, offering advantages such as superior cybersecurity [12].“

II. CONCEPT OF ZERO-TRUST ARCHITECTURE

The Zero Trust Architecture (ZTA) represents a security model based on the assumption that no element within the system possesses implicit trust. „No user, device, or application – not even those inside the network – should be automatically trusted." [13] The fundamental principle of ZTA is expressed as „never trust, always verify," which means that every connection and request for access to resources is verified in real time. [13] [14] The National Institute of Standards and Technology (NIST) defines Zero Trust Architecture as „an enterprise cybersecurity architecture based on zero trust principles and designed to prevent data breaches and limit internal lateral movement of attackers," [1] viewing the network as potentially compromised and applying the strictest criteria for identity verification and authorization of every request for resource access. [13], [15] Conventional perimeter-based security models assume that threats originate outside the network, treating the internal environment as inherently secure. However, IT systems – including cloud services, IoT devices – are geographically and technologically distributed, and thus the network boundary practically does not exist. As a result, traditional measures such as Firewalls and VPNs are insufficient to prevent and protect against threats originating from within [14], [1], and Zero Trust Architecture (ZTA) has emerged as a paradigm representing the „presence of an attacker within the environment" [1] and requiring continuous verification of the identity of all users, regardless of their location. ZTA is based on a set of technical principles that NIST classifies as seven fundamental tenets, defining how an organization should protect data and resources regardless of network context:

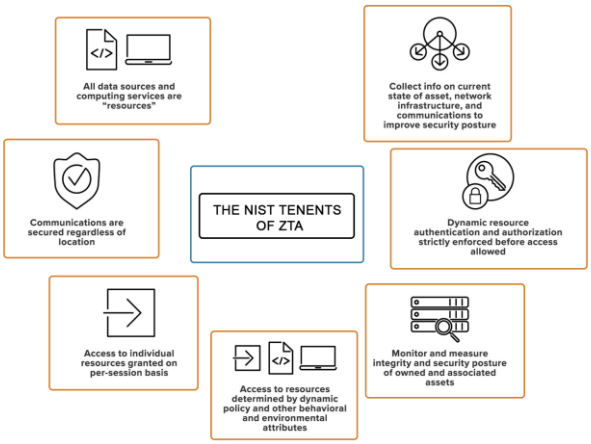


Illustration 1. NIST tenets of Zero Trust Architecture. [16]

According to the National Institute of Standards and Technology, the key elements of the ZTA model include control points (Policy Enforcement Points – PEP), a decision-making module (Policy Engine – PE), and a component responsible for implementing decisions (Policy Administrator – PA). [1] The set of control points forms the control layer of the network, separated from the data flow, so that every connection is verified through an autonomous decision system. The Policy Engine collects information from various sources (databases, device management systems, etc.) and applies a trust algorithm to approve or deny the access request – the policy is established for a specific resource based on initial rules and additional real-time factors. [15]

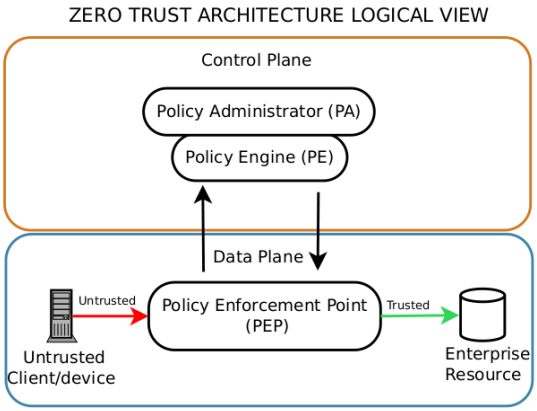
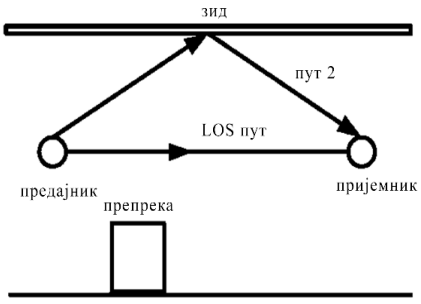


Illustration 2. Zero Trust Architecture logical view [17]

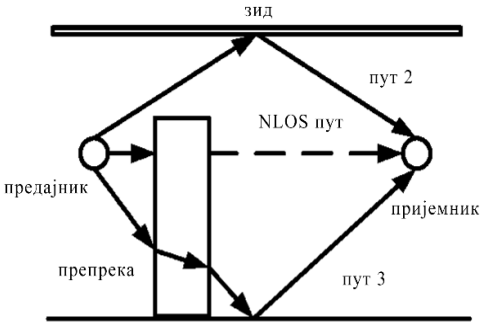
III. LI-FI (LIGHT FIDELITY) COMMUNICATION OVERVIEW

In a Li-Fi system, the transmitter is usually an LED light source (or a group of LEDs as in a lighting fixture), while the receiver is a photodetector (PD) consisting of one or more photodiodes (or a group of photodiodes). Data is transmitted by modulating the current of the LED, which changes the light intensity, and the photodetector converts the light intensity into an electrical current. [11]

A Li-Fi system uses light photons instead of RF waves, so the signal requires optical visibility or reflections in order to reach the receiver. Unlike radio waves, light does not penetrate opaque obstacles (e.g., walls) [11], which means that the coverage of a Li-Fi network is limited to the room in which the light source is located. [12] The advantage of this property is that there is no mutual interference between neighboring rooms, and security is improved (the signal is „contained" within the room). The drawback, however, is sensitivity to signal blockage – if an obstacle appears between the LED and the photodiode, the direct signal will be interrupted. In such situations, reception is possible through diffuse reflections from walls or the ceiling, but with a significantly weaker signal level. [12] Because of this, Li-Fi systems usually require multiple lighting fixtures within a single room in order to ensure good coverage regardless of the user's position. The Li-Fi channel consists of two types of paths: a direct path with a line of sight (Line-of-Sight, LOS) and indirect paths without direct visibility (Non-Line-of-Sight, NLOS) [18] created by reflections from surfaces within the room.



a) LOS path



b) NLOS path

Diagram 1. Schematic diagram of signal propagation paths within a room with obstacles (LOS and NLOS) [11]

The limited range and the signal contained within the room naturally increase security against remote attacks (e.g., an attacker standing outside the room cannot eavesdrop on the connection, unlike in Wi-Fi systems [11]). In addition, it is important to emphasize that the Li-Fi connection is limited to the illuminated zone, i.e., it is easier to physically control user access (e.g., motion detectors in the room). [12] On the other hand, in the case where light passes through a window or similar openings, the signal can be intercepted from the immediate surroundings, which indicates that, without encryption, there is still a risk of interception. [11]

Encryption can be implemented in the application software itself before the data enters the Li-Fi interface (SSL/TLS tunnel, or VPN, or some other tool) – advantage: high flexibility and independence from the physical characteristics of the connection; disadvantage: it depends on the built-in cryptography on end devices and reduced performance (additional processing) [20]. At the MAC layer level, Li-Fi devices can use standards similar to Wi-Fi mechanisms. IEEE 802.15.7 standards for visible optical communication allow the use of encryption that is otherwise applied in wireless networks (AES, WPA2 [11]). The advantage of this encryption is in terms of standardization and a smaller impact on the physical layer (entire MAC frames are encrypted before modulation), but latency increases [20].

The most important cryptosystem for Li-Fi is AES (Advanced Encryption Standard). It is also considered an industry standard and is usually used with an authenticated mode (e.g., CCM or GCM). Advanced Encryption Standard (AES) is a symmetric block cryptography algorithm that is an international standard for the security of digital data. [21] It replaced DES, which was widely used but was replaced due to its short key length. It makes all actions that an entity may use more difficult, preventing code breaking by entities that should not have access to the information. Other symmetric algorithms include Blowfish and older Rivest ciphers such as RC4, RC5, and RC6. [20] These algorithms are mentioned in the literature as examples that can be applied within the Li-Fi framework. The application of appropriate cryptographic algorithms enables a high level of protection: the use of AES-128-GCM [23], for example, in demonstration Li-Fi systems protects against eavesdropping and unauthorized modifications. This project combines authenticated encryption and persistent key management to ensure the confidentiality and integrity of Li-Fi-transmitted data. By using AES-128-GCM and secure session-key provisioning between the Raspberry Pi Pico and the host, it establishes a protected communication channel resistant to unauthorized access and message tampering.

IV. CONCLUSION

This paper examined the limitations of traditional perimeter-based security models in the context of modern, decentralized IT environments and highlighted the necessity for more adaptive and resilient security paradigms. In this regard, Zero Trust Architecture (ZTA) was analyzed as a contemporary approach that eliminates implicit trust and enforces continuous verification of all entities, regardless of their location within or outside the network.

In parallel, the paper explored Li-Fi (Light Fidelity) communication as an emerging wireless technology with inherent physical-layer security advantages. Due to its reliance on visible light, Li-Fi offers spatial confinement of the signal, reduced penetration through physical barriers, and lower susceptibility to remote interception compared to conventional radio-frequency systems. However, it was emphasized that these physical properties alone are not sufficient to ensure complete security, which necessitates the implementation of robust cryptographic mechanisms.

The main contribution of this paper lies in highlighting the complementary nature of ZTA and Li-Fi technologies. While ZTA provides a strong logical and architectural security framework based on strict access control and continuous authentication, Li-Fi enhances security at the physical layer by limiting signal exposure. Their combined application enables a layered security approach that significantly reduces the risk of eavesdropping, unauthorized access, and lateral movement within internal networks.

Future research directions should focus on the development of integrated architectures that explicitly combine ZTA principles with Li-Fi communication systems in

real-world environments. Additionally, experimental validation of such models through simulations or prototype implementations is necessary to evaluate performance, scalability, and resistance to advanced attack scenarios.

REFERENCES

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology, 2020, pp. 1, 4, 6-7.

[2] F. Mensah, "Zero Trust Architecture: A Comprehensive Review of Principles, Implementation Strategies, and Future Directions in Enterprise Cybersecurity," International Journal of Academic and Industrial Research Innovations (IJAIRI), vol. 10, 2024, pp. 340.

[3] J. Kindervag, *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*, Cambridge, MA, USA: Forrester Research Inc., 2010, pp. 9.

[4] S. N. Asha, B. Asiya Banu, and M. J. Swetha, "Cybersecurity: Evolution, challenges, and future directions in digital security," *World Journal of Advanced Research and Reviews*, vol. 10, no. 01, 2021, pp. 428.

[5] M. Kont, M. Pihelgas, J. Wojtkowiak, L. Trinberg, and A.-M. Osula, *Insider Threat Detection Study*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2018.

[6] D. Kipkoech and S. Ng'etich, A Survey of Security in Zero Trust Network Architectures, GSC Advanced Research and Reviews, vol. 22, 2025, pp. 182-183.

[7] S. Pagadala Sekar, Integrating software-defined perimeter and zero trust in platform engineering: A security framework for modern infrastructure, *World Journal of Advanced Engineering Technology and Sciences*, vol. 15, no. 02, 2025, pp. 357–379.

[8] R. Chandramouli, *Guide to a Secure Enterprise Network Landscape*, NIST Special Publication 800-215, National Institute of Standards and Technology, Gaithersburg, MD, 2022, pp. 5.

[9] P.-Y. Chen, S. Choudhury, L. Rodriguez, A. O. Hero III, and I. Ray, Enterprise Cyber Resiliency Against Lateral Movement: A Graph Theoretic Approach, arXiv preprint, 2019, pp. 1-2.

[10] M. Chauhan and M. Sharma, A Comprehensive Survey on Zero Trust Architecture: Advancements, Challenges, and Future Trends, Journal of Emerging Technologies and Innovative Research (JETIR), vol. 12, no. 6, 2025, pp. 321-322, 324.

[11] Lj. Stojanović, LI-FI Systems, Master's thesis, Faculty of Computer Science and Informatics, Sinergija University, Bijeljina, Republic of Srpska, 2025, pp. 1, 3, 15-20.

[12] Lj. Stojanović, V. Radojčić, S. Mitrović, and P. Spalević, Li-Fi Technology for Cybersecurity Solutions + SEON, 2025, pp. 56-58.

[13] S. Mushtaq, M. Mohsin, and M. M. Mushtaq, A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains, Sensors (Basel), vol. 25, no. 19, 2025, pp. 2, 5.

[14] M. L. Gambo i A. Almulhem, Zero Trust Architecture: A Systematic Literature Review, *arXiv preprint*, 2025, pp. 1, 3, 25, 28.

[15] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, „Verify and trust: A multidimensional survey of zero-trust security in the age of IoT," Internet of Things, vol. 27, 2024, p. 101227.

[16] M. Heath and S. Vinberg, What Is Zero Trust Architecture (ZTA)?, F5 Labs, Figure 1: NIST tenets of zero trust architecture, [Online]. Available: https://www.f5.com/labs/articles/what-is-zero-trust-architecture-zta.

[17] A. Blanc, My take on Zero Trust – SP 800-207, Blog Inforeseau.com, 2019, [Online]. Available: https://blog.inforeseau.com/my-take-on-zero-trust-sp-800-207.

[18] S. Ullah, S. U. Rehman, and P. H. J. Chong, "A comprehensive open-source simulation framework for LiFi communication", Sensors, vol. 21, no. 7, 2021, pp. 2, 4-6.

[19] Lj. Stojanović, V. Radojčić, and P. Spalević, Li-Fi, AI and IoT Technologies in Creating Sustainable Business, 2025, pp. 62-63, 65.

[20] M. M. Msallam and R. Samet, A Review of Security Methods in Light Fidelity Technology, Proceedings of Engineering and Technology Innovation, vol. 27, 2024, pp. 6-8, 9, 12.

[21] T. Sukiman, C. Sandy, R. Meiyanti, R. Rizal, and S. Anshari, Implementation of AES Algorithm for Text Message Encryption and Decryption Process, Gameology and Multimedia Expert, vol. 3, no. 1, 2026, pp. 25-27.

[22] N. Kumar, P. Lalwani, H. Lamkuche, G. Samara, H. Abu Mariah, and N. Patel, Deep Learning Based Analysis of the Key Scheduling Algorithm of AES Cipher, 2026, pp. 1975.

[23] Iotauth, „Lifi-auth," GitHub repository, [Online]. Available: https://github.com/iotauth/lifi-auth.

UDK 005.334:338.583]:004.85(100)
DOI 10.7251/ZRSNG2526069S

Authentication and Access Control in Li-Fi-Based Wireless Networks

Ljubinko Stojanović, Petar Spalević, University Sinergija, Bijeljina

***Abstract* — Light Fidelity (Li-Fi) represents an emerging wireless communication paradigm that operates within heterogeneous network environments characterized by high mobility, multi-user access, and frequent handovers between technologies. While Li-Fi offers significant advantages in terms of bandwidth and spatial confinement through optical „attocell" domains, these same characteristics introduce a distinct and complex security landscape.**

Threat models emphasize the importance of the attacker's spatial position and optical visibility, going beyond the traditional division into internal and external actors. Active and passive attacks, including interception through reflection and light leakage, etc., can exploit the physical characteristics of the system to compromise the confidentiality and integrity of communication. Special focus is placed on the CIA+Auth model (confidentiality, integrity, availability, and authentication) as the basis for designing secure systems. The ABAC model provides greater flexibility and suitability for Li-Fi environments due to the ability to include contextual factors such as location, time, and risk level.

Keywords – CIA (Confidentiality, Integrity, Availability), Li-Fi (Light Fidelity), Authentication, Access Control

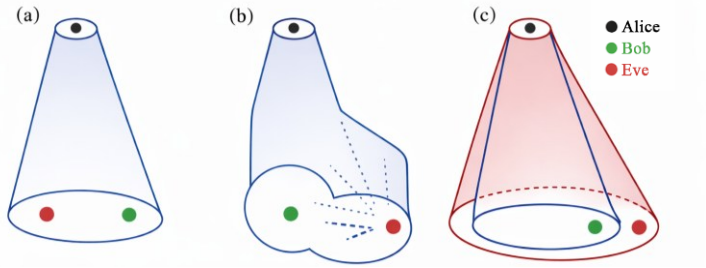
I. INTRODUCTION

In practice, we can encounter two standardization lines: 1. The IEEE 802.11bb standard from 2023 formally introduced light communications into the IEEE 802.11 ecosystem [1], thereby bringing Li-Fi closer to existing Wi-Fi network architectures and security mechanisms; 2. The IEEE 802.15.7 standard for short-range optical wireless links (PHY/MAC) [2].

Security requirements in Li-Fi networks are based on protecting communication against eavesdropping, jamming, spoofing, and node compromise, while adapting to the physical and operational behavior of the light medium [3]. The conclusion drawn in the contemporary literature on optical wireless links is that the „physical confinement of light" [1] exists, but it is not a sufficient security guarantee – reflections [4], light leakage [5], etc. From this follows the fundamental requirement – Li-Fi networks must have a cryptographically clear model (CIA+Auth) independent of assumptions about LoS/NLoS [1].

II. SECURITY THREATS IN LI-FI SYSTEMS

Li-Fi is treated as part of heterogeneous networks with mobility, handover, and multi-user access; while the optical layer provides high capacity in „attocell" [1] domains. Based on such an architecture, a) vertical handover between technologies [6], [1] and b) shared AAA policies between access domains [7] are introduced. Threat models according to the VLC/Li-Fi security literature are explicitly classified by spatial position and optical visibility, and not only by network privileges (outsider/insider) [5], and can be divided roughly, for the purpose of requirements design, into: 1) outsider threat [5] – does not possess network privileges nor cryptographic keys (attempts interception through leakage/reflections or jamming); 2) insider threat – possesses access to the light-covered zone or is a group member (e.g. possesses a group key [8]) and these attacks can be classified more into the domain of abuse of legitimate privileges, especially when group keys are concerned; 3) active threat with an optical injector [5] – uses an LED or laser source (or a compromised „smart" luminaire) for spoofing [9] or jamming, which is particularly important for „smart lighting" – IoT ecosystems [1]; 4) passive threat with enhanced optics (uses receivers to improve SNR and intercept weak reflected components), while attacks can be divided into: 1) interception through reflections and light leakage (sniffing) which can escalate into spoofing or Man-in-the-Middle (MITM) [10]; 2) jamming (optical interference); 3) spoofing/impersonation of light sources [9]; 4) side channels (e.g. optical emanations) [5].



(a) LoS interception[1] (b) NLoS interception[1] (c) Passive adversary model

Illustration 1. Sniffing attack scenario [11]

In Illustration 1[11], different interception (sniffing) attack scenarios are shown, which can escalate into spoofing or Man-in-the-Middle (MITM) attacks [10]. Alice is the transmitter, Bob is the receiver, and Eve is the attacker. In (a) a scenario of an interception attack is shown where Alice (transmitter) sends data to Bob (receiver) and any other receiver (in this

case Eve - attacker) can receive the signal and intercept the message. The scattering of light caused by surfaces that produce it (scattering) is shown in (b). The attacker is outside the zone covered by the emission from Alice, in a corner of the room or outside it – Eve can in this way receive enough information for interception. In (c) Eve functions as a passive entity and receives the signal without direct interaction with it – such a scenario opens the possibility for attackers not only to intercept traffic, but also to actively interact with the network.

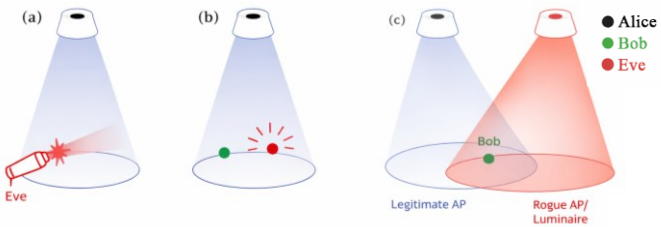
Table 1. Comparative Analysis of Li-Fi Security Standards and Protocols

Item	Year	Standard / Source	Focus	Method	Advantages	Disadvantages	Applicability in Li-Fi
IEEE 802.11bb [12]	2023	IEEE standard	Introduction of Li-Fi into WLAN	802.11 Light Communications	Easier integration with existing WLAN/AAA systems	Security details are not clearly specified in public summaries	High
IEEE 802.15.7 [13]	2018	IEEE standard	Link-layer security in OWC	PHY/MAC for OWC	Basic standard for VLC/Li-Fi systems	Key management is not defined	Medium to high
802.15.7 MAC security [14]	2011/ 2018	IEEE 802.15.7	Confidentiality, integrity, anti-replay	AES-128 CCM*, MIC, frame counter	Multiple security levels, replay protection	Does not protect all headers, key management not defined	High
IEEE 802.1X [15]	2020	IEEE standard	Network access control	Port-based access control	Mature AAA model	Requires additional infrastructure	High
EAP-TLS 1.3 [16]	2022	IETF RFC 9190	Mutual authentication and key exchange	TLS 1.3 over EAP	Strong identity and robust security	Certificates can be large and difficult to deploy	High
TLS 1.3 [17]	2018	IETF RFC 8446	Transport security	TLS 1.3	Standard and strong data protection	Does not address physical attacks on the Li-Fi link	High
EDHOC [18]	2024	IETF RFC 9528	Lightweight authentication for IoT	Compact AKE	Suitable for constrained devices	Requires a compatible IoT ecosystem	High
OSCORE [19]	2019	IETF RFC 8613	End-to-end protection of CoAP messages	COSE-based protection	Protects data even through gateways/proxies	Does not handle network access control	High
EPLSSBJ [20]	2019	IEEE TIFS	Eavesdropping protection	Beamforming + jamming	Improves secrecy performance	Depends on attacker and channel assumptions	High
VL-Watchdog [21]	2022	IEEE IoT Journal	Spoofing attack detection	Redundant coding + monitoring	Practical detection of fake light sources	Increased complexity and additional hardware	High
BGPHA [22]	2023	Optics Communications	Secure handover and authentication	Group authentication + reauthentication + quick rejoin	Reduced latency and fewer interruptions	Focused on a specific scenario	High

Table 2. Classification of Attacks in Li-Fi Systems [11]

Attack Category	Representative Attacks
Physical Attacks	Rogue access point (rogue luminaire), jamming, signal injection, sensor blinding/saturation, light leakage exploitation
Passive Attacks	Snooping, sniffing, eavesdropping, reflection-based interception, traffic analysis
Active Attacks	Man-in-the-Middle (MITM), spoofing, replay attack, frame injection, DoS/DDoS attacks, authentication flooding, deauthentication/disassociation
MAC Layer Attacks	MAC spoofing, beacon spoofing, association hijacking, frame collision exploitation
PHY Layer Attacks	Optical jamming, optical injection, signal distortion, photodetector saturation, interference attacks

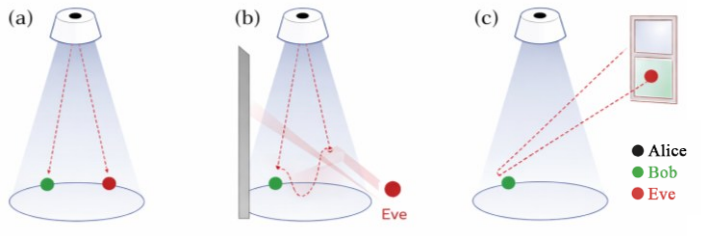
The table systematizes different categories of threats in the Li-Fi environment according to the level at which they operate and the manner in which the attack is carried out. The classification includes physical, passive, and active approaches, as well as attacks directed at specific communication layers.



(a) External optical jamming; (b) In-cell jamming; (c) Rogue luminaire/infrastructure jamming

Illustration 2. Jamming attack scenario

In scenario (a), the attacker Eve is located outside the direct Line-of-Sight (LoS) path, but uses a strong light source (e.g. a laser or a directed LED) toward Bob. Unlike (a), where Eve is outside the LoS, in scenario (b) Eve is located within the same attocell zone as Bob and generates interference using her own device (LED transmitter) with the same or similar modulation, causing an increase in BER (Bit Error Rate) and a drop in SNR (Signal-to-Noise Ratio). Bit Error Rate (BER) directly describes the reliability of data transmission. In its most basic form, BER is defined as the ratio of the number of incorrectly detected bits to the total number of transmitted bits in a communication system. In a Li-Fi system, where high data transmission rates are targeted, BER represents a trade-off between spectral efficiency and reliability. If a low BER is required, it is necessary either to increase SNR by increasing power or applying filtering, or to sacrifice part of the spectral efficiency by using simpler modulation. A high SNR means that the signal power is much greater than the noise power, while a low SNR leads to the signal being comparable to noise, meaning that the receiver has difficulty distinguishing bits, which results in an increase in Bit Error Rate (BER). [1]



(a) LoS snooping; (b) Reflection-based snooping; (c) Light leakage snooping

Illustration 3. Snooping attack scenario

In scenario (a), Eve is located within the illumination cone (LoS) and directly receives the signal that Alice sends to Bob. Eve uses a photodetector to receive the signal and compromises confidentiality without active interaction with the network. Signal scattering (diffuse reflection) shown in (b) reaches Eve who is located outside the LoS zone, reconstructs the signal where the quality is weaker, but still usable. Also, signal scattering occurs due to the reflection of light from surfaces (walls, floor, glass) [1]. In scenario (c), Eve is located outside the physical space (window) and, based on light leakage, intercepts communication without physical access to the space.

III. CIA+AUTH

CIA (confidentiality, integrity, availability) is a practical model for defining the objectives of information security and measuring the consequences of compromise – unauthorized disclosure (C), unauthorized modification (I), and interruption/slowing of service (A). [23] There are at least 3 steps of access control: 1. identification – the user says „who they are"; 2. authentication – the user proves identity; 3. authorization – the system decides what is permitted [24]. Authentication by itself does not guarantee either confidentiality or integrity, but without authentication it is difficult or even impossible to consistently enforce authorization, audit, and accountability. Authentication reduces the probability of unauthorized access to data by making it harder for an attacker to present themselves as an authorized user – session theft, password theft, or a compromised token; it links modifications to identity and enables control of „who changed what," digital signatures (PKI) [23], stronger audit trails, and non-repudiation mechanisms in high-stakes transactions, and it can help in defense against abuse, but it can also threaten availability if it is poorly designed. [25]

A single compromised identity typically leads to: (1) unauthorized reading (C), (2) unauthorized modifications and fraud (I), and (3) operational disruptions (A) through privilege escalation, configuration changes, or locking out legitimate users. Incidents show that even when „production data" does not leak, an attacker can compromise the availability and integrity of internal tools through a compromised account.

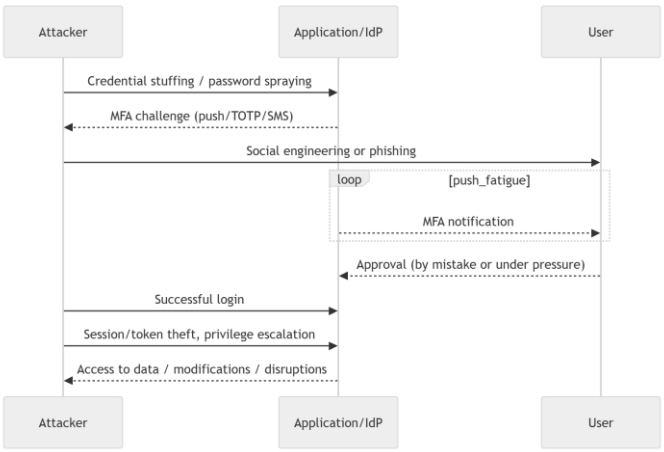


Diagram 1. MFA Bypass Attack

The role-based access control (RBAC) model introduces the idea that access decisions are based on the user's function/role within the organization, whereby users obtain privileges through role assignment (administrator, editor, manager), rather than through ad-hoc access lists per object. Here, privileges are not discretionary „ownership" of the user, but are centrally defined through organizational functions. [26] Unlike RBAC, the attribute-based access control (ABAC) model formalizes authorization as the evaluation of policies over a set of attributes of subjects (users or devices), object attributes, and environmental conditions. According to NIST, it is a method where a subject's request to perform operations on an object is approved or denied based on assigned subject attributes, assigned object attributes, and policies expressed over those attributes. What makes it relevant for Li-Fi are environmental conditions. Environmental conditions in the NIST framework are described as stationary context independent of the subject and object, and can explicitly include current time, user location, and threat state – thereby naturally incorporating decision factors. [27]

There are 2 reasons why ABAC is more practical than RBAC: 1. Li-Fi cells are small and user mobility is expected

[1], so handover is frequent, which makes static policies based only on roles less efficient [4]. In such an environment, authorization that includes conditions such as: „while the user is in zone X / during working hours / under low risk" is more naturally expressed as an ABAC rule than as a multitude of specialized roles. [27] 2. The Li-Fi/VLC ecosystem naturally enables relatively precise contextualization of location [1] [2], and at the same time VLC-based systems can achieve accuracy on the order of 10 cm in controlled conditions [1], which makes „location" a realistic candidate for an attribute in policy.

IV. CONCLUSION

This paper analyzed security in Li-Fi systems, where the context is modern wireless networks, with a particular focus on threats arising from the specific physical and communication characteristics of the optical medium. Although Li-Fi, due to the spatial confinement of the light signal and non-penetration through physical obstacles, has an advantage over conventional RF systems, this is not sufficient. Reflections, light leakage, jamming, spoofing of sources, node compromise, and others confirm the requirement for a comprehensive and cryptography-based network model.

In parallel, the importance of the CIA+Auth model as a basis for defining security requirements in Li-Fi networks was considered, due to characteristics such as the protection of confidentiality, integrity, and availability, which cannot be effective without clearly defined mechanisms of identification, authentication, and authorization, especially in modern Li-Fi systems which, due to user mobility, frequent handover processes, and the need for contextual decision-making, exceed the capabilities of static access control, and in this sense, models such as RBAC and particularly ABAC provide a significant foundation for establishing flexible and precise access management in optical networks.

Future research should be focused on the development of integrated security architectures for Li-Fi systems that would combine physical protection of the optical layer with advanced authentication models and contextual authorization.

REFERENCES

[1] Lj. Stojanović, LI-FI Systems, Master's thesis, Faculty of Computer Science and Informatics, Sinergija University, Bijeljina, Republic of Srpska, 2025, pp. 5, 11, 14-19, 47-49, 50.

[2] Lj. Stojanovic, V. Radojcic, and P. Spalević, *Li-Fi, AI, and IoT Technologies in Creating Sustainable Business*, 2025, pp. 63-64.

[3] Lj. Stojanović, V. Radojčić, S. Mitrović and P. Spalević, Li-Fi Technology for Cybersecurity Solutions + SEON, 2025, pp. 56-58.

[4] H. Haas, L. Yin, C. Chen, S. Videv, D. Parol, E. Poves, H. Alshaer, and M. S. Islim, „Introduction to indoor networking concepts and challenges in LiFi," *Journal of Optical Communications and Networking*, vol. 12, no. 2, 2020, pp. 193-196.

[5] J. Classen, J. Chen, D. Steinmetzer, M. Hollick, and E. W. Knightly, „The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications," in Proc. 2nd Int. Workshop on Visible Light Communication System, Paris, France, Sep. 2015, pp. 11–14.

[6] J. Sanusi, A. Aibinu, S. Adeshina, and S. Idris, „Review of Handover in Li-Fi and Wi-Fi Networks", 2020, pp. 956-960.

[7] X. Wu, M. D. Soltani, L. Zhou, M. Safari, and H. Haas, „Hybrid LiFi and WiFi Networks: A Survey," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, 2021, pp. 1399-1401.

[8] X. Zhang, G. Klevering, X. Lei, Y. Hu, L. Xiao, and G. Tu, „The Security in Optical Wireless Communication: A Survey," *ACM Computing Surveys*, vol. 55, no. 12, 2023, pp. 9.

[9] J. Chen and T. Shu, „VL-Watchdog: Visible Light Spoofing Detection With Redundant Orthogonal Coding," IEEE Internet of Things Journal, vol. 9, no. 13, 2022, pp. 9859-9862.

[10] V. Guerra, J. Rabadan, L. Palmas, and D. G. Canaria, „Data Sniffing Over an Open VLC Channel," in Proc. IEEE Int. Conf. on Consumer Electronics (ICCE), 2012, pp. 1-6.

[11] E. Ramadhani, „A Mini Review of LiFi Technology: Security Issue," International Journal of Computer and Information System (IJCIS), vol. 3, no. 3, 2022, pp. 92.

[12] IEEE, „IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Light Communications," IEEE Std 802.11bb-2023, 2023.

[13] IEEE, „IEEE Standard for Local and Metropolitan Area Networks—Part 15.7: Short-Range Optical Wireless Communications," IEEE Std 802.15.7-2018, 2019.

[14] G. J. Blinowski, „Practical Aspects of Physical and MAC Layer Security in Visible Light Communication Systems," International Journal of Electronics and Telecommunications, vol. 62, no. 1, 2016.

[15] IEEE, „IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control," IEEE Std 802.1X-2020, 2020.

[16] J. Preuß Mattsson and M. Sethi, „EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3," RFC 9190, 2022.

[17] E. Rescorla, „The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, 2018.

[18] G. Selander, J. Preuß Mattsson, and F. Palombini, „Ephemeral Diffie-Hellman Over COSE (EDHOC)," RFC 9528, 2024.

[19] G. Selander, J. Preuß Mattsson, F. Palombini, and L. Seitz, „Object Security for Constrained RESTful Environments (OSCORE)," RFC 8613, 2019.

[20] S. Cho, G. Chen, and J. P. Coon, „Enhancement of Physical Layer Security With Simultaneous Beamforming and Jamming for Visible Light Communication Systems," IEEE Trans. Inf. Forensics Security, vol. 14, no. 10, pp. 2633–2648, 2019.

[21] J. Chen and T. Shu, „VL-Watchdog: Visible Light Spoofing Detection With Redundant Orthogonal Coding," IEEE Internet Things J., vol. 9, no. 12, pp. 9858–9871, 2022

[22] X. Wang, C. Gan, S. Wu, Y. Chen, and Y. Chen, „Bi-group pre-handover authentication model solving signaling congestion of subway LiFi network," Optics Communications, vol. 536, art. no. 129384, 2023.

[23] National Institute of Standards and Technology (NIST), „Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events (Executive Summary)," NIST Special Publication 1800-26A, 2020, pp. 1-3.

[24] CERT, „Višefaktorska autentifikacija," CERT.hr-PUBDOC-2018-12-370, Dec. 2018, pp. 3-10.

[25] OWASP Foundation, „Authentication Cheat Sheet," OWASP Cheat Sheet Series. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[26] D. F. Ferraiolo and D. R. Kuhn, „Role-Based Access Controls," in Proc. 15th National Computer Security Conference (NCSC), Baltimore, MD, USA, 1992, pp. 555–563.

[27] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, „Guide to Attribute Based Access Control (ABAC) Definition and Considerations," NIST Special Publication 800-162, 2014, pp. 5-17.

UDK 004.738.5:[343.983:62-229.316
DOI 10.7251/ZRSNG2526073T

Digitalna forenzika Android infotainment sistema u vozilu VW Golf 6: studija slučaja
Digital Forensics of an Android Infotainment System in a VW Golf 6: A Case Study

Adel Tahirović, Univerzitet Sinergija, Bijeljina

***Sažetak* — U ovom radu predstavljena je studija slučaja digitalne forenzike nad Android infotainment sistemom instaliranim u vozilu VW Golf 6. Digitalni dokazi prikupljeni su pomoću alata Android Debug Bridge (ADB). Zbog ograničenja unutar USB režima rada implementiranih od strane proizvođača, pristup uređaju ostvaren je putem bežičnog (wireless) protokola. Pokušaj integralne akvizicije podataka putem ADB protokola nije rezultirao validnom kopijom sistema, zbog čega se pristupilo selektivnom logičkom izuzimanju aplikacijskih artefakata, uključujući log zapise aplikacije Torque Pro. Pristup podacima ostvaren je putem On-Board Diagnostics (OBD-II) interfejsa, čime je omogućena direktna komunikacija sa elektronskim kontrolnim jedinicama (ECU) vozila preko Controller Area Network (CAN) magistrale. Dodatno su izuzeti podaci globalnog navigacionog satelitskog sistema (GNSS), generisani od strane Android infotainment sistema. Analizom CSV track-log zapisa rekonstruisana je vremenska linija kretanja vozila, procenjena pređena udaljenost i identifikovane faze mirovanja uz evaluaciju kvaliteta GNSS signala Horizontal Dilution of Precision (HDOP). Analiza potvrđuje da parcijalni artefakti Android infotainment sistema mogu imati značajnu dokaznu vrednost u rekonstrukciji događaja, uz jasno dokumentovana ograničenja akvizicije.**

Ključne reči – digitalna forenzika; Android infotainment sistem; Android Debug Bridge (ADB); GNSS podaci; OBD-II/CAN komunikacija;

***Abstract* – This paper presents a digital forensic case study conducted on an Android-based infotainment system installed in a VW Golf 6 vehicle. Digital evidence was collected using the Android Debug Bridge (ADB) tool. Due to USB debugging restrictions implemented by the manufacturer, access to the device was gained through the wireless debugging method. A full ADB backup did not yield a usable copy of the data; therefore, a targeted logical extraction of available application artifacts was performed, including log records generated by the Torque Pro application. The analyzed logs contained data collected through OBD-II communication with the vehicle's ECU (CAN bus), as well as GNSS location data generated by the Android infotainment system. By analyzing CSV track log records, a timeline of the vehicle's movement was reconstructed, the traveled distance was estimated, and stationary phases were identified, along with an evaluation of GNSS signal quality (HDOP). The results demonstrate that even partially available artifacts from Android infotainment systems can have significant evidential value in reconstructing events, provided that the limitations of the acquisition process are clearly documented.**

***Keywords* – digital forensics; Android infotainment system; Android Debug Bridge (ADB); OBD-II/CAN communication; GNSS data**

I. UVOD

Savremena vozila integrišu veliki broj elektronskih kontrolnih jedinica, senzora i infotainment sistema koji generišu i pohranjuju podatke ključne za rekonstrukciju saobraćajnih nezgoda i izradu istražnih vremenskih linija [19]. Automobilska digitalna forenzika definiše se kao proces pronalaženja, izdvajanja i interpretacije podataka iz modula vozila, mrežne komunikacije poput Controller Area Network (CAN) poruka i drugih ugrađenih sistema [16].

Budući da su infotainment sistemi danas standardni deo opreme, njihov značaj kao izvora dokaza postaje sve veći. Najčešće su to sistemi zasnovani na Android platformi, koji omogućavaju uvid u kretanje vozila, multimedijalni sadržaj i mrežnu povezanost [8]. Dosadašnja saznanja ukazuju na to da se istraživanja sve više usmeravaju na ove sisteme, ali se često zanemaruju praktična ograničenja prikupljanja podataka kada je konekcija putem USB veze na uređaju tvornički onemogućena [10]. Prethodno poznavanje forenzike mobilnih uređaja pruža osnovu, ali specifični hardverski restriktivni protokoli proizvođača automobila zahtevaju prilagođen pristup.

U ovoj studiji slučaja istraživao sam mogućnosti razvoja ponovljivog istraživačkog pristupa koji obuhvata:

(a) prikupljanje digitalnih dokaza sa Android infotainment sistema u uslovima ograničene konektivnosti, te

(b) kvantitativnu analizu Torque Pro log datoteka generisanih putem On-Board Diagnostics (OBD-II) komunikacije.

Fokusirao sam se na postupke provere integriteta podataka i dokumentovanje procesa akvizicije, nastojeći da jasno definišem metodološka ograničenja u skladu sa standardima rukovanja digitalnim dokazima [2].

II. TEORIJSKI OKVIR

Komunikacija između elektronskih sistema vozila najčešće se ostvaruje putem CAN magistrale, koja predstavlja standardizovanu tehnologiju za razmenu podataka unutar vozila definisanu standardom ISO 11898-1 [18]. CAN okvir sadrži identifikator poruke koji određuje prioritet komunikacije i pristup magistrali, što je od značaja i za inženjersku analizu i za forenzičku interpretaciju mrežnog saobraćaja [18].

Pristup dijagnostičkim podacima vozila ostvaruje se putem standardizovanog OBD-II 16-pinskog konektora, poznatog kao Data Link Connector (J1962 DLC).

Na ovom konektoru dostupne su različite komunikacione linije, uključujući CAN High i CAN Low, koje omogućavaju komunikaciju sa Electronic Control Unit (ECU) modulima vozila [17].

U praksi se za komunikaciju sa vozilom najčešće koriste OBD-II adapteri zasnovani na ELM327 arhitekturi, koji funkcionišu kao protokolarni prevodioci između mobilnih aplikacija i elektronskih sistema vozila [17]. Na aplikacionom nivou, podaci su adresirani preko standardizovanih OBD-II PID identifikatora definisanih standardom SAE J1979, koji omogućavaju pretvaranje sirovih bajtova odgovora iz ECU modula u fizičke veličine. Tipični primeri u forenzičkoj analizi su PID 0C (broj obrtaja motora), gde se vrednost dobija izrazom (1), i PID 0D (brzina vozila), definisan izrazom (2) [17]. Standardni PID primeri:

PID 0C (Engine RPM):

$$RPM = \frac{256A + B}{4} \quad (1)$$

Objašnjenje:

Ovaj izraz se koristi za interpretaciju odgovora na PID 0C. ECU vozila vraća dva bajta podataka, označena kao **A** (viši bajt) i **B** (niži bajt). Množenjem bajta A sa 256 vrši se pomeranje u 16-bitnom prostoru, dok se deljenjem sa 4 postiže rezolucija od 0,25 o/min, što je standard za OBD-II protokol [17]. U analiziranoj log-datoteci, ovaj parametar služi kao potvrda rada motora sa unutrašnjim sagorevanjem tokom zabeleženih Global Navigation Satellite System (GNSS) koordinata.

PID 0D (Vehicle speed):

$$\left[v_{\{OBD\}}\left(\frac{km}{h}\right) = A \right] \quad (2)$$

Objašnjenje:

Brzina vozila se dobija iz PID-a 0D. Za razliku od broja obrtaja motora (RPM), ovde se koristi samo jedan bajt (**A**), što znači da je maksimalna vrednost koju protokol može prijaviti 255 km/h. Važno je napomenuti da ova vrednost potiče direktno sa senzora na menjaču ili ABS prstenova točkova vozila VW Golf 6, te predstavlja 'unutrašnju' brzinu vozila koja može odstupati od 'spoljašnje' GNSS brzine usled faktora kao što su veličina pneumatika ili proklizavanje [20].

Za ekstrakciju podataka iz Android baziranih infotainment sistema koristi se Android Debug Bridge (ADB) protokol. ADB funkcioniše kao klijent-server arhitektura koja se sastoji od klijenta (forenzička radna stanica), servera i pozadinskog procesa (daemon) koji se izvršava na samom uređaju [21]. U kontekstu digitalne forenzike, ADB omogućava logičku akviziciju podataka putem komandne linije, čime se ostvaruje interakcija sa fajl-sistemom bez potrebe za modifikacijom hardvera [22].

Standardi digitalne forenzike naglašavaju potrebu očuvanja integriteta, revizionog traga i reproduktibilnosti postupaka [2]. Standard ISO/IEC 27037 definiše procese identifikacije, prikupljanja i očuvanja digitalnih dokaza, dok smernice organizacija poput NIST-a i SWGDE naglašavaju minimalnu izmenu originalnih podataka i detaljno dokumentovanje procesa analize [3].

III. MATERIJALI I METODE

Predmet istraživanja bio je Android infotainment sistem instaliran u vozilu VW Golf 6 čije su detaljne tehničke specifikacije i forenzički parametri prikazani u tabeli 1. Cilj analize bio je utvrditi da li je moguće rekonstruisati vremensku liniju kretanja vozila na osnovu aplikacionih artefakata generisanih tokom vožnje [10].

Podaci su generisani koristeći aplikaciju Torque Pro, koja je bila povezana sa vozilom putem ELM327 OBD-II adaptera [1]. Radi očuvanja integriteta podataka izračunate su Secure Hash Algorithm 256-bit (SHA-256) kriptografske hash vrednosti za sve izdvojene digitalne artefakte, prikazane u tabeli 2 [2].

Inicijalni pokušaji direktnog fizičkog povezivanja putem USB režima rada nisu dali rezultate usled restriktivnih sigurnosnih polisa proizvođača. Razmatrana je i metoda fizičke ekstrakcije podataka direktno sa memorijskog čipa (*chip-off*), ali je ona odbačena zbog rizika od trajnog uništenja hardvera i narušavanja integriteta sistema u ovoj fazi istrage. Shodno tome, kao primarna metoda za akviziju podataka odabrano je bežično (wireless) povezivanje. U forenzičkom kontekstu, ovakav pristup se klasifikuje kao udaljena logička akvizicija (eng. remote logical acquisition), jer kanal pristupa nije neposredni fizički medij, već mrežna infrastruktura koja zahteva uparivanje i autorizaciju [11]. Bilo je neophodno detaljno dokumentovati svaki korak uspostavljanja veze uključujući, mrežni interfejs, logički identitet radne stanice i tačno vreme svake akcije kako bi se osigurao potpun revizioni trag i minimizovao rizik od nenamernih izmena na uređaju.

TABELA 1. TEHNIČKI I FORENZIČKI KONTEKST ANALIZIRANOG UREĐAJA

Parametar	Vrednost
Vozilo	VW Golf 6
Tip uređaja	Android infotainment sistem u vozilu
Operativni sistem	Android 11
Build verzija	V1.07.10-20250629
Način pristupa	Wireless debugging (ADB)
Root pristup	Nije dostupan
USB ADB pristup	Ograničen / nije omogućio potpunu akviziciju
Pokušaj ADB full backup-a	Izvršen, ali nije dao upotrebljiv rezultat
Tip akvizicije	Ciljano logičko izdvajanje podataka
Relevantna aplikacija	Torque Pro ver. 1.12.108
Korišćeni adapter	ELM327 ver. 1.5
Izvor analiziranih podataka	OBD-II/CAN komunikacija i GNSS zapisi aplikacije
Izdvojeni artefakti	CSV log, bugreport/dumpstate, ADB backup artefakt

Dokazni paket je sadržao: (1) Torque Pro export u ZIP formatu, (2) CSV track log kao primarni analitički artefakt, (3) sistemski dijagnostički izveštaj (bugreport/dumpsys), te (4) ADB full_backup artefakt koji je ukazivao na neuspešan pokušaj potpunog izvlačenja sigurnosne kopije iz uređaja.

TABELA 2. DIGITALNI ARTEFAKTI I SHA-256 VREDNOSTI ZA PROVERU INTEGRITETA

Artefakt	Veličina (bytes)	SHA-256
dumpsys_detalji.txt	13859517 bytes	34a30c6237bfe28972b93859db82ceb78bda3adf48be2d907da931ce173a5cd
trackLog-2026-Mar-02_19-30-20.csv	713614 bytes	a70c149bcd347b96046042735f49fb77f87329a3b0d2754abb3f90c99edc543
zipExport-2026-03-02_19-38-48.zip	43509 bytes	7975c754c0fbba980d404ca5aa597be2a00a3b848cb22a3309ba213744ae4c9f
full_backup.ab	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Izračunavanje kriptografskih hash vrednosti predstavlja standardnu proceduru u digitalnoj forenzici, jer omogućava verifikaciju integriteta digitalnih dokaza između faze akvizicije i faze analize. Ukoliko se hash vrednost artefakta promeni, to ukazuje na potencijalnu izmenu podataka.

IV. REZULTATI

Analiza izdvojene datoteke trackLog.csv rezultovala je identifikacijom preko 90 različitih dijagnostičkih, lokacionih i sistemskih parametara koji su beleženi u realnom vremenu. Za potrebe forenzičke rekonstrukcije događaja, iz bogatog skupa podataka izvršena je ciljana selekcija varijabli koje omogućavaju precizno mapiranje kretanja i stanja vozila:

Vremensko-lokacioni parametri: GPS Time, Latitude i Longitude poslužili su kao osnova za hronološko mapiranje kretanja.

Dijagnostički parametri vozila (OBD-II): Engine RPM (broj obrtaja) i Speed (OBD) odabrani su kao primarni indikatori rada motora i mehaničkog kretanja vozila, dok su parametri poput *Throttle Position* (položaj pedale gasa) korišćeni za analizu ponašanja vozača.

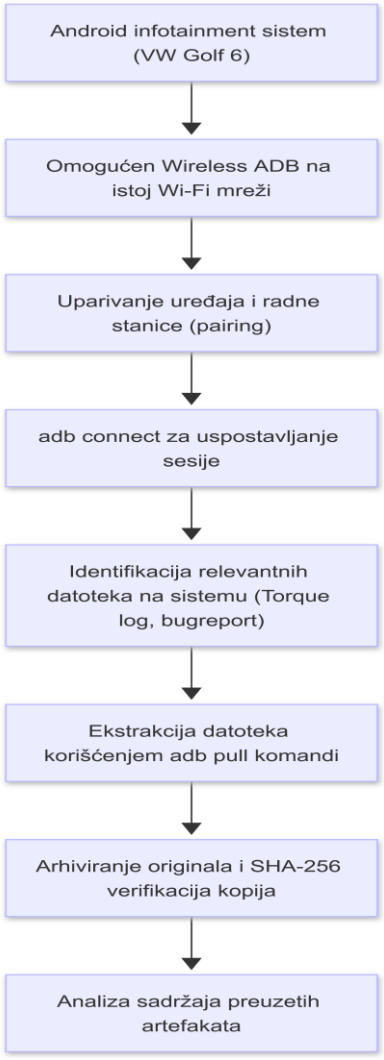
Metapodaci validacije: Horizontal Dilution of Precision (HDOP) i GPS Satellites ekstrahovani su radi evaluacije pouzdanosti lokacionih podataka, što je ključno za forenzičku verifikaciju preciznosti zapisa.

Klasifikacija ovih podataka omogućila je formiranje korelacionog modela između unutrašnjih senzora vozila i eksternih GNSS podataka, čime je potvrđen integritet celokupne vožnje. Tabela 3 prikazuje pregled ključnih ADB naredbi korišćenih tokom postupka akvizicije digitalnih artefakata sa Android infotainment sistema.

TABELA 3. PREGLED KLJUČNIH ADB NAREDBI KORIŠĆENIH U PROCESU AKVIZICIJE PODATAKA

ADB naredba	Opis operacije	Svrha u forenzičkom procesu
adb pair 192.168.1.15:37445 842931	Uparivanje uređaja sa radnom stanicom	Autentifikacija i dozvola pristupa sistemu
adb connect 192.168.1.15:41029	Uspostavljanje aktivne mrežne sesije	Kreiranje kanala za prenos digitalnih dokaza
adb shell bugreport > b.zip	Generisanje sveobuhvatnog izveštaja	Ekstrakcija sistemskih log datoteka i dijagnostike

Celokupan operativni postupak akvizicije strukturiran je kao forenzički tok obrade dokaza, koji je precizno definisan i vizuelno predstavljen na slici 1.



Sl.1 Dijagram toka procesa bežične akvizicije podataka sa Android infotainment sistema

Primenjeni model sa slike 1 podrazumeva identifikaciju relevantnih izvora podataka (dnevnički zapisi aplikacija, datoteke izvoza podataka, privremene datoteke) i njihovo

izdvajanje uz minimalnu izmenu originalnog sadržaja [2]. Proces obuhvata sledeće ključne faze:

1. identifikaciju relevantnih digitalnih artefakata.
2. izradu forenzičke kopije dostupnih podataka.
3. izračunavanje kriptografskih hash vrednosti radi provere integriteta.
4. očuvanje originalnih datoteka u read-only režimu.
5. analizu podataka nad verifikovanim kopijama artefakata.

Ovakav pristup je u potpunosti u skladu sa preporukama standarda ISO/IEC 27037 i smernicama organizacije SWGDE za rukovanje digitalnim dokazima [2].

V. ANALIZA I TUMAČENJE IZDVOJENIH ARTEFAKATA

Analiza je bila usmerena na rekonstrukciju kretanja vozila na osnovu podataka track log zapisa aplikacije Torque Pro. Skup podataka je sadržavao 1513 uzoraka u vremenskom periodu od približno 45 minuta i 29 sekundi. Prosečni interval uzorkovanja bio je oko jedne sekunde. Ovakav način uzorkovanja je u skladu sa tipičnim načinom rada aplikacija za praćenje vožnje, gde se podaci beleže u kratkim vremenskim intervalima, ali može doći do povremenih prekida usled gubitka GNSS signala ili promena stanja aplikacije [20].

Za procenu udaljenosti između uzastopnih GNSS koordinata korišćena je haversine formula definisana jednačinom (4), koja omogućava izračunavanje udaljenosti između dve tačke na površini Zemlje na osnovu njihove geografske širine i dužine [20]. Pošto GNSS koordinatni zapisi koriste vrednosti izražene u stepenima, neophodno je izvršiti njihovu konverziju u radijane prema jednačini (3).

Jednačina za pretvaranje stepeni u radijane:

$$\varphi_{(\text{rad})} = \varphi_{(\text{deg})} \cdot \frac{\pi}{180} \qquad (3)$$

Jednačina za izračunavanje udaljenosti između dve GNSS tačke definisana je sledećim izrazom:

$$d = 2R\ arcsin\left(\sqrt{sin^{2\left(\frac{\Delta\varphi}{2}\right)} + cos(\varphi_1)cos(\varphi_2)sin^{2\left(\frac{\Delta\lambda}{2}\right)}}\right) \qquad (4)$$

gde su:

- **R** – radijus Zemlje (približno 6371 km)
- **φ_1 i φ_2** – geografske širine dve GNSS tačke
- **λ_1 i λ_2** – geografske dužine dve GNSS tačke
- **$\Delta\varphi$** – razlika geografskih širina između dve tačke
- **$\Delta\lambda$** – razlika geografskih dužina između dve tačke
- **d** – udaljenost između dve GNSS pozicije.

Na osnovu izračunate udaljenosti između uzastopnih GNSS koordinata i vremenskog intervala između uzoraka moguće je proceniti trenutnu brzinu kretanja vozila [20]. Procena brzine može se izračunati pomoću sledeće jednačine (5):

$$v = \frac{\Delta d}{\Delta t} = \frac{(d_2 - d_1)}{t_2 - t_1} \qquad (5)$$

gde je:

- **v** – procenjena brzina kretanja vozila
- **Δd**– udaljenost između dve uzastopne GNSS pozicije
- **Δt** – vremenski interval između dva uzorka.

S obzirom na to da su sirovi podaci u log-datoteci aplikacije Torque Pro za parametar GPS Speed izraženi u metrima po sekundi (m/s), izvršena je konverzija u kilometre na čas (km/h) primenom sledeće jednačine (6):

$$v_{\frac{km}{h}} = v_{\frac{m}{s}} \cdot 3{,}6 \qquad (6)$$

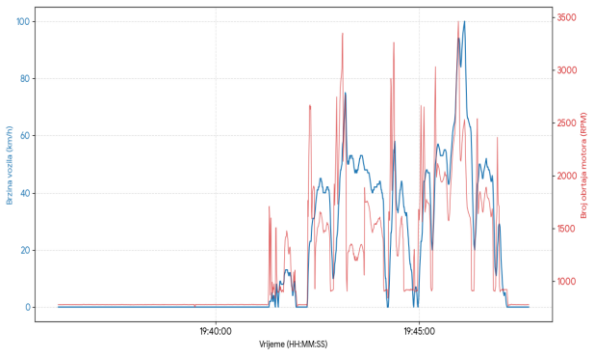
Ova transformacija je neophodna radi standardizacije prikaza rezultata i lakše korelacije sa brzinom očitane putem OBD-II interfejsa vozila [17]. Primenom navedenog matematičkog modela nad verifikovanim skupom podataka, dobijeni su sledeći rezultati kretanja:

- ukupna pređena udaljenost: 14,39 km
- prosečna brzina vozila: 26,95 km/h
- maksimalna zabeležena brzina: 64,12 km/h

Analiza distribucije brzine pokazala je da je približno 20,36% uzoraka imalo vrednost manju od 1 km/h, što ukazuje na faze mirovanja (stajanje na semaforima, raskrsnicama ili parkiranje).

A. Forenzička korelacija i validacija podataka

Ključni aspekt analize artefakata je potvrda autentičnosti zapisa korelacijom različitih senzora. U digitalnoj forenzici vozila, podudaranje rada motora sa kinetikom vozila služi kao dokaz da podaci nisu naknadno manipulisani ili generisani greškom softvera.

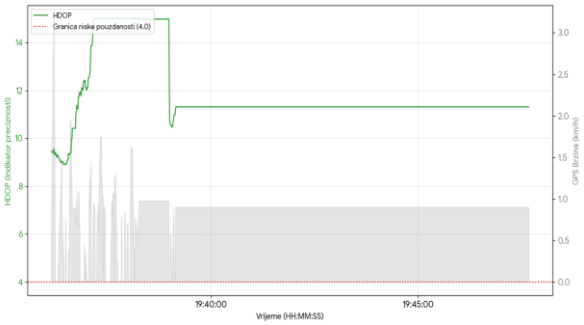


Sl.2 Korelacija brzine kretanja vozila (OBD) i broja obrtaja motora (RPM)

Podaci na slici 2 pokazuju visoku koherentnost: svaki porast broja obrtaja motora (RPM) korelira sa promenom brzine očitane preko OBD-II interfejsa. Ovakva podudarnost potvrđuje da je Android infotainment sistem ispravno procesuirao podatke dobijene putem aplikacije i ELM327 adaptera sa CAN magistrale vozila u realnom vremenu [18].

B. *Analiza pouzdanosti GNSS signala*

Pored kinetičkih parametara, analiziran je i Horizontal Dilution of Precision (HDOP) parametar kao primarni indikator kvaliteta geolokacijskih podataka. Niže vrednosti HDOP-a ukazuju na bolju geometriju satelita i veću preciznost, dok visoke vrednosti sugerišu povećanu marginu greške.



Sl.3 Analiza pouzdanosti GNSS signala (HDOP) i brzine kretanja

U analiziranom skupu podataka, HDOP vrednosti su varirale između 1,7 i 15. Kao što je prikazano na slici 3, određeni segmenti vožnje karakterišu se HDOP vrednostima iznad kritične granice od 4,0, što ukazuje na periode smanjene forenzičke pouzdanosti. Ovi ekstremi su verovatno uzrokovani ambijentalnim faktorima poput urbanih kanjona ili drvoreda koji ometaju direktnu vidljivost GNSS satelita.

C. *Analiza strukture ekstrahovanih podataka*

Detaljnim pregledom ekstrahovane datoteke utvrđeno je da sistem beleži preko 30 senzorskih parametara. Za potrebe istraživanja, kao primarni markeri izdvojeni su: GPS Time, Latitude, Longitude, GPS Speed, HDOP i Engine RPM. Posebna pažnja posvećena je koloni Device Time. Njeno prisustvo omogućava forenzičku proveru eventualnog odstupanja između sistemskog sata Android infotainment sistema i atomskog vremena dobivenog putem GNSS-a. U analiziranim uzorcima uočena je potpuna sinhronizacija, što olakšava precizno smeštanje događaja u vremensku liniju istrage.

Na osnovu rezultata možemo potvrditi da, uprkos ograničenjima poput povremenih prekida u zapisu ili varijabilne preciznosti signala, artefakti iz Android infotainment sistema predstavljaju robustan izvor dokaza [10]. Za maksimalnu naučnu sigurnost, preporučuje se da se ovi podaci uvek interpretiraju uz uvažavanje HDOP indikatora i, gde je moguće, potvrde eksternim izvorima poput ECU log datoteka ili telemetrije.

VI. DISKUSIJA

Rezultati studije slučaja potvrđuju da Android infotainment sistemi predstavljaju izuzetno relevantan izvor digitalnih dokaza u automobilskim istragama, naročito kada se zahteva precizna rekonstrukcija vremenske linije kretanja, analiza obrasca brzine i identifikacija faza mirovanja vozila [10]. Temeljni dokazni materijal u ovom istraživanju zasnovan je na log-datoteci aplikacije Torque Pro, pomoću koje je izvršena detaljna kvantitativna rekonstrukcija kretanja u trajanju od oko 45 minuta. Takav tip artefakta je praktično vredan jer se često može pribaviti i u uslovima kada je potpuna fizička akvizicija ograničena ili tehnički neizvodiva [11].

Ipak, interpretacija zapisa zasnovanih na GNSS tehnologiji mora ostati forenzički konzervativna [20]. Prvo, kvalitet GNSS signala varira u zavisnosti od okruženja (urbani kanjoni, tuneli, drvoredi), što može dovesti do povećanih grešaka pozicioniranja [20]. Zbog toga je parametar HDOP ključan indikator nesigurnosti: niže vrednosti tipično impliciraju bolju geometriju satelita i manju horizontalnu grešku, dok više vrednosti ukazuju na slabiju pouzdanost lokacijskog podatka [20]. U kontekstu digitalne forenzike, to znači da se segmenti sa povećanim HDOP vrednostima ne bi smeli koristiti za precizne tvrdnje o apsolutnoj lokaciji bez dodatne potvrde, već prvenstveno za prepoznavanje opšteg obrasca kretanja [2].

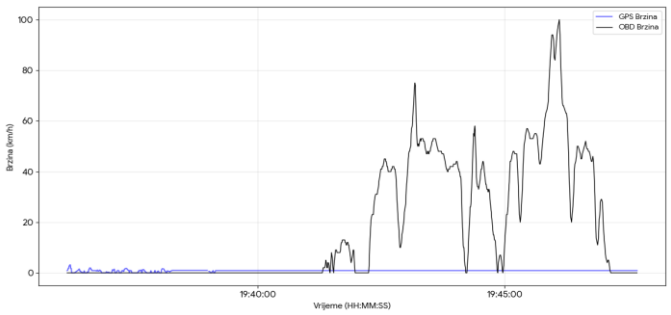
Drugo, prisutni prekidi u logovanju (time gaps) uvode rizik da kumulativna udaljenost izračunata haversine formulom potceni realnu pređenu udaljenost, jer se preskaču segmenti između dve zabeležene tačke. Iz tog razloga, preporučuje se da se prekidi eksplicitno označe u rezultatima (npr. broj prekida dužih od 10 s i maksimalna pauza), te da se u diskusiji naglasi da su takvi intervali empirijski „nepoznati“, a ne interpolirani [2].

Treće, ključni doprinos rada je detaljno dokumentovanje ograničenja akvizicije: USB komunikacija je bila onemogućena od strane proizvođača, pa je pristup ostvaren putem metode bežičnog debugovanja (wireless debugging), dok je pokušaj kreiranja potpune ADB sigurnosne kopije sistema rezultovao praznom datotekom. Takva ograničenja su tipična za savremene infotainment sisteme, gde proizvođači primenjuju ograničenja pristupa sistemskim interfejsima, a novije verzije Android operativnog sistema dodatno ograničavaju generičke mehanizme sigurnosne kopije [10]. Iz forenzičke perspektive, to zahteva jasnu distinkciju između:

(a) podataka koji su bili dokazno dostupni i analizirani i

(b) podataka koji bi potencijalno postojali, ali nisu mogli biti prikupljeni u datim uslovima.

U dobroj praksi, ova distinkcija se jasno navodi u metodologiji i diskusiji, kako bi zaključci bili zasnovani isključivo na stvarno prikupljenim i verifikovanim artefaktima. Preporučuje se metodološka triangulacija izvora podataka gde god je moguća: korelacija dnevničkih zapisa infotainment sistema sa nezavisnim izvorima kao što su ECU log datoteke ili drugim vremenski sinhronizovanim izvorima lokacijskih podataka [3].



Sl.4 Komparativna analiza GPS i OBD brzine vozila (Validacija podataka)

Takva korelacija, prikazana na slici 4, može dodatno ojačati dokaznu vrednost istraživanja i značajno smanjiti nesigurnost, posebno u segmentima sa slabijim GNSS kvalitetom ili prekidima u evidentiranju podataka [2].

VII. ZAKLJUČAK

Ovaj rad predstavlja studiju slučaja digitalne forenzike nad Android infotainment sistemom instaliranim u vozilu VW Golf 6. Sa primarnim fokusom na metodologiju izdvajanja i analize podataka, istraživanje je pokazalo da savremena vozila predstavljaju kompleksne digitalne ekosisteme čiji artefakti mogu biti od presudnog značaja za forenzičku rekonstrukciju događaja.

Zbog implementiranih ograničenja USB ADB komunikacije i neuspešnog pokušaja kreiranja potpunog backup-a (potpune sigurnosne kopije) uređaja, proces akvizicije uspešno se oslonio na metodu bežičnog debugovanja (Wireless debugging) i ciljano logičko izvlačenje aplikacionih artefakata. Analizom dnevničkih zapisa (track log) aplikacije Torque Pro, precizno je rekonstruisana vremenska linija kretanja vozila u trajanju od približno 45 minuta, uz procenu pređene udaljenosti od 14,39 km i jasnu identifikaciju perioda mirovanja.

Korelacija dobijenih rezultata putem komparativne analize brzine i broja obrtaja motora potvrdila je integritet i autentičnost izuzetih digitalnih dokaza. Rezultati istraživanja nedvosmisleno potvrđuju da Android infotainment sistemi predstavljaju vredan izvor podataka u automobilskim istragama, čak i u scenarijima u kojima je dostupna samo parcijalna akvizicija. Ključ uspešne forenzičke obrade leži u preciznom dokumentovanju procesa, verifikaciji integriteta putem kriptografskih hash vrednosti i kritičkom uvažavanju ograničenja preciznosti GNSS signala.

Buduća istraživanja trebalo bi da se usmere na automatizaciju korelacije između artefakata dobijenih iz Android infotainment i podataka iz drugih elektronskih kontrolnih jedinica vozila (ECU) radi postizanja još većeg stepena forenzičke sigurnosti.

LITERATURA

[1] A. Årnes, Ed., *Digital Forensics: An Academic Introduction*. Hoboken, NJ: Wiley, 2018.

[2] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. Waltham, MA: Academic Press, 2011.

[3] E. Casey, *Handbook of Digital Forensics and Investigation*. Burlington, MA: Academic Press, 2009.

[4] J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*, 2nd ed. Waltham, MA: Syngress/Morgan Kaufmann, 2015.

[5] B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*, 6th ed. Boston, MA: Cengage, 2019.

[6] N. A. Hassan, *Digital Forensics Basics: A Practical Guide Using Windows OS*. Berkeley, CA: Apress, 2019.

[7] B. Carrier, *File System Forensic Analysis*. Boston, MA: Addison-Wesley Professional, 2005.

[8] A. Hoog, *Android Forensics: Investigation, Analysis, and Mobile Security for Google Android*. Waltham, MA: Syngress, 2011.

[9] O. Skulkin, D. Tindall, and R. Tamma, *Learning Android Forensics*, 2nd ed. Birmingham, U.K.: Packt Publishing, 2018.

[10] R. Tamma, O. Skulkin, H. Mahalik, and S. Bommisetty, *Practical Mobile Forensics: Forensically Investigate and Analyze iOS, Android, and Windows 10 Devices*, 4th ed. Birmingham, U.K.: Packt Publishing, 2020.

[11] L. Reiber, *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*, 2nd ed. New York, NY: McGraw-Hill Education, 2019.

[12] C. Easttom, *An In-Depth Guide to Mobile Device Forensics*. Boca Raton, FL: CRC Press, 2022.

[13] J. Bair, *Seeking the Truth from Mobile Evidence: Basic Fundamentals, Intermediate and Advanced Overview of Current Mobile Forensic Investigations*. Cambridge, MA: Academic Press, 2017.

[14] I. I. Androulidakis, *Mobile Phone Security and Forensics: A Practical Approach*, 2nd ed. Cham: Springer, 2016.

[15] A. Gehlot, R. Singh, J. Singh, and N. R. Sharma, Eds., *Digital Forensics and Internet of Things: Impact and Challenges*. Hoboken, NJ: Wiley, 2022.

[16] S. Kim and R. Shrestha, *Automotive Cyber Security: Introduction, Challenges, and Standardization*. Singapore: Springer, 2020.

[17] C. Smith, *The Car Hacker's Handbook: A Guide for the Penetration Tester*. San Francisco, CA: No Starch Press, 2016.

[18] W. Lawrenz, Ed., *CAN System Engineering: From Theory to Practical Applications*, 2nd ed. London: Springer, 2013.

[19] D. P. F. Möller and R. E. Haas, *Guide to Automotive Connectivity and Cybersecurity: Trends, Technologies, Innovations and Applications*. Cham: Springer, 2019.

[20] E. D. Kaplan and C. Hegarty, Eds., *Understanding GPS/GNSS: Principles and Applications*, 3rd ed. Norwood, MA: Artech House, 2017

UDK 658.8:502.131.1]:339.13(4-672EU)
DOI 10.7251/ZRSNG2526079M

Zelena tranzicija Evropske Unije i izvozni potencijal Bosne i Hercegovine: Sektorska analiza izloženosti i rizika

The Green Transition of the European Union and the Export Potential of Bosnia and Herzegovina: A Sectoral Analysis of Exposure and Risks

Luka Marković, Petar Marković, Ekonomski fakultet Pale, Univerzitet u Istočnom Sarajevu
Marinko Marković, JU SŠC „Ivo Andrić“ Višegrad

Sažetak **— Zelena tranzicija Evropske unije i uvođenje Mehanizma za prekogranično prilagođavanje ugljenika (CBAM) značajno mijenjaju regulatorni okvir međunarodne trgovine, posebno za zemlje čija se izvozna struktura oslanja na energetski intenzivne industrije. Cilj ovog rada je analiza sektorske izloženosti Bosne i Hercegovine efektima zelene tranzicije EU, sa fokusom na sektore sa visokim intenzitetom emisija CO2 i izvoz prema tržištu Evropske unije. Istraživanje je zasnovano na deskriptivno-komparativnoj analizi podataka o spoljnotrgovinskoj razmjeni Bosne i Hercegovine u periodu 2015–2024. godine, uz primjenu indikatora sektorske izloženosti CBAM mehanizmu (ICBAM). Rezultati ukazuju na visoku geografsku koncentraciju izvoza prema Evropskoj uniji, koja prelazi 70% ukupnog izvoza, kao i značajan udio sektora sa visokim intenzitetom emisija CO2 u izvoznoj strukturi. Vrijednost indikatora izloženosti ostala je relativno stabilna tokom posmatranog perioda, što upućuje na spor proces strukturne transformacije industrije uprkos rastu ukupnog izvoza. Nalazi potvrđuju postojanje dvostruke ranjivosti privrede Bosne i Hercegovine — sektorske i geografske — dok CBAM kratkoročno predstavlja konkurentski izazov, ali dugoročno može djelovati kao podsticaj energetskoj tranziciji i modernizaciji industrije.**

Ključne riječi **— zelena tranzicija, CBAM, izvozna struktura, Bosna i Hercegovina, Evropska unija.**
JEL klasifikacija: F18, Q48, Q54, Q14

Abstract — The European Union’s green transition and the introduction of the Carbon Border Adjustment Mechanism (CBAM) significantly reshape the regulatory framework of international trade, particularly for countries whose export structures rely on energy-intensive industries. The aim of this paper is to analyse the sectoral exposure of Bosnia and Herzegovina to the effects of the EU green transition, with a particular focus on high carbon-emission sectors and exports to the European Union market. The research is based on a descriptive and comparative analysis of Bosnia and Herzegovina’s foreign trade data for the period 2015–2024, applying an indicator of sectoral exposure to the CBAM mechanism (ICBAM). The results indicate a high geographical concentration of exports toward the European Union, exceeding 70% of total exports, as well as a significant share of carbon-intensive sectors within the export structure. The exposure indicator remained relatively stable during the observed period, suggesting a slow process of industrial structural transformation despite overall export growth. The findings confirm the existence of a dual vulnerability of the economy of Bosnia and Herzegovina — sectoral and geographical — while CBAM represents a short-term competitiveness challenge but may, in the long run, act as an incentive for energy transition and industrial modernization.

Keywords **— green transition, CBAM, export structure, Bosnia and Herzegovina, European Union.**
JEL Classification**: F18, Q48, Q54, Q14.**

I. UVOD

Regulatorni i razvojni kontekst zelene tranzicije Evropske unije

Zelena tranzicija Evropske unije (EU) predstavlja jednu od najambicioznijih strukturnih transformacija savremene globalne ekonomije. Usvajanjem Evropskog zelenog plana 2019. godine, EU je postavila cilj postizanja klimatske neutralnosti do 2050. godine, uz smanjenje neto emisija gasova sa efektom staklene bašte za najmanje 55% do 2030. godine u odnosu na nivo iz 1990. godine [12], [14]. Evropski zeleni plan i paket „Fit for 55“ institucionalizuju klimatsku politiku EU kroz reformu sistema trgovine emisijama i uvođenje CBAM mehanizma, koji je ušao u tranzicionu fazu primjene 2023. godine [15]. CBAM ima za cilj sprječavanje „curenja ugljenika“, ali istovremeno mijenja uslove pristupa tržištu EU za trgovinske partnere, uvodeći regulatorni trošak proporcionalan ugljeničnom intenzitetu proizvodnje. Ovakva regulatorna

transformacija ima direktne implikacije za zemlje Zapadnog Balkana, čije su ekonomije snažno integrisane sa tržištem EU. Kao odgovor na potrebu usklađivanja sa klimatskim i energetskim standardima EU, 2020. godine usvojena je Zelena agenda za Zapadni Balkan, kao regionalni okvir za implementaciju principa Evropskog zelenog plana [13].

Međutim, strukturni izazovi regiona ostaju izraženi. Prema [42], ugljenični intenzitet ekonomija Zapadnog Balkana, uključujući Bosnu i Hercegovinu, višestruko je veći od prosjeka EU. Energetski sistemi i dalje su dominantno zasnovani na uglju, uz nisku energetsku efikasnost i zastarjelu infrastrukturu. [26] naglašavaju da dekarbonizacija regiona zahtijeva dubinsku transformaciju energetskog miksa i značajne investicione kapacitete, dok [22] ukazuju na ograničene fiskalne i institucionalne resurse za sprovođenje tranzicije. U tom kontekstu, Bosna i Hercegovina predstavlja paradigmatičan slučaj strukturne izloženosti. Elektroenergetski sektor BiH i dalje se dominantno oslanja na termoelektrane na ugalj, koje učestvuju sa približno 60% u ukupnoj proizvodnji električne energije, dok obnovljivi izvori – uprkos značajnom potencijalu – imaju relativno ograničen udio [11]. Prosječna starost termoenergetskih postrojenja prelazi četiri decenije, a investicije u modernizaciju i smanjenje emisija su ograničene. Iako BiH raspolaže značajnim potencijalom za razvoj vjetroenergije, solarne energije i biomase [32], institucionalne i regulatorne prepreke usporavaju realizaciju projekata. Istovremeno, energetska tranzicija ima i makroekonomsku dimenziju, budući da izvoz električne energije predstavlja važan izvor deviznih prihoda. Uvođenje CBAM-a može generisati dodatne troškove za energetski i industrijski sektor, čime se direktno utiče na izvoznu konkurentnost zemlje. Dodatnu složenost uvodi činjenica da izvozna struktura Bosne i Hercegovine prema EU ostaje dominantno koncentrisana u sektorima sa višim intenzitetom emisija CO_2, uključujući metalnu industriju, bazne materijale i energiju [31]. Empirijska istraživanja zasnovana na gravitacionim modelima pokazuju da BiH ne ostvaruje puni izvozni potencijal prema EU tržištu [8], [4], [38], što dodatno povećava osjetljivost na regulatorne promjene. Zelena tranzicija stoga za Bosnu i Hercegovinu ne predstavlja isključivo klimatski izazov, već kompleksno razvojno i konkurentsko pitanje. Ona istovremeno podrazumijeva restrukturiranje energetskog sektora, tehnološku modernizaciju industrije i redefinisanje izvozne strategije u skladu sa novim regulatornim standardima EU. Upravo u toj tački nastaje istraživačka potreba ovog rada: analiza sektorske izloženosti Bosne i Hercegovine regulatornim efektima zelene tranzicije EU, sa posebnim fokusom na intenzitet emisija CO_2, strukturu izvoza i potencijalne konkurentske rizike u uslovima primjene CBAM mehanizma.

Energetski sektor u Bosni i Hercegovini: strukturne karakteristike i izazovi tranzicije

Energetski sektor Bosne i Hercegovine i dalje je dominantno oslonjen na proizvodnju električne energije iz fosilnih goriva, prvenstveno uglja. Prema dostupnim podacima, termoelektrane učestvuju sa približno 55–60% u ukupnoj proizvodnji električne energije, dok hidroelektrane čine oko 35–40%, a vjetroelektrane i solarni izvori zajedno učestvuju sa manje od 5% [11]. Ovakva struktura energetskog miksa svrstava BiH među elektroenergetske sisteme u Evropi sa visokim intenzitetom emisije CO_2. Formalni okvir za energetsku tranziciju uspostavljen je 2013. godine usvajanjem Strategije prilagođavanja klimatskim promjenama i niskougljeničnog razvoja. Međutim, implementacija postavljenih ciljeva odvija se sporije od planiranog, uz izražene institucionalne i političke barijere. Prema [28], u javnom diskursu i dalje je prisutan izražen skepticizam prema obnovljivim izvorima energije, uz percepciju da proces dekarbonizacije primarno reflektuje regulatorne i geopolitičke interese Evropske unije. Energetska tranzicija u BiH stoga ne zavisi isključivo od tehničkih i finansijskih kapaciteta, već prvenstveno od institucionalne sposobnosti da se sprovedu strukturne reforme. U kontekstu primjene CBAM mehanizma, transformacija energetskog sektora postaje ne samo klimatski, već i konkurentski imperativ. Bez smanjenja intenziteta emisija CO_2 u elektroenergetskom i industrijskom sektoru, izvozna konkurentnost Bosne i Hercegovine mogla bi biti dodatno narušena, posebno na tržištu Evropske unije, koja je najznačajnije izvozno tržište BiH.

II. PREGLED DOSADAŠNJIH ISTRAŽIVANJA

Savremena literatura koja se bavi zelenom tranzicijom Evropske unije i njenim spoljnim efektima, može se sistematizovati u tri međusobno povezane cjeline: 1) radovi o političko – ekonomskim i trgovinskim implikacijama CBAM-a; 2) istraživanja o strukturnim i energetskim izazovima zemalja Zapadnog Balkana u procesu dekarbonizacije, te 3) empirijske studije o trgovinskom potencijalu i izvoznim ograničenjima Bosne i Hercegovine. Integracijom ovih pristupa dobija se koherentan okvir za analizu sektorske izloženosti i rizika u kontekstu zelene tranzicije Evropske unije. Prva grupa autora pokazuje visok stepen saglasnosti da Carbon Border Adjustment Mechanism (CBAM) predstavlja hibridni instrument klimatske, trgovinske i industrijske politike Evropske unije. [23] naglašava da je CBAM odgovor Evropske unije na rizik „curenja ugljenika“, ali i instrument zaštite konkurentnosti evropske industrije. Slično tome, [40] ukazuje na njegovu višestruku pravnu i regulatornu dimenziju, ističući problem njegove kompatibilnosti sa pravilima međunarodne trgovine. Modelske simulacije potvrđuju da efekti CBAM-a zavise od njegovog dizajna i obuhvata. [1] pokazuju da širi sektorski obuhvat i strožiji obračun emisija, povećavaju klimatsku efikasnost, ali istovremeno produbljuju negativne trgovinske efekte po treće zemlje. [45] zaključuju da CBAM može poboljšati relativnu konkurentnost evropske industrije, ali uz potencijalne „beggar – thy – neighbour“ efekte na trgovinske partnere. Posebno su relevantni radovi koji analiziraju razvojnu dimenziju CBAM-a. [29] pokazuju da zemlje sa visokim intenzitetom emisije CO_2 i slabim investicionim kapacitetima snose relativno veći teret prilagođavanja. [10] uvode koncept „karbonske ljestvice“, prema kojem CBAM može podstaći dekarbonizaciju, ali i produbiti zavisnost perifernih ekonomija od privrede Evropske unije. Slične zaključke iznose i [37], naglašavajući rizike za zemlje

Globalnog juga, dok [39] zagovaraju diferencirani pristup kako bi se mehanizam učinio klimatski i razvojno prihvatljivim. Druga grupa radova fokusira se na energetsku i institucionalnu spremnost Zapadnog Balkana za zelenu tranziciju. [26] i [22] ističu visok intenzitet emisije CO_2, zavisnost od uglja i ograničene kapacitete kao ključne prepreke dekarbonizaciji. [16] kroz energetsko modeliranje pokazuju da je tehnički izvodljiva tranzicija ka obnovljivim izvorima, ali uz visoke finansijske troškove i potrebu regionalne integracije. [17] naglašavaju razvojna ograničenja regiona, dok [5] ukazuju na zavisnost BiH od međunarodnog klimatskog finansiranja. [8] potvrđuju da digitalizacija može imati komplementarnu ulogu u smanjenju emisija, dok [41] ističu značaj energetske efikasnosti kao pokretača cirkularne ekonomije. Sektorski pristupi dodatno rasvjetljavaju izloženost pojedinih grana. [19] kroz LCA analizu rudarskog sektora ukazuju na visok intenzitet emisije CO_2 pri eksploataciji boksita. [44] potvrđuju slične obrasce u teškoj industriji, dok [20] i [2] identifikuju potencijal biomase i „waste – to – energy“ sistema kao alternativnih pravaca dekarbonizacije. Širi institucionalni kontekst razmatraju [18], [42] i [43], naglašavajući da institucionalna fragmentacija i geopolitičke tenzije mogu usporiti implementaciju evropskih politika. [24] dodatno pokazuje da valutni odbor ograničava makroekonomsku fleksibilnost BiH u suočavanju sa eksternim šokovima, uključujući klimatske regulatorne promjene. Treću grupu čine radovi koji primjenjuju gravitacione i druge modele za procjenu spoljnotrgovinskog potencijala BiH. Već rani radovi [6], [25], [4] ukazuju da je trgovina BiH sa EU ispod mogućeg potencijala, količinski i vrijednosno. [7] i [21] potvrđuju značaj regionalne integracije, ali i postojanje necarinskih barijera koje značajno ograničavaju obim spoljnotrgovinske razmjene između zemalja Zapadnog Balkana i Evropske unije. Institucionalni kapacitet se pokazuje kao ključni faktor [27], dok [3] i [30] naglašavaju ograničavajuću ulogu tehničkih i administrativnih prepreka. [38] potvrđuju da liberalizacija trgovine sa zemljama članicama EU daje rezultate tek nakon strukturalnog prilagođavanja izvoza. Najnovija empirijska analiza [31] pokazuje da je BiH u periodu 2003 – 2022. godine koristila svega oko 49% svog izvoznog potencijala u trgovini sa zemljama članicama EU, uz dominantno sirovinsku strukturu izvoza. [9] dodatno potvrđuju da postoje neiskorišteni bilateralni potencijali u trgovini BiH sa svojim glavnim spoljnotrgovinskim partnerima. Ovi nalazi su od presudnog značaja u kontekstu CBAM-a i zelene tranzicije na prostoru zemalja Zapadnog Balkana, sa posebnim osvrtom na Bosnu i Hercegovinu. Ukoliko je izvozni potencijal Bosne i Hercegovine već ograničen strukturnim i institucionalnim faktorima, dodatni troškovi regulative emisija CO_2 mogu dodatno smanjiti konkurentnost sektora poput metalurgije, električne energije i baznih materijala. Literatura pokazuje visok stepen saglasnosti u tri ključne tačke: CBAM ima izražene geoekonomske efekte, zemlje Zapadnog Balkana karakteriše visok intenzitet emisija CO_2 i institucionalna ograničenja, a BiH nije u potpunosti iskoristila svoj izvozni potencijal prema tržištu EU. Međutim, u literaturi se uočava istraživački jaz u povezivanju sektorske analize emisija CO_2 sa procjenom ranjivosti izvozne strukture u kontekstu CBAM regulative. Većina radova posmatra ili makroekonomske efekte, ili energetsku tranziciju, ili spoljnotrgovinski potencijal, ali rijetko kombinuje ove dimenzije u jedinstven analitički okvir. Upravo taj jaz nastoji da ispuni ovo istraživanje, kroz sektorsku analizu ranjivosti izvozne strukture i rizika BiH u uslovima zelene tranzicije EU. U tom smislu, istraživanje polazi od sljedećih istraživačkih hipoteza:

H1: Sektori BiH sa višim intenzitetom emisija CO_2 i značajnim udjelom izvoza prema EU izloženi su povećanom regulatornom i konkurentskom riziku u uslovima primjene CBAM mehanizma

H2: Izvozna struktura BiH prema tržištu EU pokazuje dugoročnu koncentraciju u izvoznim sektorima sa visokom energetskom intenzivnošću i visokim intenzitetom emisija CO_2.

III. METODOLOGIJA

Metodologija i empirijska procjena sektorske izloženosti CBAM mehanizmu

Empirijsko istraživanje zasnovano je na deskriptivno-komparativnoj analizi izvozne strukture Bosne i Hercegovine, uz primjenu indikatora sektorske izloženosti CBAM regulativi u cilju procjene regulatornog i konkurentskog rizika povezanog sa zelenom tranzicijom Evropske unije. Analiza koristi sekundarne podatke o spoljnotrgovinskoj razmjeni Bosne i Hercegovine za 2015, 2019, 2020. i 2024. godinu, čime je omogućeno sagledavanje dugoročnih strukturnih obrazaca izvoza u različitim ekonomskim fazama, uključujući stabilni predpandemijski period, krizne poremećaje i savremeni kontekst tranzicione primjene CBAM mehanizma. Metodološki pristup zasniva se na identifikaciji sektora obuhvaćenih Uredbom (EU) 2023/956 — električne energije, željeza i čelika, aluminijuma, cementa i đubriva — te kvantifikaciji njihovog udjela u ukupnom izvozu Bosne i Hercegovine, u skladu sa pristupima primijenjenim u savremenim analizama trgovinskih efekata klimatskih politika [10], [23].

U tu svrhu definisan je indikator sektorske izloženosti CBAM mehanizmu (ICBAM), izražen kao odnos izvoza emisijski intenzivnih sektora i ukupnog izvoza zemlje.

U nastavku je dat tabelarni pregled izračunatih pokazatelja:

Tabela 1. Procijenjeni izvoz CBAM sektora i vrijednosti ICBAM

Godina	Procijenjeni izvoz CBAM sektora (mil. KM)	Ukupan izvoz (mil. KM)	ICBAM
2015.	≈ 850	≈ 9.034	0,094
2019.	≈ 1.050	≈ 11.900	0,088
2020.	≈ 820	≈ 10.500	0,078
2024.	1.224	16.070	0,076

Izvor: Obrada autora na osnovu podataka MVTEO 2016; MVTEO 2020; MVTEO 2021; MVTEO 2025

IV. REZULTATI

Geografska koncentracija izvoza

Bosna i Hercegovina pokazuje dugoročnu i izrazitu zavisnost od tržišta Evropske unije, što predstavlja jednu od ključnih strukturnih karakteristika njene spoljnotrgovinske razmjene. U 2015. godini izvoz u zemlje EU činio je 71,8% ukupnog izvoza [33]. Ovaj udio je u 2019. godini porastao na 73% [34], dok je u kriznoj 2020. godini, uprkos poremećajima izazvanim pandemijom, zadržan na visokom nivou od 72,4% [35]. Najnoviji podaci za 2024. godinu potvrđuju kontinuitet ovog obrasca: izvoz u EU iznosio je 11,75 milijardi KM, što predstavlja više od 70% ukupnog izvoza Bosne i Hercegovine [36]. Ovakva stabilna i dugotrajna geografska koncentracija izvoza ukazuje na izraženu strukturnu upućenost BiH privrede na tržište Evropske unije. Istovremeno, ona povećava osjetljivost domaće ekonomije na regulatorne, klimatske i trgovinske promjene koje se uvode unutar EU, uključujući primjenu Mehanizma za prekogranično prilagođavanje ugljenika (CBAM).

Sektorska struktura izvoza i proizvodi osjetljivi na CBAM

Analiza sektorske strukture izvoza Bosne i Hercegovine u periodu 2015–2024. godine ukazuje na dugoročnu stabilnost udjela energetskih i metaloprerađivačkih proizvoda, koji su ujedno i najrelevantniji u kontekstu CBAM regulative. U 2015. godini među najznačajnijim izvoznim kategorijama nalazili su se metalni proizvodi, električna energija i bazne sirovine [33]. Već u tom periodu energetski i metalni sektor činili su važan segment izvozne strukture, što ukazuje na ranu prisutnost sektora sa većim intenzitetom emisija CO_2 u ukupnom izvozu. Predpandemijska 2019. godina potvrđuje kontinuitet tog obrasca. Električna energija činila je približno 5% ukupnog izvoza [34], dok su proizvodi od željeza i čelika zadržali značajan udio u ukupnoj robnoj razmjeni. Ovi podaci ukazuju da energetski i metaloprerađivački sektor predstavljaju strukturne, a ne ciklične komponente izvozne baze. U 2020. godini, obilježenoj globalnim ekonomskim poremećajima usljed pandemije, ukupna spoljnotrgovinska razmjena zabilježila je pad, ali je izvoz električne energije ostao relativno stabilan, dostižući 497,19 miliona KM [35]. Ova činjenica potvrđuje otpornost energetskog sektora, ali istovremeno i njegovu kontinuiranu relevantnost u ukupnoj izvoznoj strukturi. Najnoviji podaci za 2024. godinu dodatno potvrđuju strukturnu važnost CBAM-osjetljivih sektora. Vrijednost izvoza električne energije iznosila je 669,8 miliona KM, dok su željezne i čelične konstrukcije dostigle 554,4 miliona KM. Istovremeno, izolovani kablovi – kao industrijski proizvod povezan sa metaloprerađivačkim i elektroenergetskim lancem vrijednosti – ostvarili su izvoz od 684,9 miliona KM [36]. Ukupan izvoz Bosne i Hercegovine u 2024. godini iznosio je 16,07 milijardi KM [36]. Ukoliko se analiza ograniči na sektore direktno obuhvaćene CBAM regulativom – prvenstveno električnu energiju te proizvode od željeza i čelika – njihov zbirni izvoz u 2024. godini iznosio je približno 1,224 milijarde KM, što predstavlja oko 7,6% ukupnog izvoza. Kada se u širu procjenu uključe i aluminijski proizvodi, kao i ostale energetski intenzivne industrije, realna izloženost CBAM regulativi prelazi 10% ukupne izvozne strukture.

Tabela 2. Komparativni pregled (2015–2024. godine)

Godina	**Izvoz u EU (%)**	**Električna energija (mil. KM)**	**Proizvodi od metala**	**Procijenjeni CBAM udio**
2015.	71,8 %	značajan udio	visok	~7–9%
2019.	73%	~5% ukupnog izvoza	visok	~8–10%
2020.	72,4 %	497,19	stabilan	~7–9%
2024.	>70%	669,8	554,4	≥7,6% (direktno), >10% (šire)

Izvor: Obrada autora na osnovu podataka MVTEO 2016; MVTEO 2020; MVTEO 2021; MVTEO 2025

S obzirom na visoku geografsku koncentraciju izvoza i značajan udio sektora sa većim intenzitetom emisija CO_2, Bosna i Hercegovina se može smatrati strukturno izloženom efektima CBAM-a.

Indikator ICBAM

Rezultati analize pokazuju da je vrijednost ovog indikatora u posmatranom periodu ostala relativno stabilna, krećući se u rasponu od približno 0,076 do 0,094, uprkos značajnom rastu ukupnog izvoza Bosne i Hercegovine između 2015. i 2024. godine. Blago smanjenje vrijednosti indeksa sektorske izloženosti CBAM mehanizmu u posmatranom periodu ne ukazuje na značajnu transformaciju industrijske strukture Bosne i Hercegovine, već prvenstveno odražava brži rast ukupnog izvoza u odnosu na emisijski intenzivne sektore. Istovremeno, snažna geografska koncentracija izvoza prema tržištu Evropske unije (više od 70% izvoza BiH odlazi u zemlje članice EU [36]) dodatno intenzivira ukupni nivo ranjivosti, stvarajući kombinaciju sektorske i trgovinske zavisnosti.

V. ZAKLJUČAK

Zelena tranzicija Evropske unije, institucionalizovana kroz Evropski zeleni plan i primjenu Mehanizma za prekogranično prilagođavanje ugljenika (CBAM), predstavlja značajnu transformaciju regulatornog okvira međunarodne trgovine, sa posebno izraženim implikacijama za ekonomije koje su snažno integrisane sa tržištem Evropske unije. Rezultati sprovedenog istraživanja potvrđuju da Bosna i Hercegovina ulazi u ovaj proces sa izraženim strukturnim ograničenjima koja proizlaze iz karakteristika energetskog sistema i postojeće izvozne specijalizacije. Empirijska analiza pokazuje da

sektori direktno obuhvaćeni CBAM regulativom, prvenstveno proizvodnja električne energije te željezo i čelik, zadržavaju značajan udio u ukupnom izvozu Bosne i Hercegovine. Njihovo učešće iznosi približno 7,6% ukupnog izvoza, odnosno više od 10% ukoliko se uključe šire energetski zahtjevne industrije. Istovremeno, dugoročna geografska koncentracija izvoza prema Evropskoj uniji, koja kontinuirano prelazi 70% ukupnog izvoza, dodatno povećava osjetljivost domaće privrede na regulatorne promjene unutar EU tržišta. Analiza dinamike sektorske izloženosti u periodu 2015–2024. ukazuje na relativnu stabilnost indikatora CBAM izloženosti uz njegovo blago smanjenje. Međutim, takav trend prvenstveno odražava brži rast ukupnog izvoza u odnosu na sektore sa visokim intenzitetom emisija CO_2, a ne suštinsku transformaciju industrijske strukture ili značajnije smanjenje emisijskog intenziteta proizvodnje. Time se potvrđuje da proces diverzifikacije izvozne baze i prilagođavanja zahtjevima zelene tranzicije napreduje sporije od regulatornih promjena koje dolaze iz Evropske unije.

Na osnovu sprovedene analize može se zaključiti da su postavljene istraživačke hipoteze potvrđene. Rezultati potvrđuju da sektori sa višim intenzitetom emisija CO_2 i značajnim udjelom izvoza prema Evropskoj uniji predstavljaju glavne nosioce regulatornog i konkurentskog rizika u uslovima primjene CBAM mehanizma. Takođe, potvrđeno je da izvozna struktura Bosne i Hercegovine pokazuje dugoročnu koncentraciju upravo u energetski intenzivnim i industrijama sa visokim intenzitetom emisija CO_2, što povećava ukupnu izloženost klimatskim trgovinskim mjerama EU. Analiza pokazuje da zelena tranzicija Evropske unije ne utiče samo na postojeću izvoznu strukturu, već i na budući izvozni potencijal Bosne i Hercegovine, budući da regulatorni troškovi povezani sa emisijama CO_2 mogu ograničiti konkurentnost tradicionalnih izvoznih sektora ukoliko ne dođe do ubrzane energetske i tehnološke transformacije. Istovremeno, CBAM ne predstavlja isključivo ograničenje, već i potencijalni razvojni impuls. Dugoročno posmatrano, prilagođavanje novim klimatskim standardima može podstaći modernizaciju industrijske proizvodnje, povećanje energetske efikasnosti i jačanje investicija u obnovljive izvore energije. Ključni izazov ekonomske politike Bosne i Hercegovine stoga se odnosi na smanjenje intenziteta emisije CO_2 pri proizvodnji električne energije i postepenu transformaciju izvozne strukture ka proizvodima veće dodatne vrijednosti, čime bi se očuvala konkurentnost na tržištu Evropske unije u uslovima ubrzane zelene tranzicije.

U tom smislu, BiH predstavlja primjer ekonomije sa dvostrukom ranjivošću: sektorskom i geografskom.

Uprkos određenim ograničenjima vezanim za dostupnost detaljnijih sektorskih podataka o emisijama i troškovima prilagođavanja, rezultati ovog istraživanja pružaju relevantan empirijski osnov za razumijevanje odnosa između klimatske regulative Evropske unije i buduće dinamike izvoznog razvoja Bosne i Hercegovine.

LITERATURA

[1] Beaufils, T., Ward, H., Jakob, M., & Wenz, L. (2023). Assessing different European Carbon Border Adjustment Mechanism implementations and their impact on trade partners. Communications Earth & Environment. https://doi.org/10.1038/s43247-023-00788-4

[2] Bjelić, D., Markić, D. N., Prokić, D., Malinović, B., & Andrejević Panić, A. (2024). "Waste to energy" as a driver towards a sustainable and circular energy future for the Balkan countries. Energy, Sustainability and Society.

[3] Bjelić, P., Dragutinović Mitrović, R., & Popović Petrović, I. (2013). Administrative barriers to trade as predominant non-tariff barriers in the Western Balkans trade. Paper presented at the 3rd International Conference on International Trade and Investment, Mauritius.

[4] Bussière, M., Fidrmuc, J., & Schnatz, B. (2005). Trade integration of Central and Eastern European countries: Lessons from a gravity model. European Central Bank Working Paper No. 545.

[5] Causević, A., Avdić, S., Padegimas, B., & Macura, B. (2022). Analysis of international public funding flows for the environment, climate change, and sustainability: The case of Bosnia and Herzegovina. Energy, Sustainability and Society.

[6] Christie, E. (2002). Potential trade in Southeast Europe: A gravity model approach. WIIW Working Papers, No. 21. Vienna, AT: The Vienna Institute for International Economic Studies.

[7] Damijan J. P., Sousa J., & Lamotte O. (2006). The effect of trade liberalization in South-Eastern European countries. WIIW Balkan Observatory Working Paper No. 070. Vienna, AT: The Vienna Institute for International Economic Studies.

[8] Dedaj, B., Ogruk-Maz, G., Carabregu-Vokshi, M., Aliu-Mulaj, L., & Kisswani, K. M. (2022). Improving ICTs (mobile phone and internet) for environmental sustainability in the Western Balkan countries. Energies.

[9] Đogo, M., Gligorić, D., & Berecz, M. (2024). TRADE RELATIONS BETWEEN HUNGARY AND BOSNIA AND HERZEGOVINA: THE EVIDENCE FROM THE GRAVITY MODEL. Economic Horizons/Ekonomski Horizonti, 26(2).

[10] [Eicke, L., Weko, S., Apergi, M., & Marian, A. (2021). Pulling up the carbon ladder? Decarbonization, dependence, and third-country risks from the European carbon border adjustment mechanism. Energy Research & Social Science. https://doi.org/10.1016/j.erss.2021.102240

[11] Energy Community. (2023). Annual Implementation Report 2023. Vienna: Energy Community Secretariat.

[12] European Commission. (2019a). The European Green Deal. COM(2019) 640 final.

[13] European Commission. (2020). Guidelines for the implementation of the Green Agenda for the Western Balkans.

[14] European Commission. (2021). Fit for 55 package.

[15] European Commission. (2023). Regulation (EU) 2023/956 establishing a carbon border adjustment mechanism. Official Journal of the European Union.

[16] Fejzić, E., Niet, T., Wade, C., & Usher, W. (2023). Aligning the Western Balkans power sectors with the European Green Deal. Environmental Research Communications.

[17] Filipović, S., & Ignjatović, J. (2022). Economic development of the Western Balkans: Opportunities and limitations for green transition. Megatrend Revija.

[18] Golemi, E. (2013). The common challenges of South-East European countries in the process of European integration.

[19] Grbeš, A., Galić, I., Farkaš, B., & Budeš, I. (2021). Modelling-friendly life cycle inventory of underground mining of bauxite: A case study from Jajce mines in Bosnia and Herzegovina. Rudarsko-geološko-naftni zbornik.

[20] Gvero, P., Petrović, S., Papuga, S., & Kotur, M. (2013). Biomass as potential sustainable development driver: Case of Bosnia and Herzegovina.

[21] Herderschee, J., & Qiao, Z. (2007). Impact of intra-European trade agreements, 1990-2005: Policy implications for the Western Balkans and Ukraine. IMF Working Paper WP/2007/126.

Washington, DC: International Monetary Fund. https://doi.org/10.5089/9781451866902.001
[22] Ignjatović, J., Filipović, S., & Radovanović, M. (2024). Challenges of the green transition for the recovery of the Western Balkans. Energy, Sustainability and Society.
[23] Jakob, M. (2023). The political economy of carbon border adjustment in the EU. Oxford Review of Economic Policy. https://doi.org/10.1093/oxrep/grac044
[24] Jerinić, M. (2021). Adaptation to external shocks within the currency board system on the example of the Baltic countries and Bosnia and Herzegovina. DIEM: Dubrovnik International Economic Meeting.
[25] Kaminski, B. (2003). Stabilization and association process in the Balkans: integration options and their assessment. Available at SSRN 636472.
[26] Knez, S., Štrbac, S., & Podbregar, I. (2022). Climate change in the Western Balkans and EU Green Deal: Status, mitigation and challenges. Energy, Sustainability and Society. https://doi.org/10.1186/s13705-021-00328-y
[27] Kucharčuková O. B., Babecký J., & Raiser M. (2012). Gravity approach for modelling international trade in SouthEastern Europe and the Commonwealth of Independent States: The role of geography, policy and institutions. Open Economies Review, 23(2), 277-301. https://doi.org/10.1007/s11079-010-9187-8
[28] Kušljugić M., Miljević D. (2023). Guideline for Sustainable Energy Transition in Bosnia and Herzegovina., zelenaekonomija.komorabih.ba/wp-content/uploads/ 2023/10/Vodic-za-odrzivu-energetsku-tranziciju-u-Bosni-i-Hercegovini.pdf
[29] Magacho, G. R., Espagne, É., & Godin, A. (2023). Impacts of the CBAM on EU trade partners: Consequences for developing countries. Climate Policy. https://doi.org/10.1080/14693062.2023.2200758
[30] Marković I., Popović Petrović I., & Bjelić P. (2021). Elimination of non-tariff barriers in regional trade integrations: The CEFTA 2006 experience. Teme, 45(2), 601-620. https://doi.org/10.22190/TEME200505035M
[31] Marković, L. (2024). Istraživanje potencijala za porast izvoza Bosne i Hercegovine na tržišta zemalja Evropske unije. Master rad. Univerzitet u Istočnom Sarajevu, Ekonomski fakultet Pale
[32] Miljević, D., & Ribić, D. (2022). Financing energy transition in Bosnia and Herzegovina.
[33] Ministarstvo vanjske trgovine i ekonomskih odnosa Bosne i Hercegovine. (2016). Analiza spoljnotrgovinske razmjene BiH za 2015. godinu.
[34] Ministarstvo vanjske trgovine i ekonomskih odnosa Bosne i Hercegovine. (2020). Analiza spoljnotrgovinske razmjene BiH za 2019. godinu.
[35] Ministarstvo vanjske trgovine i ekonomskih odnosa Bosne i Hercegovine. (2021). Analiza spoljnotrgovinske razmjene BiH za 2020. godinu.
[36] Ministarstvo vanjske trgovine i ekonomskih odnosa Bosne i Hercegovine. (2025). Analiza spoljnotrgovinske razmjene BiH za 2024. godinu.
[37] Morone, P., & Alfino, A. (2025). Impact of the EU Carbon Border Adjustment Mechanism on the Global South. Discover Sustainability.
[38] Omerika, H., & Hadžović, M. (2019). Uticaj liberalizacije trgovine na izvoz iz Bosne i Hercegovine u Evropsku uniju, Časopis za ekonomiju i tržišne komunikacije, 17(1), 85-103. https://doi.org/10.7251/EMC1901085O
[39] Perdana, S., & Vielle, M. (2022). Making the EU Carbon Border Adjustment Mechanism acceptable and climate friendly for least developed countries. Energy Policy. https://doi.org/10.1016/j.enpol.2022.113245
[40] Pirlot, A. (2021). Carbon border adjustment measures: A straightforward multi-purpose climate change instrument?
[41] Ramčilović Jesih, A., Šimić, G., Konatar, L., Brljak, Z., & Šprajc, P. (2024). Energy efficiency as a driver of the circular economy and carbon neutrality in selected countries of Southern Europe: A soft computing approach. Energy, Sustainability and Society.
[42] Solioz, C. (2021). Facing democratic indeterminacy: The consequences of the Dayton Agreement. SEER.
[43] Turčalo, S., & Smajić, M. (2024). Eastern promise and EU integration: Deciphering the strategic implications of external influences in the Western Balkans. Studia Europejskie – Studies in European Affairs.
[44] Üçtuğ, F. G., Ediger, V., Küçüker, M. A., Berk, İ., İnan, A., & Fereidani, B. M. (2025). Cradle-to-gate life cycle assessment of heavy machinery manufacturing: A case study in Türkiye. The International Journal of Life Cycle Assessment.
[45] Zhong, J., & Luther, M. (2021). Beggar thy neighbor? On the competitiveness and welfare impacts of the EU's proposed carbon border adjustment mechanism.

UDK 347.426(497.6):[007.52:343.451
DOI 10.7251/ZRSNG2526085T

Građanskopravna odgovornost za štetu uzrokovanu sistemima vještačke inteligencije u Bosni i Hercegovini

Civil law liability for damage caused by artificial intelligence systems in Bosnia and Herzegovina

Marko Tomić, Univerzitet Sinergija Bijeljina, Jelena Manojlović, Univerzitet Sinergija Bijeljina

***Sažetak*— Oblast vještačke inteligencije (AI) je generalno gledano nepoznanica za domaći pravni sistem u mnogim aspektima. U tom kontekstu i pitanje građanskopravne odgovornosti za štetu uzrokovanu sistemima vještačke inteligencije predstavlja svojevrsni izazov kako za pravnu teoriju, tako i za pravnu praksu. Članak analizira kako se tradicionalni principi građanskog prava primjenjuju na štete koje uzrokuju sistemi vještačke inteligencije, te ukazuje na izazove koje donosi njihova autonomija i kompleksnost. Kada govorimo o AI sistemima u većini slučajeva teško je utvrditi ko je odgovoran za štetu — proizvođač, programer, korisnik ili sam operater sistema. Klasični modeli odgovornosti (krivica i objektivna odgovornost) nisu uvijek adekvatni jer AI može donositi odluke i bez direktne ljudske kontrole. Što je sistem autonomniji, to je teže dokazati uzročnu vezu i krivicu, što komplikuje sudske postupke. U Bosni i Hercegovini ne postoji poseban zakon koji direktno uređuje odgovornost za štetu uzrokovanu AI sistemima pa se primjenjuju opšta pravila građanskog prava sadržana prvenstveno u Zakonu o obligacionim odnosima. Sudskih presuda koje se direktno bave ovim pitanjem gotovo da i nema a u predmetima koji su povezani sa ovom oblašću, odgovornost za štetu se utvrđuje ili kao odgovornost za krivicu ili kao objektivna odgovornost. U ovom kontekstu značajno je istaći da BiH postepeno usklađuje svoje pravo sa pravom Evropske unije, što će neminovno dovesti do regulisanja ove i oblasti putem preuzimanja EU pravnih standarda.**

***Ključne riječi* – Građanskopravna oblast, šteta uzrokovana AI sistemima, pravna regulativa u Bosni i Hercegovini, pravni standardi Evropske unije**

Abstract – The field of artificial intelligence (AI) is generally unknown to the domestic legal system in many respects. In this context, the issue of civil liability for damage caused by artificial intelligence systems is a unique challenge for both legal theory and legal practice. The article analyzes how the traditional principles of civil law are applied to damages caused by artificial intelligence systems, and points to the challenges brought by their autonomy and complexity. When talking about AI systems, it is often difficult to determine who is responsible for the damage — the manufacturer, the developer, the user or the operator of the system itself. Classical models of responsibility (guilt and objective responsibility) are not always adequate because AI can make decisions without direct human control. The more autonomous the system, the more difficult it is to prove causation and guilt, which complicates court proceedings. In Bosnia and Herzegovina, there is no special law that directly regulates liability for damage caused by AI systems, so the general rules of civil law contained primarily in the Law on Obligations apply. There are almost no court rulings directly dealing with this issue, and in cases related to this area, responsibility for damage is determined either as liability for guilt or as objective responsibility. In this context, it is important to point out that BiH is gradually harmonizing its law with the law of the European Union, which will inevitably lead to the regulation of this area through the adoption of EU legal standards

***Keywords* – Civil law area, damage caused by AI systems, legal regulations in Bosnia and Herzegovina, legal standards of the European Union**

I. UVOD

Građanskopravna odgovornost za štetu uzrokovanu sistemima vještačke inteligencije predstavlja savremeno i sve značajnije pravno pitanje u Bosni i Hercegovini. Razvoj i sve šira primjena AI tehnologija otvaraju niz dilema u vezi sa utvrđivanjem odgovornosti za nastalu štetu.

Tradicionalni instituti obligacionog prava često nisu u potpunosti prilagođeni specifičnostima autonomnih i samoučećih sistema. Poseban izazov predstavlja identifikacija odgovornog subjekta, imajući u vidu kompleksan lanac učesnika koji uključuje proizvođače, programere, korisnike i operatere AI sistema.

Pitanje krivice dodatno se komplikuje zbog nepredvidivosti ponašanja određenih algoritama. U pravnom sistemu Bosne i Hercegovine još uvijek ne postoji poseban normativni okvir koji bi izričito regulisao ovu oblast. Stoga se u praksi primjenjuju opšta pravila o naknadi štete, uključujući odgovornost po osnovu krivice i objektivnu odgovornost.

Uporednopravna rješenja i inicijative na nivou Evropske unije mogu poslužiti kao smjernice za buduće zakonodavne

reforme. Takođe, važno je razmotriti balans između podsticanja tehnološkog razvoja i zaštite oštećenih lica.

Ovaj rad ima za cilj da analizira postojeći pravni okvir i ukaže na ključne izazove i moguće pravce razvoja regulacije odgovornosti za štetu uzrokovanu AI sistemima.

II. PRAVNI OKVIR U BOSNI I HERCEGOVINI

U Bosni i Hercegovini pitanje građanskopravne odgovornosti za štetu uzrokovanu sistemima vještačke inteligencije još uvijek nije posebno normirano, već se rješava primjenom opštih pravila obligacionog prava a što može dovesti do pravne nesigurnosti. [1]

Ključni propis u ovoj oblasti predstavlja Zakon o obligacionim odnosima koji uređuje osnove odgovornosti za štetu kroz institute subjektivne i objektivne odgovornosti. U Bosni i Hercegovini postoje tri zakona (Republike Srpske, Federacije BiH i Brčko Distrikta) koji uređuju oblast obligacionih odnosa, u suštini na gotovo identičan način jer se temelje na istom starom zakonu iz vremena Socijalističke Federativne Republike Jugoslavije. Rad će se bazirati na Zakonu o obligacionim odnosima Republike Srpske (ZOO RS), ("Sl. list SFRJ", br. 29/1978, 39/1985, 45/1989 - odluka USJ i 57/1989 i "Sl. glasnik RS", br. 17/1993, 3/1996, 37/2001 - dr. zakon, 39/2003 i 74/2004).[2] Prema ovom zakonu, odgovornost se najčešće zasniva na principu krivice (čl. 158-163 ZOO RS) što podrazumijeva postojanje protivpravne radnje, štete, uzročne veze i krivice štetnika. Takođe, moguće je primijeniti i princip objektivne odgovornosti (čl. 173-177 ZOO RS) koji reguliše odgovornost za opasnu stvar ili djelatnost.

Međutim, kod AI sistema problem nastaje u dokazivanju krivice, jer algoritamsko odlučivanje može biti netransparentno i teško razumljivo. U takvim situacijama, sudovi bi potencijalno mogli posegnuti za pravilima o objektivnoj odgovornosti, naročito ako se AI sistem kvalifikuje kao opasna stvar ili djelatnost.

Dodatni relevantni propisi uključuju Zakon o zaštiti potrošača, koji može biti primjenljiv u slučajevima kada AI proizvodi ili usluge uzrokuju štetu krajnjim korisnicima. U BiH postoje Zakon o zaštiti potrošača BiH ("Sl. glasnik BiH", br. 25/2006 i 88/2015) [3] i entitetski Zakon o zaštiti potrošača Republike Srpske (ZZP RS), ("Sl. glasnik RS", br. 101/2025). [4] koji je novijeg datuma i adekvatnije reguliše ovu problematiku. Takođe, određeni aspekti mogu biti obuhvaćeni pravilima o odgovornosti za neispravan proizvod, iako ni ova oblast nije detaljno razrađena u kontekstu AI tehnologija. Pravna praznina posebno dolazi do izražaja kada je riječ o autonomnim sistemima koji djeluju bez neposredne ljudske kontrole.

U sudskoj praksi Bosne i Hercegovine još uvijek nema značajnog broja sudskih odluka koje se direktno odnose na štetu uzrokovanu vještačkom inteligencijom. Ipak, hipotetički je moguće povezati konkretne članove zakona sa mogućim sa situacijama iz prakse koje se odnose na AI sisteme.

Ako se se fokusiramo na Zakon o zaštiti potrošača RS možemo navesti sljedeći primjer:

Članovi 7–9 ZZP RS (obaveza stavljanja na tržište samo sigurnih proizvoda) se može primijeniti ako pametni uređaj sa AI funkcijama (npr. “smart home” sistem) izazove štetu zbog greške u algoritmu. U tom slučaju potrošač se može pozvati na pravo na sigurnost i odgovornost trgovca.

Ako se baziramo na odredbe sadržane u ZOO RS, koje su primjenljive na konkretne slučajeve iz prakse, onda možemo navesti sljedeće primjere:

- *Član 158-163 ZOO RS (odgovornost po osnovu krivice)* može se primijeniti u situaciji kada, na primjer, kompanija implementira AI sistem bez adekvatnog testiranja ili nadzora. Ukoliko takav sistem donese pogrešnu odluku (npr. u medicinskoj dijagnostici ili finansijskom odlučivanju), oštećeno lice bi moglo dokazivati da je šteta posljedica nemara ili propusta u postupanju odgovornog subjekta (npr. operatera ili implementatora sistema).
- *Članovi 173–177 ZOO RS (objektivna odgovornost za opasnu stvar ili djelatnost)* posebno su interesantni u kontekstu AI. Na primjer, ako bi se autonomno vozilo koristilo na putevima u Republici Srpskoj i izazvalo saobraćajnu nezgodu, moglo bi se smatrati „opasnom stvari“. U tom slučaju, vlasnik ili korisnik vozila odgovarao bi bez obzira na krivicu, što olakšava položaj oštećenog lica.
- *Član 171 ZOO RS (odgovornost za zaposlenog)* dolazi u obzir kada zaposleni nepravilno koristi AI sistem. Na primjer, ako službenik unese netačne podatke u sistem, a AI na osnovu toga generiše štetnu odluku, poslodavac bi mogao odgovarati za štetu prema trećim licima.
- *Član 172 ZOO RS (odgovornost pravnog lica za rad svojih organa)* može biti primjenjiv kada AI sistem koristi određena kompanija (npr. banka ili osiguravajuće društvo). Ako AI sistem donese štetnu odluku (npr. diskriminatornu odluku o kreditu), odgovornost bi se pripisala pravnom licu, bez obzira na to što je odluku formalno „donio“ algoritam.
- *Član 177 ZOO RS (oslobađanje od odgovornosti)* mogao bi se primijeniti u situacijama kada šteta nastane usljed nepredvidivog ponašanja AI sistema koje se nije moglo izbjeći ni uz dužnu pažnju. Međutim, u praksi bi dokazivanje ovih okolnosti bilo izuzetno složeno, posebno zbog pitanja transparentnosti algoritama.
- *Član 177 st. 3 ZOO RS (doprinos oštećenog)* može biti relevantan ako je i sam korisnik doprinio nastanku štete, na primjer nepravilnim korištenjem AI aplikacije ili ignorisanjem jasnih upozorenja sistema.
- Konačno, *član 200 ZOO RS (nematerijalna šteta)* može se primijeniti u slučajevima gdje AI sistemi povrijede lična prava, poput časti, ugleda ili privatnosti (npr. pogrešna obrada ličnih podataka ili automatizovano donošenje odluka koje imaju diskriminatorne efekte).

S obzirom na sve navedeno, može se zaključiti da pravni okvir Bosne i Hercegovine trenutno nije u potpunosti prilagođen izazovima koje donosi vještačka inteligencija. Nedostatak specifičnih propisa dovodi do pravne nesigurnosti i otežava efikasnu zaštitu oštećenih lica. Zbog toga se sve više ističe potreba za normativnim intervencijama koje bi preciznije uredile ovu oblast. U tom kontekstu, iskustva i

zakonodavne inicijative Evropske unije mogu imati značajan uticaj na budući razvoj domaćeg prava.

III. MEĐUNARODNOPRAVNI OKVIR – PRAVO EVROPSKE UNIJE

Građanskopravna odgovornost za štetu uzrokovanu sistemima vještačke inteligencije predstavlja jedno od najaktuelnijih pitanja u pravu Evropske unije. Evropska unija nastoji da uspostavi ravnotežu između podsticanja inovacija i zaštite prava oštećenih lica. Tradicionalni instituti odgovornosti, poput krivice i uzročnosti, suočavaju se s izazovima zbog autonomije i kompleksnosti AI sistema. Poseban problem predstavlja tzv. "crna kutija" efekat, gdje je teško utvrditi kako je sistem donio određenu odluku.

Postavlja se pitanje da li postojeći sistemi građanskopravne odgovornosti mogu adekvatno odgovoriti na izazove koje donosi vještačka inteligencija, ili je neophodno razviti poseban pravni režim prilagođen njenim specifičnostima. [5]

U postojećem pravnom okviru EU, odgovornost za štetu se uglavnom zasniva na nacionalnim pravilima država članica. Međutim, zbog fragmentacije pravnih sistema, Evropska komisija je prepoznala potrebu za harmonizacijom. U tom kontekstu, predložene su reforme koje uključuju prilagođavanje pravila o odgovornosti za proizvode.

Komparativna analiza pokazuje da nacionalni pravni sistemi država članica nisu u potpunosti prilagođeni izazovima koje donosi vještačka inteligencija, naročito u pogledu dokazivanja uzročnosti i identifikacije odgovornog subjekta. [6]

Jedan od ključnih izazova jeste utvrđivanje odgovornog subjekta. U lancu razvoja i korištenja AI sistema mogu učestvovati proizvođači, programeri, distributeri i korisnici. EU pravo teži modelu u kojem odgovornost snosi onaj ko ima kontrolu nad rizikom. Ovo može uključivati i operatere visokorizičnih AI sistema.

Posebna pažnja posvećuje se visokorizičnim sistemima definisanim u okviru regulative o vještačkoj inteligenciji. Za ove sisteme predviđeni su stroži standardi sigurnosti i transparentnosti. Kršenje tih standarda može imati direktan uticaj na građanskopravnu odgovornost. Time se stvara veza između regulatornog i obligacionog prava.

EU takođe razmatra mogućnost uvođenja režima objektivne odgovornosti za određene AI sisteme. Ovaj pristup bi omogućio naknadu štete bez potrebe dokazivanja krivice. Takvo rješenje se smatra prikladnim za sisteme koji predstavljaju povećan rizik za društvo.

Zaštita potrošača je jedan od ključnih ciljeva ovih reformi. AI sistemi se sve više koriste u svakodnevnim uslugama, od zdravstva do finansija. Greške u radu takvih sistema mogu imati ozbiljne posljedice po korisnike. Zbog toga EU insistira na visokom nivou pravne sigurnosti.

Postojeći režim odgovornosti u Evropskoj uniji, posebno u oblasti odgovornosti za neispravne proizvode, zahtijeva prilagođavanje kako bi adekvatno obuhvatio specifičnosti AI sistema, uključujući njihovu autonomiju i sposobnost učenja. [7]

Važno pitanje je i odnos između ugovorne i vanugovorne odgovornosti. U mnogim slučajevima, oštećeni će imati mogućnost izbora pravnog osnova za naknadu štete. EU nastoji osigurati da pravila budu komplementarna i efikasna.

Takođe se razmatra i uloga osiguranja u pokrivanju šteta uzrokovanih AI sistemima. Obavezno osiguranje moglo bi biti uvedeno za određene kategorije visokorizičnih sistema. Ovo bi dodatno olakšalo obeštećenje žrtava.

Pristup zasnovan na procjeni rizika predstavlja ključni element budućeg razvoja odgovornosti za štetu uzrokovanu AI sistemima, omogućavajući fleksibilnije i efikasnije pravne odgovore na tehnološke izazove. [8]

U kontekstu pozitivnog prava Evropske unije, oblast građanskopravne odgovornosti za štetu uzrokovanu sistemima vještačke inteligencije uređena je kombinacijom postojećih i novijih (predloženih i usvojenih) pravnih akata. Najvažniji među njima su sljedeći:

Direktiva o odgovornosti za neispravne proizvode (85/374/EEZ) iz 1985. godine. [9] Ona uspostavlja režim objektivne odgovornosti proizvođača za štetu uzrokovanu neispravnim proizvodima. U kontekstu AI, značajna je njena revizija kojom se pojam proizvoda proširuje na softver i digitalne komponente.

Akt o vještačkoj inteligenciji (AI Act) iz 2024. godine. [10] Ovaj akt ne uređuje direktno građansku odgovornost, ali uspostavlja pravila o sigurnosti, transparentnosti i klasifikaciji AI sistema (posebno visokorizičnih). Kršenje ovih pravila može biti osnova za odgovornost za štetu.

Direktiva o odgovornosti za vještačku inteligenciju (AI Liability Directive) [11] – još uvijek u zakonodavnom procesu). Njen cilj jeste olakšavanje dokazivanja u sporovima koji uključuju AI sisteme, kroz mehanizme poput pretpostavke uzročnosti i pristupa dokazima.

Opšta uredba o zaštiti podataka (2016/679 (GDPR). [12] Iako primarno uređuje zaštitu ličnih podataka, ona sadrži odredbe o odgovornosti i naknadi štete u slučaju nezakonite obrade podataka, što je često povezano s AI sistemima.

U širem kontekstu digitalnog prava, važnu ulogu imaju i *Akt o digitalnim uslugama (Digital Services Act 2022/2065)* [13] i *Akt o digitalnim tržištima (Digital Markets Act iz 2024.)*. [14] Ovi akti uređuju odgovornost platformi i digitalnih posrednika, što može biti relevantno kada AI sistemi funkcionišu unutar online platformi.

Ne treba zanemariti ni *Direktivu o određenim aspektima ugovora o isporuci digitalnog sadržaja i digitalnih usluga (2019/770).* [15] Ona reguliše odgovornost za neispravnost digitalnih usluga, uključujući AI komponente koje se pružaju korisnicima.

Takođe, *Direktiva o prodaji robe (2019/771)* [16] obuhvata robu sa digitalnim elementima, što uključuje proizvode koji koriste AI tehnologiju.

Konačno, u razvoju su i dodatne inicijative Evropske komisije koje imaju za cilj dalje usklađivanje pravila o odgovornosti u digitalnom okruženju. U cjelini gledano, pravni okvir EU u ovoj oblasti je kombinacija klasičnih pravila o odgovornosti i novih digitalnih regulativa, sa jasnim

trendom ka jačoj zaštiti oštećenih i prilagođavanju tehnološkim izazovima.

Može se zaključiti da Evropska unija aktivno razvija pravni okvir za odgovornost za štetu uzrokovanu vještačkom inteligencijom. Cilj je stvoriti sistem koji je pravedan, predvidiv i prilagođen tehnološkom razvoju. Očekuje se da će buduće zakonodavne inicijative dodatno precizirati ova pitanja.

U pogledu konkretnih primjera iz sudske prakse može se istaći da je teško naći predmete koji se *direktno* odnose na građanskopravnu odgovornost za štetu uzrokovanu sistemima vještačke inteligencije u pravu EU, jer je riječ o relativno novoj oblasti. Međutim, postoje relevantni slučajevi iz prakse Evropskog suda pravde koji se tiču srodnih pitanja (npr. odgovornost za digitalne tehnologije, zaštita podataka, automatizovano odlučivanje), a koji se često koriste kao analogija.

Jedan od najočitijih primjera je predmet Google Spain SL i Google Inc. protiv Agencia Española de Protección de Datos (C-131/12). [17] U ovom slučaju, Sud je razmatrao odgovornost internet pretraživača za obradu ličnih podataka. Iako nije riječ o AI odgovornosti u užem smislu, presuda je utvrdila da operatori digitalnih sistema mogu snositi odgovornost za posljedice automatizovane obrade podataka. Ova logika je značajna i za AI sisteme koji obrađuju velike količine podataka.

Drugi važan slučaj je Lloyd protiv Google LLC [18], koji se, iako vođen pred britanskim sudovima, oslanja na evropske standarde zaštite podataka. Ovdje se raspravljalo o naknadi štete zbog povrede privatnosti putem automatizovanog praćenja korisnika. Ovaj predmet ukazuje na širenje koncepta nematerijalne štete u digitalnom okruženju, što je relevantno i za AI.

Takođe, vrijedi pomenuti predmet Schrems II (C-311/18) [19], gdje je Sud razmatrao zakonitost prijenosa podataka u treće zemlje. Iako fokus nije na odgovornosti za štetu, presuda naglašava visoke standarde zaštite podataka i odgovornosti subjekata koji koriste kompleksne digitalne sisteme, uključujući AI.

Iz ovih primjera može se zaključiti da sudska praksa EU još uvijek indirektno oblikuje pravila o odgovornosti za AI. Sud pravde postepeno razvija principe koji se mogu primijeniti na nove tehnologije, poput proširenog pojma odgovornosti, zaštite korisnika i olakšanog dokazivanja štete.

Kako AI sistemi postaju sve autonomniji i složeniji, pravni okvir će morati evoluirati od tradicionalnih modela krivice ka fleksibilnijim pristupima zasnovanim na procjeni rizika i raspodjeli odgovornosti između više aktera. [20]

U budućnosti se očekuje veći broj predmeta koji će se direktno odnositi na AI sisteme, posebno nakon pune primjene Akta o vještačkoj inteligenciji (AI Act) i eventualnog usvajanja Direktive o odgovornosti za AI.

IV. PERSPEKTIVE RAZVOJA U OVOJ OBLASTI U BIH

Perspektive razvoja građanskopravne odgovornosti za štete uzrokovane sistemima vještačke inteligencije u Bosni i Hercegovini potrebno je posmatrati u širem kontekstu procesa evropskih integracija i obaveze usklađivanja sa pravnom tekovinom Evropske unije. U tom smislu, budući razvoj ove oblasti biće u velikoj mjeri determinisan normativnim rješenjima koja se razvijaju na nivou Unije, naročito kroz instrumente poput AI Liability Directive i reformisanog režima odgovornosti za neispravne proizvode. Ovi instrumenti imaju za cilj prilagoditi tradicionalne institute građanskog prava specifičnostima autonomnih i kompleksnih tehnoloških sistema.

Koncept vještačke inteligencije predstavlja značajan izazov za tradicionalno građansko pravo u BiH, posebno u dijelu odgovornosti za štetu, zbog čega je neophodno razmotriti kreativnu interpretaciju i eventualnu reformu postojećih normi. [21]

Važeći sistem deliktne odgovornosti u Bosni i Hercegovini, koji se dominantno zasniva na principu krivice, suočava se sa značajnim izazovima u primjeni na štete uzrokovane vještačkom inteligencijom. Naime, složenost AI sistema, njihova autonomija i nepredvidivost otežavaju utvrđivanje subjektivne odgovornosti, kao i dokazivanje uzročne veze između radnje i nastale štete. U tom kontekstu, može se očekivati postepeno napuštanje dominantno subjektivnog modela odgovornosti u korist uvođenja elemenata objektivne odgovornosti, odnosno razvoja hibridnih modela koji kombinuju krivicu i rizik.

Poseban značaj imaće i procesne inovacije koje se razvijaju u pravu Evropske unije, a koje uključuju olakšavanje tereta dokazivanja za oštećena lica, uključujući pretpostavke uzročnosti i pravo pristupa relevantnim dokazima. Implementacija ovakvih rješenja u pravni sistem Bosne i Hercegovine zahtijevaće ne samo izmjene materijalnog prava, već i prilagođavanje procesnih pravila kako bi se osigurala efikasna i pravična sudska zaštita.

Dalji razvoj ove oblasti podrazumijeva i preciznije normiranje kruga odgovornih subjekata. Za razliku od klasičnih deliktnih odnosa, kod AI sistema odgovornost se može raspodijeliti između više aktera, uključujući proizvođače, programere, operatere i korisnike sistema. Takva disperzija odgovornosti zahtijevaće normativnu razradu kriterija za njeno pravično raspoređivanje, uzimajući u obzir stepen kontrole nad sistemom i mogućnost prevencije štete.

U kontekstu harmonizacije sa pravom Evropske unije, značajnu ulogu ima i povezivanje pravila o građanskopravnoj odgovornosti sa širim regulatornim okvirom za vještačku inteligenciju, koji razvija Evropska komisija kao glavno izvršno tijelo EU. Ovaj okvir zasniva se na pristupu regulaciji prema nivou rizika, što će neminovno uticati i na oblikovanje standarda dužne pažnje u građanskopravnim odnosima. Time se odgovornost sve više veže za procjenu i upravljanje rizicima koje AI sistemi mogu proizvesti.

Dodatni impuls razvoju ove oblasti u Bosni i Hercegovini predstavlja i pristupanje međunarodnim inicijativama,

uključujući aktivnosti Savjeta Evrope u oblasti regulacije vještačke inteligencije. Ovakvi koraci ukazuju na opredjeljenost ka prihvatanju evropskih i međunarodnih standarda, što će dugoročno doprinijeti harmonizaciji domaćeg pravnog sistema.

U perspektivi, može se očekivati donošenje posebnih normativnih akata koji će sistemski urediti pitanja vještačke inteligencije, uključujući i građanskopravnu odgovornost za štetu. Ipak, jednako važnu ulogu imaće i razvoj sudske prakse, koja će kroz konkretne slučajeve dati sadržaj apstraktnim pravnim normama i prilagoditi ih tehnološkoj realnosti.

Konačno, razvoj građanskopravne odgovornosti za štete uzrokovane AI sistemima u Bosni i Hercegovini treba da teži uspostavljanju ravnoteže između zaštite oštećenih lica i podsticanja tehnoloških inovacija. Takav balans predstavlja osnovni izazov savremenog prava, ali i ključni cilj harmonizacije sa pravnim standardima Evropske unije.

V. ZAKLJUČAK

Građanskopravna odgovornost za štetu uzrokovanu sistemima vještačke inteligencije u Bosni i Hercegovini nalazi se u početnoj fazi razvoja, suočena sa brojnim teorijskim i praktičnim izazovima. Postojeći pravni okvir, zasnovan na tradicionalnim propisima obligacionog prava, pokazuje ograničenja u primjeni na kompleksne i autonomne AI sisteme. Usklađivanje sa standardima Evropske unije predstavlja ključni pravac daljeg normativnog razvoja, naročito kroz prihvatanje savremenih rješenja u pogledu dokazivanja i raspodjele odgovornosti. Budući razvoj ove oblasti zahtijevaće kombinaciju zakonodavnih reformi, razvoja sudske prakse i jačanja institucionalnih kapaciteta. Konačno, cilj pravnog uređenja treba biti uspostavljanje efikasne zaštite oštećenih uz istovremeno očuvanje prostora za tehnološki napredak i inovacije.

VI. LITERATURA

[1] Nasir Muftić, *Artificial Intelligence and Tortious Liability: Case Study of Bosnia and Herzegovina* (2024)

[2] Zakon o obligacionim odnosima Republike Srpske ("Sl. list SFRJ", br. 29/1978, 39/1985, 45/1989 - odluka USJ i 57/1989 i "Sl. glasnik RS", br. 17/1993, 3/1996, 37/2001 - dr. zakon, 39/2003 i 74/2004)

[3] Zakon o zaštiti potrošača BiH ("Sl. glasnik BiH", br. 25/2006 i 88/2015)

[4] Zakon o zaštiti potrošača Republike Srpske ("Sl. glasnik RS", br. 101/2025)

[5] Baris Soyer i Andrew Tettenborn, 'Artificial Intelligence and Civil Liability—Do We Need a New Regime?' (2022).

[6] European Commission, *Comparative Law Study on Civil Liability for Artificial Intelligence* (2021).

[7] Curzio Fossati, 'AI Systems and Product Liability in the EU' (2023).

[8] Sundaraparipurnan Narayanan, 'A Risk-Based Approach to Assessing Liability Risk for AI-Driven Harms' (2023).

[9] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L 210/29.

[10] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts [2024] OJ L 1689.

[11] Directive (EU) 2023/XXXX of the European Parliament and of the Council of 15 June 2023 on liability for damage caused by artificial intelligence (AI Liability Directive) [2023]

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR) [2016] OJ L 119/1.

[13] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC [2022] OJ L 277/1.Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L 265/1.

[14] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L 136/1.

[15] Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods [2019] OJ L 136/28.

[16] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (Case C-131/12) [2014] ECLI:EU:C:2014:317.

[17] Google LLC v Lloyd [2021] UKSC 50 (UK Supreme Court).

[18] Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18) [2020] ECLI:EU:C:2020:559

[19] Ha-Chi Tran, 'Unbounded Harms, Bounded Law: Liability in the Age of Borderless AI' (2024) *Journal of Law and Technology.*

[20] Nasir Muftić, 'Liability for Artificial Intelligence – Adaptation of the Bosnian Legal Framework to the Challenges of the 21st Century' (2023) ***Društvene i humanističke studije*** 8(1) 213–232.

UDK 347.121(4/672EU):004.9(497.6)
DOI 10.7251/ZRSNG2526090S

Digitalni identitet i pravna regulativa podataka u EU i Bosni i Hercegovini - komparativni prikaz

Digital identity and legal regulation of data in the EU and Bosnia and Herzegovina - a comparative view

Dijana Savić Božić, Pravni fakultet Bijeljina, Ljubiša Mićić, Osnovni sud u Bijeljini

***Sažetak* – Razvoj informaciono-komunikacionih tehnologija i ubrzana digitalizacija društva doveli su do značajnog povećanja značaja digitalnog identiteta u savremenom pravnom i društvenom okruženju. Digitalni identitet predstavlja skup elektronskih podataka koji omogućavaju identifikaciju pojedinca u digitalnom prostoru i koji se koriste u različitim oblastima, uključujući elektronsku upravu, elektronsku trgovinu i finansijske usluge. Istovremeno, njegova upotreba podrazumijeva obradu velikog broja ličnih podataka, zbog čega pitanje pravne regulacije i zaštite privatnosti postaje jedno od ključnih pitanja savremenog informacionog prava. Cilj ovog rada je analiza pravnog okvira koji uređuje digitalni identitet i zaštitu ličnih podataka u Evropskoj uniji i Bosni i Hercegovini, uz poseban fokus na komparativni pristup koji omogućava sagledavanje sličnosti i razlika između ova dva regulatorna sistema. U radu se analizira evropski regulatorni okvir zasnovan na Opštoj uredbi o zaštiti podataka (GDPR) i uredbi eIDAS, kao i postojeće zakonodavstvo Bosne i Hercegovine u oblasti zaštite ličnih podataka. Posebna pažnja posvećena je komparativnoj analizi normativnih rješenja i institucionalnih mehanizama zaštite podataka. Rezultati istraživanja ukazuju da Evropska unija posjeduje razvijen i harmonizovan regulatorni sistem, dok se Bosna i Hercegovina i dalje nalazi u procesu usklađivanja zakonodavstva sa evropskim standardima. Zaključuje se da dalji razvoj pravnog okvira u Bosni i Hercegovini zahtijeva modernizaciju zakonodavstva i jačanje institucionalnih kapaciteta kako bi se obezbijedila efikasna zaštita digitalnog identiteta i ličnih podataka u savremenom digitalnom društvu.**

***Ključne reči* – digitalni identitet, zaštita ličnih podataka, GDPR, eIDAS, Evropska unija, Bosna i Hercegovina**

Abstract – The development of information and communication technologies and the accelerated digitization of society have led to a significant increase in the importance of digital identity in the modern legal and social environment. A digital identity is a set of electronic data that enables the identification of an individual in the digital space and is used in various fields, including e-government, e-commerce and financial services. At the same time, its use involves the processing of a large amount of personal data, which is why the issue of legal regulation and privacy protection becomes one of the key issues of modern information law. The aim of this work is the analysis of the legal framework that governs digital identity and personal data protection in the European Union and Bosnia and Herzegovina, with a special focus on a comparative approach that enables an overview of the similarities and differences between these two regulatory systems. The paper analyzes the European regulatory framework based on the General Data Protection Regulation (GDPR) and the eIDAS regulation, as well as the existing legislation of Bosnia and Herzegovina in the field of personal data protection. Special attention is paid to the comparative analysis of normative solutions and institutional data protection mechanisms. The research results indicate that the European Union has a developed and harmonized regulatory system, while Bosnia and Herzegovina is still in the process of harmonizing legislation with European standards. It is concluded that the further development of the legal framework in Bosnia and Herzegovina requires the modernization of legislation and the strengthening of institutional capacities in order to ensure the effective protection of digital identity and personal data in the modern digital society.

Keywords – digital identity, personal data protection, GDPR, eIDAS, European Union, Bosnia and Herzegovina

I. UVOD

Savremeno društvo obilježeno je intenzivnim razvojem informaciono-komunikacionih tehnologija, digitalizacijom javnih i privatnih usluga, kao i sve većom upotrebom elektronskih sistema za identifikaciju i autentifikaciju korisnika. U takvom okruženju koncept identiteta dobija novu dimenziju, koja se ne odnosi samo na tradicionalne oblike identifikacije pojedinca, već i na skup digitalnih podataka i atributa koji omogućavaju njegovo prepoznavanje i verifikaciju u digitalnom prostoru. Ovaj skup podataka, koji se u savremenoj literaturi označava kao digitalni identitet, postao je ključni element funkcionisanja digitalne ekonomije, elektronske uprave i različitih onlajn servisa, ali istovremeno otvara i brojna pitanja u vezi sa zaštitom privatnosti i pravnom regulacijom obrade ličnih podataka [1].

Digitalni identitet u najširem smislu predstavlja skup informacija u elektronskom obliku koje su povezane sa

određenim fizičkim ili pravnim licem i koje omogućavaju njegovu identifikaciju u digitalnom okruženju. Takvi podaci mogu uključivati osnovne identifikacione informacije, kao što su ime, prezime ili jedinstveni identifikacioni broj, ali i širi spektar atributa, uključujući elektronske identifikatore, biometrijske podatke, digitalne sertifikate ili druge elemente koji omogućavaju autentifikaciju korisnika u različitim informacionim sistemima. Razvoj digitalnih identiteta povezan je sa širim procesom digitalne transformacije društva, u kojem sve veći broj društvenih, ekonomskih i administrativnih aktivnosti prelazi u elektronsko okruženje, čime se povećava potreba za pouzdanim i bezbjednim sistemima identifikacije [2].

Istovremeno, digitalizacija društvenih procesa dovela je do značajnog povećanja obima prikupljanja i obrade ličnih podataka. Organizacije javnog i privatnog sektora danas raspolažu velikim količinama informacija koje se odnose na pojedince, pri čemu obrada takvih podataka često predstavlja osnovu za funkcionisanje savremenih digitalnih servisa. Upravo zbog toga zaštita ličnih podataka postaje jedno od centralnih pitanja savremenog informacionog prava, s obzirom na to da neadekvatna obrada ili zloupotreba podataka može dovesti do ozbiljnih povreda prava na privatnost i drugih osnovnih prava građana [3]. Povezanost između digitalnog identiteta i zaštite podataka posebno je naglašena u kontekstu razvoja elektronske identifikacije, biometrijskih tehnologija i automatizovanih sistema obrade informacija.

Evropska unija razvila je jedan od najnaprednijih pravnih okvira za zaštitu ličnih podataka i regulisanje digitalnog identiteta na globalnom nivou. Posebno značajnu ulogu u tom pogledu ima Opšta uredba o zaštiti podataka (General Data Protection Regulation – GDPR), koja je stupila na snagu 2018. godine i koja predstavlja temelj savremenog evropskog sistema zaštite podataka. Ova uredba uspostavlja jedinstven skup pravila o obradi ličnih podataka na teritoriji Evropske unije, definišući osnovne principe obrade, prava pojedinaca i obaveze organizacija koje obrađuju podatke [4]. Pored GDPR-a, značajan regulatorni instrument predstavlja i Uredba o elektronskoj identifikaciji i uslugama povjerenja za elektronske transakcije na unutrašnjem tržištu (eIDAS), koja uređuje pravni okvir za elektronsku identifikaciju i digitalne usluge povjerenja, čime se omogućava razvoj interoperabilnih sistema digitalnog identiteta na nivou Evropske unije [5]. Za države koje teže članstvu u Evropskoj uniji, uključujući Bosnu i Hercegovinu, usklađivanje nacionalnog zakonodavstva sa evropskim standardima u oblasti zaštite podataka predstavlja važan dio procesa evropskih integracija. Bosna i Hercegovina je usvojila Zakon o zaštiti ličnih podataka, kojim su postavljeni osnovni principi obrade i zaštite podataka, kao i institucionalni okvir za nadzor nad primjenom zakona kroz rad Agencije za zaštitu ličnih podataka. Međutim, iako postoje određeni elementi usklađenosti sa evropskim standardima, pravni okvir Bosne i Hercegovine još uvijek ne prati u potpunosti savremene regulatorne trendove Evropske unije, posebno u kontekstu novih tehnologija i digitalnih identitetskih sistema [6].

U tom kontekstu, pitanje pravne regulacije digitalnog identiteta dobija poseban značaj, jer efikasan regulatorni okvir mora istovremeno omogućiti razvoj digitalnih usluga i obezbijediti adekvatnu zaštitu prava građana. Balansiranje između tehnološkog razvoja i zaštite privatnosti predstavlja jedan od ključnih izazova savremenog prava informacionih tehnologija. Posebno je važno obezbijediti da sistemi digitalne identifikacije budu zasnovani na principima zakonitosti, transparentnosti i proporcionalnosti u obradi ličnih podataka, kako bi se spriječile potencijalne zloupotrebe i očuvalo povjerenje korisnika u digitalne servise [3].

Predmet rada jeste analiza pravnog okvira koji uređuje digitalni identitet i zaštitu ličnih podataka u Evropskoj uniji i Bosni i Hercegovini, sa posebnim fokusom na komparativni pristup koji omogućava sagledavanje sličnosti i razlika između ova dva regulatorna sistema. Cilj rada je da se identifikuju osnovne karakteristike evropskog modela regulacije digitalnog identiteta, da se analizira postojeći pravni okvir Bosne i Hercegovine u ovoj oblasti, kao i da se utvrdi u kojoj mjeri je nacionalno zakonodavstvo usklađeno sa standardima Evropske unije. Pored toga, rad ima za cilj da ukaže na ključne izazove u razvoju pravne regulacije digitalnog identiteta, posebno u kontekstu brzog tehnološkog razvoja i sve veće digitalizacije društva.

II. POJAM I ZNAČAJ DIGITALNOG IDENTITETA U SAVREMENOM DRUŠTVU

Razvoj savremenog informacionog društva doveo je do značajnih promjena u načinu na koji pojedinci učestvuju u društvenim, ekonomskim i administrativnim procesima. Digitalizacija velikog broja aktivnosti, uključujući elektronsku trgovinu, elektronsku upravu, finansijske usluge i komunikaciju putem interneta, dovela je do potrebe za pouzdanim mehanizmima identifikacije korisnika u digitalnom okruženju. U tom kontekstu razvija se koncept digitalnog identiteta, koji predstavlja skup podataka i atributa povezanih sa određenim licem, a koji omogućavaju njegovu identifikaciju i autentifikaciju u informacionim sistemima. Digitalni identitet tako postaje ključni element funkcionisanja savremenog digitalnog društva, jer omogućava bezbjedno i efikasno korišćenje digitalnih usluga, ali istovremeno otvara i brojna pitanja u vezi sa zaštitom privatnosti i upravljanjem ličnim podacima [7].

U najširem smislu, digitalni identitet može se definisati kao skup elektronskih informacija koje predstavljaju određenu osobu u digitalnom prostoru i koje omogućavaju njeno prepoznavanje u različitim informacionim sistemima. Ove informacije mogu obuhvatati osnovne identifikacione podatke, kao što su ime i prezime, datum rođenja ili identifikacioni broj, ali i dodatne elemente poput korisničkih naloga, elektronskih identifikatora, digitalnih sertifikata ili biometrijskih podataka. Digitalni identitet često uključuje i različite atribute koji opisuju karakteristike korisnika, kao što su profesionalni status, obrazovanje ili druge relevantne informacije koje se koriste u različitim digitalnim servisima [8]. Upravo zbog toga digitalni identitet ne predstavlja samo

tehnički identifikator, već kompleksan skup podataka koji može imati značajan uticaj na privatnost pojedinca i način na koji se njegovi lični podaci obrađuju.

U savremenom digitalnom okruženju digitalni identitet ima centralnu ulogu u omogućavanju pristupa različitim elektronskim uslugama. Elektronska uprava, na primjer, u velikoj mjeri zavisi od pouzdanih sistema digitalne identifikacije koji omogućavaju građanima da bez fizičkog prisustva ostvaruju svoja prava i koriste javne usluge putem interneta. Sličan značaj digitalni identitet ima i u oblasti elektronskog bankarstva, elektronske trgovine i različitih platformi koje omogućavaju interakciju između korisnika i pružalaca usluga. Pouzdani sistemi digitalne identifikacije omogućavaju smanjenje administrativnih troškova, povećanje efikasnosti javnih usluga i olakšavanje prekograničnih digitalnih transakcija, što je posebno značajno u kontekstu razvoja digitalne ekonomije [9].

Pored svojih funkcionalnih prednosti, digitalni identitet predstavlja i važan element u izgradnji povjerenja u digitalne sisteme. Korisnici digitalnih usluga moraju imati povjerenje da će njihovi lični podaci biti obrađivani na zakonit i bezbjedan način, kao i da će sistemi digitalne identifikacije biti zaštićeni od zloupotreba i neovlašćenog pristupa. Upravo zbog toga razvoj digitalnih identitetskih sistema mora biti praćen odgovarajućim pravnim i institucionalnim mehanizmima koji obezbjeđuju zaštitu prava pojedinaca i sprečavaju neadekvatnu obradu ličnih podataka. Bez adekvatne pravne regulacije, sistemi digitalnog identiteta mogu postati izvor ozbiljnih rizika za privatnost, posebno u slučajevima masovnog prikupljanja i obrade podataka ili njihove zloupotrebe od strane različitih organizacija [3].

Poseban značaj u savremenim raspravama o digitalnom identitetu imaju i tehnološke inovacije koje omogućavaju razvoj naprednih sistema identifikacije. Biometrijske tehnologije, kao što su prepoznavanje lica, otisaka prstiju ili šarenice oka, sve češće se koriste kao sredstva autentifikacije u različitim digitalnim servisima. Iako takve tehnologije mogu značajno povećati bezbjednost sistema identifikacije, one istovremeno otvaraju i složena pravna pitanja u vezi sa obradom osetljivih ličnih podataka. Biometrijski podaci smatraju se posebno osetljivom kategorijom ličnih podataka, jer njihova zloupotreba može imati dugoročne posljedice po privatnost pojedinca, s obzirom na to da takve karakteristike ne mogu biti promjenjene poput lozinki ili drugih identifikacionih sredstava [4].

U kontekstu razvoja digitalnih identiteta sve veći značaj dobija i koncept takozvanog samouvjerenog identiteta (self-sovereign identity), koji podrazumijeva model u kojem pojedinci imaju veću kontrolu nad sopstvenim digitalnim identitetskim podacima. Za razliku od tradicionalnih sistema identifikacije, gdje institucije ili organizacije upravljaju identitetskim podacima korisnika, modeli samouvjerenog identiteta zasnivaju se na principu da pojedinci mogu sami upravljati svojim digitalnim identitetom i odlučivati koje informacije će dijeliti sa određenim servisima. Ovakav pristup ima potencijal da unaprijedi zaštitu privatnosti i poveća transparentnost u obradi podataka, ali istovremeno zahtijeva razvoj odgovarajućih tehničkih i pravnih rješenja koja će omogućiti njegovu praktičnu primjenu [10].

Razvoj digitalnog identiteta usko je povezan sa širim konceptom digitalne transformacije društva. Vlade širom svijeta sve više ulažu u razvoj sistema elektronske identifikacije kako bi unaprijedile dostupnost javnih usluga i omogućile efikasnije upravljanje administrativnim procesima. Evropska unija u tom pogledu posebno naglašava značaj interoperabilnih sistema digitalne identifikacije koji omogućavaju građanima da koriste digitalne usluge u različitim državama članicama bez dodatnih administrativnih prepreka. Takav pristup doprinosi razvoju jedinstvenog digitalnog tržišta i olakšava prekograničnu saradnju u okviru Evropske unije [5].

Međutim, razvoj digitalnih identiteta istovremeno postavlja i brojne izazove za pravni sistem. Jedan od ključnih izazova odnosi se na balansiranje između potrebe za efikasnom identifikacijom korisnika i zaštite njihovih osnovnih prava, prije svega prava na privatnost i zaštitu ličnih podataka. Pravna regulacija digitalnog identiteta mora obezbijediti jasna pravila o prikupljanju, obradi i čuvanju identitetskih podataka, kao i efikasne mehanizme nadzora nad njihovom primjenom. U tom kontekstu međunarodni i regionalni pravni sistemi, uključujući pravni okvir Evropske unije, razvili su niz principa koji imaju za cilj obezbjeđivanje zakonite, transparentne i proporcionalne obrade ličnih podataka u digitalnom okruženju [4].

Sve navedeno ukazuje na činjenicu da digitalni identitet predstavlja jedan od ključnih koncepata savremenog informacionog društva, koji ima značajan uticaj na način funkcionisanja digitalnih usluga i zaštitu prava pojedinaca. Razumijevanje njegovih osnovnih karakteristika i pravnih implikacija predstavlja važan korak u analizi regulatornih okvira koji uređuju ovu oblast, što je posebno značajno u kontekstu razvoja evropskog pravnog sistema zaštite podataka i procesa harmonizacije zakonodavstva država koje teže članstvu u Evropskoj uniji.

III. PRAVNI OKVIR ZAŠTITE PODATAKA I DIGITALNOG IDENTITETA U EVROPSKOJ UNIJI

Pravni okvir zaštite ličnih podataka u Evropskoj uniji predstavlja jedan od najrazvijenijih i najuticajnijih sistema regulacije ove oblasti na globalnom nivou. Razvoj evropskog zakonodavstva u oblasti zaštite podataka povezan je sa nastojanjem da se obezbijedi efikasna zaštita osnovnih prava pojedinaca u digitalnom društvu, ali i da se istovremeno omogući slobodan protok podataka unutar jedinstvenog tržišta Evropske unije. U tom kontekstu, pravna regulacija digitalnog identiteta i obrade ličnih podataka razvijala se postepeno kroz niz pravnih akata i institucionalnih mehanizama koji imaju za cilj uspostavljanje visokog nivoa zaštite privatnosti i bezbjednosti informacija [11].

Jedan od temeljnih dokumenata koji potvrđuje značaj zaštite ličnih podataka u evropskom pravnom poretku jeste Povelja Evropske unije o osnovnim pravima, kojom je pravo na zaštitu ličnih podataka priznato kao posebno osnovno pravo. Član 8. ove Povelje predviđa da svako ima pravo na zaštitu ličnih podataka koji se odnose na njega, kao i da se takvi podaci moraju obrađivati zakonito, u određene svrhe i na osnovu pristanka lica na koje se odnose ili drugog legitimnog pravnog osnova predviđenog zakonom [12]. Ovim dokumentom postavljeni su temeljni principi koji su kasnije detaljnije razrađeni u zakonodavstvu Evropske unije koje uređuje zaštitu podataka i digitalni identitet.

Prije donošenja savremenog regulatornog okvira, zaštita ličnih podataka u Evropskoj uniji bila je uređena Direktivom 95/46/EC o zaštiti pojedinaca u vezi sa obradom ličnih podataka i slobodnim kretanjem takvih podataka. Ova direktiva predstavljala je prvi sveobuhvatni pravni instrument na nivou Evropske unije kojim su definisani osnovni principi obrade ličnih podataka, uključujući zakonitost obrade, ograničenje svrhe, proporcionalnost i bezbjednost podataka. Iako je direktiva značajno doprinijela harmonizaciji zakonodavstva država članica, njen osnovni nedostatak bio je u činjenici da su države članice imale određeni stepen slobode u njenoj implementaciji, što je dovelo do razlika u nacionalnim pravnim sistemima [13].

Sa ciljem prevazilaženja ovih nedostataka i prilagođavanja pravnog okvira novim tehnološkim izazovima, Evropska unija je 2016. godine usvojila Opštu uredbu o zaštiti podataka (General Data Protection Regulation – GDPR), koja je počela da se primjenjuje 2018. godine. Za razliku od direktive, uredba ima direktnu primjenu u državama članicama, čime je obezbjeđen veći stepen pravne harmonizacije i jedinstvena primjena pravila zaštite podataka na teritoriji Evropske unije. GDPR predstavlja jedan od najznačajnijih regulatornih instrumenata u oblasti zaštite podataka na globalnom nivou, jer uspostavlja sveobuhvatan sistem pravila koji uređuje način prikupljanja, obrade i čuvanja ličnih podataka [4].

Jedan od ključnih elemenata GDPR-a jeste definisanje osnovnih principa obrade ličnih podataka. Među najvažnijim principima izdvajaju se zakonitost, pravičnost, transparentnost i ograničenje svrhe obrade, minimizacija podataka, tačnost podataka, ograničenje perioda čuvanja i integritet i povjerljivost podataka. Ovi principi imaju za cilj da obezbijede da se lični podaci obrađuju na način koji poštuje prava i slobode pojedinaca, ali i da se organizacijama omogući zakonita obrada podataka u okviru njihovih poslovnih aktivnosti [4]. Poseban značaj imaju i prava ispitanika, kao što su pravo na pristup podacima, pravo na ispravku, pravo na brisanje podataka, poznato, „pravo na zaborav“, kao i pravo na ograničenje obrade i pravo na prenosivost podataka.

Pored definisanja principa obrade podataka, GDPR uvodi i značajne obaveze za organizacije koje obrađuju lične podatke. Organizacije su dužne da primjenjuju odgovarajuće tehničke i organizacione mjere zaštite podataka, da vode evidenciju o aktivnostima obrade, kao i da u određenim slučajevima imenuju službenika za zaštitu podataka. Takođe je uvedena obaveza prijavljivanja povreda bezbjednosti podataka nadležnim nadzornim organima, kao i obaveza obavještavanja pogođenih lica u slučajevima kada povreda može predstavljati visok rizik po njihova prava i slobode. Jedna od najznačajnijih novina GDPR-a jeste i uvođenje visokih novčanih kazni za kršenje pravila o zaštiti podataka, koje mogu iznositi do 20 miliona evra ili do četiri procenta ukupnog godišnjeg globalnog prometa organizacije [3].

U kontekstu digitalnog identiteta poseban značaj ima i Uredba o elektronskoj identifikaciji i uslugama povjerenja za elektronske transakcije na unutrašnjem tržištu, poznata kao eIDAS uredba. Ovaj pravni akt donijet je 2014. godine sa ciljem uspostavljanja jedinstvenog okvira za elektronsku identifikaciju i digitalne usluge povjerenja u Evropskoj uniji. eIDAS uredba omogućava međusobno priznavanje nacionalnih sistema elektronske identifikacije između država članica, čime se olakšava prekogranično korišćenje digitalnih usluga i unapređuje funkcionisanje jedinstvenog digitalnog tržišta [5].

Uredba eIDAS reguliše različite vrste usluga povjerenja, uključujući elektronske potpise, elektronske pečate, elektronske vremenske žigove, usluge elektronske dostave i autentifikaciju web-sajtova. Ovi instrumenti omogućavaju sigurnu elektronsku komunikaciju i verifikaciju identiteta korisnika u digitalnom okruženju, čime se povećava pravna sigurnost elektronskih transakcija. Posebno je značajno to što eIDAS uspostavlja pravni okvir koji omogućava da elektronski potpis ima istu pravnu snagu kao i tradicionalni rukopisni potpis, pod uslovom da ispunjava određene tehničke i bezbjednosne standarde [14].

Institucionalni okvir zaštite podataka u Evropskoj uniji takođe ima važnu ulogu u obezbjeđivanju efikasne primjene pravnih pravila. Svaka država članica ima sopstveno nezavisno nadzorno tijelo zaduženo za nadzor nad primjenom pravila o zaštiti podataka, dok na evropskom nivou značajnu ulogu ima Evropski odbor za zaštitu podataka (European Data Protection Board). Ovaj organ ima zadatak da obezbijedi dosljednu primjenu GDPR-a u državama članicama, da donosi smjernice za tumačenje propisa i da doprinosi koordinaciji između nacionalnih nadzornih organa [15].

Razvoj pravnog okvira Evropske unije u oblasti zaštite podataka i digitalnog identiteta predstavlja važan model za mnoge države širom svijeta, uključujući i države koje teže članstvu u Evropskoj uniji. Visoki standardi zaštite podataka koji su uspostavljeni kroz GDPR i eIDAS uredbu postali su referentni okvir za reforme nacionalnih zakonodavstava, posebno u kontekstu digitalne transformacije društva i sve veće upotrebe informacionih tehnologija. Upravo zbog toga analiza evropskog pravnog okvira predstavlja važnu osnovu za razumijevanje regulatornih izazova sa kojima se suočavaju države poput Bosne i Hercegovine u procesu usklađivanja svog zakonodavstva sa pravnim tekovinama Evropske unije.

IV. PRAVNA REGULATIVA DIGITALNOG IDENTITETA I ZAŠTITE PODATAKA U BOSNI I HERCEGOVINI

Zaštita ličnih podataka i regulacija digitalnog identiteta u Bosni i Hercegovini razvijaju se u okviru šireg procesa digitalizacije društva i usklađivanja nacionalnog zakonodavstva sa pravnim tekovinama Evropske unije. Iako Bosna i Hercegovina nije članica Evropske unije, proces evropskih integracija podrazumijeva postepeno usklađivanje domaćih propisa sa evropskim standardima, posebno u oblastima koje se odnose na zaštitu osnovnih prava građana, informaciono društvo i digitalno tržište. U tom kontekstu zaštita ličnih podataka predstavlja važan segment pravnog sistema, jer omogućava uspostavljanje ravnoteže između razvoja digitalnih tehnologija i zaštite privatnosti pojedinaca [11].

Osnovni pravni akt kojim je uređena oblast zaštite ličnih podataka u Bosni i Hercegovini jeste Zakon o zaštiti ličnih podataka. Ovim zakonom definisani su osnovni pojmovi i principi obrade ličnih podataka, kao i prava lica na koje se podaci odnose i obaveze institucija i organizacija koje vrše obradu podataka. Zakon definiše lične podatke kao svaku informaciju koja se odnosi na identifikovano ili identifikabilno fizičko lice, čime se uspostavlja širok obuhvat podataka koji mogu biti predmet pravne zaštite. Na taj način zakon obuhvata različite vrste identifikacionih informacija koje čine osnovu digitalnog identiteta pojedinca u savremenom informacionom okruženju [6].

Jedan od ključnih ciljeva Zakona o zaštiti ličnih podataka jeste obezbjeđivanje zakonite i transparentne obrade ličnih podataka, kao i sprečavanje njihove zloupotrebe. U tom smislu zakon predviđa da se lični podaci mogu prikupljati i obrađivati samo u određene, jasno definisane i zakonite svrhe, uz poštovanje principa proporcionalnosti i ograničenja obrade. Takođe se propisuje da podaci moraju biti tačni, ažurni i čuvani samo onoliko dugo koliko je potrebno za ostvarivanje svrhe zbog koje su prikupljeni. Ovi principi u velikoj mjeri odgovaraju osnovnim principima zaštite podataka koji su razvijeni u evropskom pravnom sistemu, što ukazuje na činjenicu da je zakonodavstvo Bosne i Hercegovine u ovoj oblasti od samog početka bilo inspirisano evropskim standardima [13].

Zakon takođe predviđa određena prava za lica na koja se podaci odnose, uključujući pravo na pristup ličnim podacima, pravo na ispravku netačnih podataka i pravo na brisanje podataka koji su obrađeni suprotno zakonu. Ova prava imaju za cilj da pojedincima omoguće kontrolu nad sopstvenim ličnim podacima i da obezbijede transparentnost u radu institucija i organizacija koje vrše obradu podataka. Međutim, u poređenju sa savremenim evropskim standardima, posebno onima koji su uspostavljeni kroz Opštu uredbu o zaštiti podataka (GDPR), može se uočiti da određeni mehanizmi zaštite u zakonodavstvu Bosne i Hercegovine nisu u potpunosti razvijeni ili precizno regulisani [3].

Institucionalni okvir za zaštitu ličnih podataka u Bosni i Hercegovini obezbjeđuje Agencija za zaštitu ličnih podataka u Bosni i Hercegovini, koja je uspostavljena kao nezavisno nadzorno tijelo nadležno za praćenje primjene zakona i zaštitu prava građana u vezi sa obradom ličnih podataka. Agencija ima ovlašćenja da vrši nadzor nad institucijama i organizacijama koje obrađuju lične podatke, da izdaje preporuke i smjernice za pravilnu primjenu zakona, kao i da pokreće postupke u slučajevima kada se utvrdi da je došlo do povrede propisa o zaštiti podataka. Na taj način Agencija predstavlja centralni institucionalni mehanizam za sprovođenje politike zaštite privatnosti u Bosni i Hercegovini [16]. U praksi, međutim, implementacija pravila o zaštiti podataka u Bosni i Hercegovini suočava se sa određenim izazovima. Jedan od ključnih problema odnosi se na ograničene institucionalne kapacitete nadzornih organa, kao i na nedovoljnu svjest institucija i organizacija o značaju zaštite ličnih podataka. Pored toga, ubrzani razvoj digitalnih tehnologija i povećana upotreba informacionih sistema u javnom i privatnom sektoru doveli su do pojave novih izazova koji nisu u potpunosti obuhvaćeni postojećim zakonodavnim okvirom. Ovi izazovi posebno dolaze do izražaja u kontekstu razvoja sistema elektronske identifikacije, biometrijskih tehnologija i različitih digitalnih platformi koje obrađuju velike količine ličnih podataka [7].

Poseban aspekt razvoja digitalnog identiteta u Bosni i Hercegovini odnosi se na digitalizaciju javne uprave i uvođenje elektronskih usluga koje građanima omogućavaju komunikaciju sa institucijama putem interneta. Razvoj elektronske uprave zahtijeva uspostavljanje pouzdanih sistema identifikacije korisnika, kako bi se obezbijedila bezbjedna razmjena informacija i zaštita osetljivih podataka. Međutim, za razliku od Evropske unije, gdje je kroz uredbu eIDAS uspostavljen jedinstven pravni okvir za elektronsku identifikaciju i usluge povjerenja, Bosna i Hercegovina još uvijek nema potpuno razvijen sistem digitalne identifikacije koji bi bio usklađen sa evropskim standardima [5].

Proces usklađivanja zakonodavstva Bosne i Hercegovine sa pravnim tekovinama Evropske unije predstavlja važan korak ka unapređenju zaštite ličnih podataka i regulacije digitalnog identiteta. Evropska komisija u svojim izvještajima o napretku Bosne i Hercegovine redovno naglašava potrebu modernizacije zakonodavnog okvira u oblasti zaštite podataka, posebno u cilju njegovog usklađivanja sa standardima GDPR-a. Takva reforma podrazumijevala bi uvođenje preciznijih pravila o obradi podataka, jačanje prava pojedinaca i unapređenje institucionalnih mehanizama nadzora nad primjenom propisa [17].

Pravni okvir zaštite ličnih podataka u Bosni i Hercegovini predstavlja važan temelj za regulaciju digitalnog identiteta, ali da je njegovo dalje unapređenje neophodno kako bi se odgovorilo na izazove savremenog digitalnog društva. Dalji razvoj zakonodavstva u ovoj oblasti trebalo bi da bude usmjeren ka usklađivanju sa evropskim standardima, jačanju institucionalnih kapaciteta nadzornih organa i unapređenju pravne sigurnosti u oblasti obrade ličnih podataka.

V. KOMPARATIVNA ANALIZA PRAVNE REGULATIVE DIGITALNOG IDENTITETA U EVROPSKOJ UNIJI I BOSNI I HERCEGOVINI

Komparativna analiza pravne regulative digitalnog identiteta i zaštite ličnih podataka u Evropskoj uniji i Bosni i Hercegovini omogućava uvid u stepen razvijenosti regulatornih sistema i nivo usklađenosti nacionalnog zakonodavstva sa evropskim standardima. Evropska unija je tokom poslednjih decenija razvila sveobuhvatan pravni okvir koji uređuje obradu ličnih podataka i sisteme digitalne identifikacije, dok je Bosna i Hercegovina u ovoj oblasti uspostavila osnovne pravne mehanizme, ali se i dalje nalazi u procesu prilagođavanja savremenim regulatornim trendovima. Upravo zbog toga poređenje ova dva sistema omogućava identifikovanje ključnih sličnosti, ali i značajnih razlika koje proizlaze iz različitog nivoa institucionalnog i normativnog razvoja [11].

Jedna od osnovnih sličnosti između pravnog sistema Evropske unije i zakonodavstva Bosne i Hercegovine ogleda se u činjenici da oba sistema polaze od principa zaštite privatnosti i ličnih podataka kao osnovnog prava pojedinca. Evropski pravni okvir prepoznaje zaštitu ličnih podataka kao fundamentalno pravo, što je potvrđeno i u Povelji Evropske unije o osnovnim pravima [12], dok zakonodavstvo Bosne i Hercegovine takođe predviđa niz mehanizama koji imaju za cilj zaštitu ličnih podataka i sprečavanje njihove zloupotrebe [6]. U oba sistema naglašava se značaj zakonite i transparentne obrade podataka, kao i potreba za postojanjem nezavisnog nadzornog tijela koje prati primjenu propisa u ovoj oblasti. Sličnosti između dva regulatorna sistema mogu se uočiti i u osnovnim principima obrade ličnih podataka. Principi kao što su ograničenje svrhe obrade, proporcionalnost, tačnost podataka i bezbjednost obrade predstavljaju zajedničke elemente evropskog i bosanskohercegovačkog zakonodavstva. Ovi principi imaju za cilj da obezbijede da se lični podaci obrađuju na način koji poštuje prava pojedinaca i sprečava njihovu neovlašćenu upotrebu. Međutim, iako su ovi principi formalno prisutni u oba pravna sistema, njihov nivo razrađenosti i praktične primjene značajno se razlikuje [3].

Najznačajnije razlike između regulatornih sistema Evropske unije i Bosne i Hercegovine odnose se na stepen normativne razvijenosti i institucionalne implementacije pravila o zaštiti podataka i digitalnom identitetu. Evropska unija je kroz Opštu uredbu o zaštiti podataka uspostavila detaljan i sveobuhvatan sistem regulacije koji obuhvata širok spektar pitanja povezanih sa obradom ličnih podataka, uključujući prava ispitanika, obaveze organizacija, mehanizme nadzora i sankcije za kršenje propisa [4]. Za razliku od toga, zakonodavni okvir Bosne i Hercegovine zasniva se na zakonu koji u određenim segmentima ne prati u potpunosti savremene regulatorne standarde razvijene u okviru Evropske unije.

Posebna razlika između ova dva sistema odnosi se na regulaciju digitalnog identiteta i elektronske identifikacije. Evropska unija je kroz uredbu eIDAS uspostavila jedinstven pravni okvir koji omogućava međusobno priznavanje sistema elektronske identifikacije između država članica i omogućava razvoj interoperabilnih digitalnih identitetskih sistema na nivou cijelog evropskog tržišta [5]. Ovaj sistem ima značajan uticaj na razvoj digitalne ekonomije i elektronske uprave, jer omogućava građanima i organizacijama da koriste digitalne usluge u različitim državama članicama bez potrebe za dodatnim administrativnim procedurama. U Bosni i Hercegovini, međutim, takav jedinstveni sistem digitalne identifikacije još uvijek nije u potpunosti razvijen, što predstavlja jedan od ključnih izazova u procesu digitalne transformacije javne uprave.

Razlike između regulatornih sistema mogu se uočiti i u institucionalnim kapacitetima za sprovođenje pravila o zaštiti podataka. U Evropskoj uniji postoji razvijen sistem nadzornih organa koji djeluju na nacionalnom i evropskom nivou, pri čemu Evropski odbor za zaštitu podataka ima važnu ulogu u koordinaciji i usklađivanju prakse između država članica [15]. Ovakav institucionalni okvir omogućava dosljednu primjenu pravila o zaštiti podataka i efikasno rješavanje sporova koji se odnose na obradu ličnih podataka. U Bosni i Hercegovini nadzor nad primjenom zakona vrši Agencija za zaštitu ličnih podataka, ali njeni kapaciteti i nadležnosti nisu uvijek uporedivi sa institucijama koje djeluju u okviru sistema Evropske unije [16]. Uprkos navedenim razlikama, proces evropskih integracija predstavlja važan podsticaj za dalji razvoj zakonodavstva Bosne i Hercegovine u oblasti zaštite ličnih podataka i digitalnog identiteta. Evropska unija kroz svoje politike i preporuke podstiče države koje teže članstvu da modernizuju svoje zakonodavne okvire i usklade ih sa evropskim standardima. U tom kontekstu reforma zakonodavstva Bosne i Hercegovine u oblasti zaštite podataka predstavlja važan korak ka unapređenju pravne sigurnosti i jačanju poverenja građana u digitalne sisteme [17].

Komparativna analiza pokazuje da, iako postoje određene sličnosti između evropskog i bosanskohercegovačkog pravnog okvira, razlike u stepenu normativne razvijenosti i institucionalne implementacije i dalje predstavljaju značajan izazov. Dalje usklađivanje zakonodavstva Bosne i Hercegovine sa standardima Evropske unije može doprinijeti unapređenju zaštite ličnih podataka, razvoju digitalne ekonomije i jačanju institucionalnih kapaciteta za regulaciju digitalnog identiteta u savremenom društvu.

VI. ZAKLJUČAK

Razvoj digitalnih tehnologija i sve intenzivnija digitalizacija društvenih i ekonomskih aktivnosti doveli su do značajnog povećanja uloge digitalnog identiteta u savremenom društvu. Digitalni identitet danas predstavlja ključni element funkcionisanja brojnih elektronskih usluga, uključujući elektronsku upravu, elektronsku trgovinu, finansijske servise i različite digitalne platforme. Istovremeno, upotreba digitalnih identiteta podrazumijeva obradu velikog broja ličnih podataka, što nameće potrebu za postojanjem jasnog i efikasnog pravnog okvira koji može obezbijediti zaštitu privatnosti i osnovnih prava pojedinaca. Upravo zbog toga pravna regulacija digitalnog identiteta i zaštite ličnih

podataka postaje jedno od ključnih pitanja savremenog informacionog prava.

Analiza pravnog okvira Evropske unije pokazuje da je u ovom regionu razvijen sveobuhvatan sistem regulacije koji obuhvata različite aspekte obrade ličnih podataka i digitalne identifikacije. Poseban značaj u tom pogledu imaju Opšta uredba o zaštiti podataka (GDPR) i uredba eIDAS, koje zajedno čine temelj evropskog regulatornog sistema u oblasti zaštite podataka i digitalnog identiteta. Ovi pravni instrumenti uspostavljaju jasna pravila o obradi ličnih podataka, definišu prava pojedinaca i obaveze organizacija koje obrađuju podatke, kao i mehanizme nadzora i sankcionisanja u slučaju kršenja propisa. Na taj način Evropska unija nastoji da obezbijedi visok nivo zaštite privatnosti, ali i da istovremeno omogući razvoj digitalne ekonomije i jedinstvenog digitalnog tržišta.

Sa druge strane, pravni okvir Bosne i Hercegovine u oblasti zaštite ličnih podataka zasniva se prvenstveno na Zakonu o zaštiti ličnih podataka, kojim su definisani osnovni principi obrade podataka i institucionalni mehanizmi za nadzor nad njihovom primjenom. Iako zakonodavstvo Bosne i Hercegovine sadrži određene elemente koji su usklađeni sa evropskim standardima, analiza pokazuje da postoje značajne razlike u stepenu normativne razrađenosti i institucionalne implementacije pravila o zaštiti podataka. Posebno se može uočiti da postojeći zakonodavni okvir nije u potpunosti prilagođen savremenim tehnološkim izazovima koji proizlaze iz razvoja digitalnih identitetskih sistema, elektronske identifikacije i obrade velikih količina podataka u digitalnom okruženju.

Komparativna analiza pravne regulative Evropske unije i Bosne i Hercegovine ukazuje na to da evropski pravni sistem predstavlja znatno razvijeniji model regulacije zaštite podataka i digitalnog identiteta. Evropska unija je kroz GDPR i eIDAS uspostavila detaljan i harmonizovan regulatorni okvir koji omogućava efikasnu zaštitu ličnih podataka i razvoj interoperabilnih sistema digitalne identifikacije na nivou cijelog unutrašnjeg tržišta. Nasuprot tome, Bosna i Hercegovina se i dalje nalazi u procesu modernizacije svog zakonodavstva i usklađivanja sa evropskim standardima, što predstavlja važan dio šireg procesa evropskih integracija.

Dalje unapređenje pravnog okvira u Bosni i Hercegovini zahtijeva modernizaciju zakonodavstva u oblasti zaštite ličnih podataka, posebno kroz usklađivanje sa standardima koje je uspostavila Opšta uredba o zaštiti podataka Evropske unije. Takva reforma mogla bi doprinijeti jačanju pravne sigurnosti, unapređenju zaštite prava građana i razvoju digitalnih javnih usluga. Pored toga, važno je unaprijediti institucionalne kapacitete nadzornih organa i podići nivo svijesti institucija i organizacija o značaju zaštite ličnih podataka u savremenom digitalnom društvu.

Na osnovu sprovedene analize može se zaključiti da digitalni identitet predstavlja jedan od ključnih elemenata savremenog informacionog društva i da njegovo efikasno pravno regulisanje zahtijeva uspostavljanje uravnoteženog sistema koji istovremeno podstiče tehnološki razvoj i obezbjeđuje zaštitu osnovnih prava pojedinaca. U tom kontekstu iskustvo Evropske unije može poslužiti kao važan model za dalji razvoj zakonodavstva Bosne i Hercegovine, posebno u oblasti zaštite ličnih podataka i digitalne identifikacije, čime bi se doprinijelo stvaranju sigurnijeg i transparentnijeg digitalnog okruženja za građane i institucije.

LITERATURA

[1] C. J. Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge, MA, USA: MIT Press, 2008.

[2] D. Birch, *Identity is the New Money*. London, UK: London Publishing Partnership, 2014.

[3] P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham, Switzerland: Springer, 2017.

[4] European Parliament and Council of the European Union, Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR), Official Journal of the European Union, 2016.

[5] European Parliament and Council of the European Union, Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS), Official Journal of the European Union, 2014.

[6] Parliamentary Assembly of Bosnia and Herzegovina, Law on Personal Data Protection of Bosnia and Herzegovina, Official Gazette of Bosnia and Herzegovina, No. 12/25.

[7] OECD, *Digital Identity Management: Enabling Innovation and Trust in the Internet* Economy. Paris, France: OECD Publishing, 2011.

[8] W. Jansen and S. Broderick, *Guidelines on Identity Management*. Gaithersburg, MD, USA: National Institute of Standards and Technology (NIST), 2011.

[9] European Commission, A Digital Single Market Strategy for Europe. Brussels, Belgium: European Commission, 2015.

[10] Tobin and D. Reed, *The Inevitable Rise of Self-Sovereign Identity*. Sovrin Foundation, 2017.

[11] L. A. Bygrave, *Data Privacy Law: An International Perspective*. Oxford, UK: Oxford University Press, 2014.

[12] European Union, Charter of Fundamental Rights of the European Union, Official Journal of the European Union, 2012.

[13] European Parliament and Council of the European Union, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities, 1995.

[14] K. Kotsoglou and M. Oswald, "Trust, but Verify: The eIDAS Regulation and the Future of Electronic Identification in Europe," *Computer Law & Security Review*, vol. 34, no. 2, pp. 394–402, 2018.

[15] European Data Protection Board, *Annual Report 2022.* Brussels, Belgium: European Data Protection Board, 2023.

[16] Agency for Personal Data Protection in Bosnia and Herzegovina, *Annual Report on Personal Data Protection*. Sarajevo, Bosnia and Herzegovina.

[17] European Commission, *Bosnia and Herzegovina 2023 Report*. Brussels, Belgium: European Commission, 2023.

UDK 174.4:[65.012.4:007.52(497.6)
DOI 10.7251/ZRSNG2526097B

Etika u primjeni AI sistema u poslovanju

Ethics in the application of AI systems in business

Pantelija Božić, Univerzitet Sinergija, Bijeljina

***Sažetak* – U radu se analizira problematika etike u primjeni vještačke inteligencije u poslovanju, sa posebnim osvrtom na pravne i regulatorne izazove koji proizlaze iz sve šire upotrebe algoritamskih sistema u donošenju poslovnih odluka. Polazeći od činjenice da AI tehnologije imaju značajan transformativni potencijal u savremenoj ekonomiji, rad istražuje na koji način njihova primjena utiče na temeljne principe odgovornog poslovanja, uključujući transparentnost, pravičnost, odgovornost i zaštitu privatnosti. Kroz interdisciplinarni pristup koji objedinjuje teorijske uvide iz oblasti vještačke inteligencije, etike i prava, razmatraju se ključni rizici, kao što su algoritamska pristrasnost, nedostatak objašnjivosti i pravna neizvjesnost u pogledu odgovornosti za odluke koje donose autonomni sistemi. Poseban fokus rada stavljen je na analizu postojećih pravnih okvira, uključujući Opštu uredbu o zaštiti podataka (GDPR) i prijedlog Akta o vještačkoj inteligenciji Evropske unije, uz kritičko sagledavanje njihove primjenjivosti u poslovnom kontekstu. Takođe, razmatra se uloga korporativne društvene odgovornosti i ESG standarda u oblikovanju etičke primjene AI sistema, pri čemu se naglašava potreba za integracijom etičkih principa u poslovne strategije i procese odlučivanja. Na osnovu sprovedene analize, rad identifikuje ključne izazove i nudi preporuke za unapređenje pravnog i etičkog okvira, uključujući razvoj regulatornih modela zasnovanih na procjeni rizika, jačanje mehanizama odgovornosti i unapređenje transparentnosti algoritamskih sistema. Rad ukazuje na to da održiva i odgovorna primjena vještačke inteligencije u poslovanju zahtijeva uspostavljanje ravnoteže između tehnološkog razvoja i zaštite osnovnih društvenih vrijednosti, pri čemu je neophodna kontinuirana saradnja između zakonodavaca, poslovnih subjekata i akademske zajednice.**

***Ključne reči* – vještačka inteligencija, etika, odgovorno poslovanje, pravna regulacija**

Abstract – The paper analyzes the issue of ethics in the application of artificial intelligence in business, with a special focus on the legal and regulatory challenges arising from the increasingly widespread use of algorithmic systems in making business decisions. Starting from the fact that AI technologies have a significant transformative potential in the modern economy, the paper investigates how their application affects the fundamental principles of responsible business, including transparency, fairness, accountability and privacy protection. Through an interdisciplinary approach that brings together theoretical insights from the fields of artificial intelligence, ethics, and law, key risks, such as algorithmic bias, lack of explainability, and legal uncertainty regarding responsibility for decisions made by autonomous systems are discussed. A special focus of the work is on the analysis of existing legal frameworks, including the General Data Protection Regulation (GDPR) and the proposal of the Act on Artificial Intelligence of the European Union, with a critical view of their applicability in the business context. Also, the role of corporate social responsibility and ESG standards in shaping the ethical application of AI systems is discussed, emphasizing the need to integrate ethical principles into business strategies and decision-making processes. Based on the analysis carried out, the paper identifies key challenges and offers recommendations for improving the legal and ethical framework, including the development of regulatory models based on risk assessment, strengthening accountability mechanisms and improving the transparency of algorithmic systems. The work indicates that the sustainable and responsible application of artificial intelligence in business requires the establishment of a balance between technological development and the protection of basic social values, whereby continuous cooperation between legislators, business entities and the academic community is necessary.

Keywords – artificial intelligence, ethics, responsible business, legal regulation

I. UVOD

U savremenim društveno-ekonomskim tokovima, obilježenim ubrzanom digitalizacijom i intenzivnim razvojem informacionih tehnologija, vještačka inteligencija (AI) zauzima centralno mjesto kao jedan od ključnih pokretača transformacije poslovnih modela, organizacionih struktura i načina donošenja odluka, pri čemu njena primjena u poslovanju više ne predstavlja pitanje izbora, već nužnosti za održavanje konkurentnosti na globalnom tržištu. Razvoj sofisticiranih algoritama, sposobnih da analiziraju velike količine podataka, predviđaju tržišne trendove i autonomno donose odluke, omogućio je kompanijama da unaprijede efikasnost, smanje troškove i optimizuju poslovne procese, ali je istovremeno otvorio niz kompleksnih pitanja koja prevazilaze tehničke i ekonomske okvire, te zadiru u sferu etike i prava [1, 4].

U kontekstu poslovne primjene, AI sistemi se koriste u različitim segmentima, uključujući upravljanje ljudskim resursima, finansijsku analitiku, marketing, logistiku i korisničku podršku, pri čemu njihova sposobnost da automatizuju procese i generišu preporuke na osnovu podataka značajno utiče na način na koji se donose odluke unutar organizacija. Međutim, upravo ta autonomija i kompleksnost

algoritamskih sistema dovode do problema transparentnosti, odgovornosti i potencijalne diskriminacije, posebno u situacijama kada odluke koje proizvodi AI imaju direktan uticaj na prava i interese pojedinaca, kao što su zapošljavanje, kreditno ocjenjivanje ili pristup određenim uslugama [5, 13]. Na taj način, pitanje etike u primjeni AI sistema postaje ne samo teorijsko, već i praktično pitanje od suštinskog značaja za održivo i odgovorno poslovanje.

Etika u kontekstu vještačke inteligencije podrazumijeva skup principa i vrijednosti koji usmjeravaju razvoj i primjenu tehnologije na način koji je usklađen sa temeljnim društvenim normama, uključujući poštovanje ljudskog dostojanstva, pravičnost, transparentnost i odgovornost. U tom smislu, brojni međunarodni i regionalni akteri razvili su smjernice i principe za tzv. „pouzdanu AI“, među kojima se posebno izdvajaju smjernice Evropske komisije, koje naglašavaju potrebu za zakonitom, etičkom i robusnom primjenom AI sistema [2]. Ipak, i pored postojanja takvih normativnih okvira, njihova implementacija u praksi ostaje izazovna, naročito zbog brzine tehnološkog razvoja koja često nadmašuje sposobnost zakonodavnih sistema da adekvatno odgovore na nove rizike.

Sa pravnog aspekta, primjena AI sistema u poslovanju otvara niz pitanja koja se odnose na odgovornost za štetu prouzrokovanu autonomnim sistemima, zaštitu ličnih podataka, kao i na regulaciju algoritamskog odlučivanja, pri čemu postojeći pravni okviri, iako djelimično primjenjivi, često nisu dovoljno precizni da obuhvate specifičnosti koje proizlaze iz upotrebe vještačke inteligencije. Na primjer, Opšta uredba o zaštiti podataka (GDPR) uvodi određene mehanizme zaštite u kontekstu automatizovanog donošenja odluka, ali ne pruža sveobuhvatno rješenje za širi spektar problema koji se javljaju u vezi sa AI sistemima [8]. S druge strane, inicijative poput prijedloga Akta o vještačkoj inteligenciji Evropske unije nastoje uspostaviti sveobuhvatan regulatorni okvir, ali se njihova konačna implementacija i praktični efekti tek trebaju sagledati [9].

Polazeći od navedenog, osnovni problem istraživanja ovog rada ogleda se u potrebi da se analizira na koji način etički principi i pravni okviri mogu efikasno odgovoriti na izazove koje donosi primjena AI sistema u poslovanju, te kako se može osigurati da upotreba ovih tehnologija bude u funkciji odgovornog i održivog razvoja. Cilj rada je da kroz interdisciplinarni pristup, koji obuhvata elemente prava, etike i poslovnih studija, identifikuje ključne rizike i izazove, te ponudi preporuke za unapređenje normativnog i praktičnog okvira za primjenu AI sistema. Metodološki pristup rada zasniva se na analizi relevantne naučne i stručne literature, kao i važećih pravnih dokumenata i međunarodnih smjernica, uz korištenje deskriptivne, komparativne i normativne metode, čime se nastoji obezbijediti sveobuhvatno sagledavanje predmetne problematike. Poseban akcenat stavljen je na analizu evropskog regulatornog pristupa, imajući u vidu njegov značaj i potencijalni uticaj na zemlje regiona, uključujući Bosnu i Hercegovinu. Struktura rada koncipirana je na način da se u narednom poglavlju razmatra teorijski okvir vještačke inteligencije i njene primjene u poslovanju, nakon čega slijedi detaljna analiza etičkih aspekata i pravnih izazova, te razmatranje koncepta odgovornog poslovanja u kontekstu AI, dok se u završnim dijelovima rada daju preporuke i zaključna razmatranja.

II. TEORIJSKI OKVIR: VJEŠTAČKA INTELIGENCIJA I POSLOVANJE

Vještačka inteligencija, kao interdisciplinarno područje koje obuhvata elemente računarstva, matematike, kognitivnih nauka i statistike, predstavlja skup tehnologija i metoda koje omogućavaju mašinama da simuliraju određene aspekte ljudske inteligencije, uključujući učenje, zaključivanje, prepoznavanje obrazaca i donošenje odluka, pri čemu savremeni razvoj ovog polja karakteriše prelazak sa simboličkih sistema na modele zasnovane na obradi velikih količina podataka i algoritmima mašinskog učenja [1]. U tom kontekstu, posebno se ističe razvoj dubokog učenja kao podgrane mašinskog učenja, koja koristi višeslojne neuronske mreže za analizu kompleksnih skupova podataka, čime se značajno unapređuju performanse sistema u zadacima kao što su prepoznavanje slike, obrada prirodnog jezika i prediktivna analitika.

Sa aspekta klasifikacije, AI sistemi se mogu posmatrati kroz više dimenzija, uključujući nivo autonomije, svrhu i način primjene, pri čemu se najčešće razlikuju uski (narrow) AI sistemi, koji su dizajnirani za obavljanje specifičnih zadataka, i opšti (general) AI, koji bi hipotetički mogao izvršavati širok spektar intelektualnih aktivnosti na nivou sličnom ljudskom. U poslovnom kontekstu, dominantnu primjenu imaju upravo uski AI sistemi, koji su optimizovani za konkretne funkcije, kao što su analiza tržišta, optimizacija lanca snabdijevanja ili personalizacija korisničkog iskustva, što omogućava organizacijama da ciljano unaprijede određene segmente svog poslovanja bez potrebe za razvojem sveobuhvatnih inteligentnih sistema [5].

Primjena vještačke inteligencije u poslovanju ogleda se u njenoj integraciji u ključne operativne i strateške procese, pri čemu AI tehnologije omogućavaju automatizaciju rutinskih zadataka, unapređenje donošenja odluka kroz analizu podataka u realnom vremenu, kao i razvoj novih proizvoda i usluga zasnovanih na digitalnim inovacijama. U oblasti upravljanja ljudskim resursima, AI sistemi se koriste za selekciju kandidata, analizu performansi zaposlenih i predviđanje potreba za radnom snagom, dok u finansijskom sektoru omogućavaju detekciju prevara, procjenu kreditnog rizika i automatizovano trgovanje, čime se povećava preciznost i brzina poslovnih operacija [5]. Istovremeno, u marketingu i prodaji, algoritmi mašinskog učenja koriste se za segmentaciju tržišta, personalizaciju ponude i optimizaciju komunikacije sa korisnicima, što doprinosi povećanju zadovoljstva potrošača i konkurentske prednosti kompanija.

Međutim, iako primjena AI sistema donosi značajne ekonomske koristi, ona istovremeno mijenja prirodu poslovanja i odnosa između organizacija i njihovih zainteresovanih strana, uključujući zaposlene, korisnike i širu

društvenu zajednicu, čime se otvaraju pitanja koja se odnose na transparentnost, odgovornost i pravičnost u donošenju odluka. Naime, algoritamski sistemi, posebno oni zasnovani na kompleksnim modelima dubokog učenja, često funkcionišu kao tzv. „crne kutije“, čiji su unutrašnji mehanizmi teško razumljivi čak i njihovim kreatorima, što otežava objašnjenje i opravdanje odluka koje takvi sistemi donose [10]. Ova karakteristika ima posebnu težinu u poslovnom kontekstu, gdje odluke zasnovane na AI mogu imati direktne posljedice na prava pojedinaca, kao što su pristup zaposlenju ili finansijskim uslugama.

Dodatno, transformacija poslovnih modela usljed primjene vještačke inteligencije ogleda se i u promjeni strukture tržišta rada, pri čemu automatizacija određenih poslova dovodi do smanjenja potražnje za određenim vrstama radne snage, dok istovremeno stvara potrebu za novim vještinama i kompetencijama, posebno u oblasti upravljanja podacima i razvoja tehnologija [4]. Ovaj proces, iako potencijalno koristan u smislu povećanja produktivnosti i ekonomskog rasta, može imati i negativne društvene posljedice, uključujući povećanje nejednakosti i nesigurnosti zaposlenja, što dodatno naglašava potrebu za odgovornim pristupom u implementaciji AI sistema. U tom smislu, savremeni pristupi razvoju i primjeni vještačke inteligencije sve više naglašavaju koncept tzv. „odgovorne AI“, koji podrazumijeva integraciju etičkih principa i društvenih vrijednosti u sve faze životnog ciklusa AI sistema, od dizajna i razvoja do implementacije i nadzora. Ovaj koncept zahtijeva interdisciplinarni pristup koji uključuje saradnju stručnjaka iz oblasti tehnologije, prava, etike i poslovanja, kako bi se obezbijedilo da AI sistemi ne samo da budu efikasni, već i usklađeni sa normativnim očekivanjima društva [7]. Polazeći od navedenog, može se zaključiti da vještačka inteligencija predstavlja moćan alat za unapređenje poslovanja, ali da njena primjena istovremeno nosi sa sobom niz izazova koji zahtijevaju pažljivo razmatranje, posebno u kontekstu etičkih i pravnih implikacija.

III. ETIČKI ASPEKTI PRIMJENE AI SISTEMA U POSLOVANJU

Razvoj i sve intenzivnija primjena vještačke inteligencije u poslovanju, iako nesumnjivo donose značajne prednosti u pogledu efikasnosti, inovacija i konkurentnosti, istovremeno otvaraju složena etička pitanja koja zahtijevaju sistematičnu analizu i normativno utemeljenje, posebno imajući u vidu činjenicu da AI sistemi sve češće učestvuju u procesima donošenja odluka koje imaju direktan i često dugoročan uticaj na pojedince i društvo u cjelini. U tom kontekstu, etički aspekti primjene AI ne mogu se posmatrati izolovano od poslovnog okruženja u kojem se takvi sistemi koriste, već zahtijevaju integrisani pristup koji obuhvata tehnološke, pravne i društvene dimenzije [6].

Jedno od centralnih etičkih pitanja odnosi se na transparentnost i objašnjivost AI sistema, posebno u situacijama kada se odluke donose na osnovu složenih algoritama čiji su unutrašnji mehanizmi teško razumljivi, što dovodi do pojave tzv. „crnih kutija“. Nedostatak transparentnosti može značajno otežati identifikaciju grešaka, pristrasnosti ili nepredviđenih posljedica u radu sistema, ali i onemogućiti pogođenim pojedincima da razumiju osnovu odluka koje se na njih odnose, što predstavlja ozbiljan izazov sa aspekta pravičnosti i odgovornosti [10]. U poslovnom kontekstu, ovo pitanje je posebno izraženo u oblastima kao što su zapošljavanje ili finansijske usluge, gdje algoritamske odluke mogu imati presudan uticaj na životne prilike pojedinaca.

Usko povezano sa pitanjem transparentnosti jeste i pitanje odgovornosti za odluke koje donose AI sistemi, pri čemu se postavlja dilema o tome ko snosi odgovornost u slučaju nastanka štete ili nepravde, odnosno da li je to proizvođač sistema, organizacija koja ga koristi ili sam korisnik. Tradicionalni pravni koncepti odgovornosti, koji su zasnovani na pretpostavci ljudskog djelovanja i kontrole, suočavaju se sa izazovima u kontekstu autonomnih sistema koji djeluju na osnovu unaprijed definisanih algoritama i podataka, ali mogu generisati ishode koji nisu direktno predvidivi od strane njihovih kreatora [7]. Ova situacija zahtijeva redefinisanje postojećih normativnih okvira kako bi se osigurala adekvatna raspodjela odgovornosti i zaštita prava pogođenih lica.

Još jedan značajan etički problem odnosi se na algoritamsku pristrasnost i diskriminaciju, koja može nastati kao posljedica korištenja neadekvatnih ili neuravnoteženih skupova podataka za treniranje AI sistema, što dovodi do reprodukcije i čak produbljivanja postojećih društvenih nejednakosti. Na primjer, sistemi za selekciju kandidata koji se oslanjaju na istorijske podatke mogu favorizovati određene grupe kandidata na osnovu prethodnih obrazaca zapošljavanja, čime se perpetuiraju diskriminatorne prakse, iako takvi ishodi nisu nužno rezultat namjerne diskriminacije [13]. U tom smislu, etička odgovornost organizacija podrazumijeva aktivno prepoznavanje i ublažavanje potencijalnih pristrasnosti kroz odgovarajuće dizajnerske i kontrolne mehanizme.

Zaštita privatnosti i podataka predstavlja još jedan ključni aspekt etike u primjeni AI sistema, posebno imajući u vidu da ovi sistemi često zahtijevaju pristup velikim količinama ličnih i osjetljivih podataka kako bi ostvarili optimalne performanse. Iako takva obrada podataka može doprinijeti unapređenju poslovnih procesa i korisničkog iskustva, ona istovremeno nosi rizik od zloupotrebe, neovlaštenog pristupa ili neadekvatne zaštite podataka, što može imati ozbiljne posljedice po prava pojedinaca. U tom kontekstu, etički pristup podrazumijeva ne samo formalno poštovanje pravnih normi, već i proaktivno usvajanje principa minimizacije podataka, sigurnosti i transparentnosti u njihovoj obradi [2]. Pored navedenog, primjena AI sistema u poslovanju ima i šire društvene implikacije, uključujući uticaj na tržište rada, raspodjelu moći i ekonomsku nejednakost, pri čemu automatizacija i digitalizacija mogu dovesti do gubitka određenih radnih mjesta, ali i stvaranja novih, što zahtijeva prilagođavanje obrazovnih i ekonomskih politika. Etika u ovom kontekstu podrazumijeva odgovornost poslovnih subjekata da razmotre šire posljedice svojih tehnoloških

odluka i da doprinesu razvoju inkluzivnih i održivih ekonomskih modela [6].

U savremenim normativnim pristupima, etički principi za razvoj i primjenu AI sistema često se formulišu kroz skup osnovnih vrijednosti, među kojima se najčešće ističu pravičnost, transparentnost, odgovornost, sigurnost i poštovanje ljudskih prava, pri čemu njihova implementacija zahtijeva konkretne mjere i mehanizme nadzora. Međutim, izazov se ogleda u tome što ovi principi, iako široko prihvaćeni na deklarativnom nivou, često ostaju nedovoljno operacionalizovani u praksi, što ograničava njihovu stvarnu efikasnost [7]. Etički aspekti primjene AI sistema u poslovanju predstavljaju kompleksno i višedimenzionalno pitanje koje zahtijeva kontinuiranu pažnju i prilagođavanje, kako bi se obezbijedilo da tehnološki napredak bude u skladu sa temeljnim društvenim vrijednostima i principima odgovornog poslovanja, što ujedno predstavlja i osnovu za dalje razmatranje pravnih okvira i regulatornih mehanizama.

IV. PRAVNI OKVIR I REGULACIJA AI SISTEMA

Ubrzan razvoj i implementacija vještačke inteligencije u poslovnom okruženju neminovno su doveli do potrebe za uspostavljanjem adekvatnog pravnog okvira koji bi omogućio kontrolu rizika, zaštitu osnovnih prava i pravnu sigurnost svih učesnika u pravnom prometu, pri čemu se poseban izazov ogleda u činjenici da tehnološki napredak u ovoj oblasti često nadmašuje brzinu zakonodavnih procesa, stvarajući normativne praznine i pravnu neizvjesnost. U tom kontekstu, pravna regulacija AI sistema ne predstavlja samo pitanje tehničkog normiranja, već zahtijeva dublje promišljanje o prilagođavanju postojećih pravnih instituta novim oblicima društvenih odnosa koji proizlaze iz primjene autonomnih i poluautonomnih sistema [10].

Jedan od ključnih aspekata pravnog okvira odnosi se na zaštitu ličnih podataka, s obzirom na to da većina AI sistema funkcioniše na osnovu obrade velikih količina podataka, uključujući i podatke koji se odnose na identifikovane ili identifikabilne pojedince. U tom smislu, Opšta uredba o zaštiti podataka (GDPR) predstavlja temeljni pravni instrument na nivou Evropske unije, koji uvodi niz principa relevantnih za primjenu AI sistema, uključujući zakonitost, pravičnost i transparentnost obrade, ograničenje svrhe, minimizaciju podataka i odgovornost rukovalaca podacima [8]. Posebno je značajna odredba koja se odnosi na automatizovano donošenje odluka, uključujući profilisanje, kojom se pojedincima priznaje pravo da ne budu predmet odluka zasnovanih isključivo na automatizovanoj obradi, ukoliko takve odluke proizvode pravne ili slične značajne posljedice po njih, osim u jasno definisanim izuzecima. Ova norma ima direktnu implikaciju na poslovne subjekte koji koriste AI sisteme u procesima odlučivanja, jer nameće obavezu obezbjeđivanja određenog stepena ljudske intervencije i mogućnosti osporavanja odluka.

Međutim, iako GDPR pruža važan okvir za zaštitu podataka u kontekstu AI, njegova primjena nije uvijek dovoljna da obuhvati sve specifične izazove koje donose savremeni algoritamski sistemi, posebno u pogledu transparentnosti i objašnjivosti kompleksnih modela. Naime, pravo na informisanost i objašnjenje odluka, iako implicitno prisutno u određenim odredbama GDPR-a, ostaje predmet različitih tumačenja u pravnoj i akademskoj praksi, što dodatno komplikuje njegovu primjenu u konkretnim poslovnim situacijama.

U cilju prevazilaženja ovih nedostataka i uspostavljanja sveobuhvatnijeg regulatornog okvira, Evropska unija je predložila donošenje posebnog pravnog akta koji se odnosi na vještačku inteligenciju, poznatog kao Akt o vještačkoj inteligenciji (AI Act), koji predstavlja prvi pokušaj sistemske regulacije AI na globalnom nivou [9]. Ovaj prijedlog zasniva se na pristupu upravljanja rizikom, pri čemu se AI sistemi klasifikuju u više kategorija, od onih koji predstavljaju neprihvatljiv rizik i koji su zabranjeni, preko sistema visokog rizika koji podliježu strogim zahtjevima u pogledu sigurnosti, transparentnosti i nadzora, do sistema minimalnog rizika koji su predmet blaže regulacije. Poseban značaj ovog akta ogleda se u njegovoj težnji da uspostavi ravnotežu između podsticanja inovacija i zaštite osnovnih prava, što predstavlja jedno od ključnih pitanja u regulaciji AI.

Pored pitanja zaštite podataka i specifične regulacije AI, značajan pravni izazov odnosi se i na odgovornost za štetu prouzrokovanu upotrebom AI sistema, pri čemu se postavlja pitanje primjenjivosti postojećih instituta građanskog prava, kao što su odgovornost za proizvod ili odgovornost za štetu, na situacije u kojima štetu uzrokuje autonomni sistem. Tradicionalni koncepti odgovornosti, koji se zasnivaju na krivici ili objektivnoj odgovornosti, suočavaju se sa poteškoćama u kontekstu AI, s obzirom na to da je često teško utvrditi uzročnu vezu između radnje konkretnog subjekta i nastale štete, posebno kada sistem djeluje na osnovu učenja iz podataka i samostalnog prilagođavanja [7]. U tom smislu, u pravnoj teoriji i praksi sve se više razmatraju alternativni modeli odgovornosti, uključujući uvođenje posebnih režima odgovornosti za AI sisteme ili obavezno osiguranje kao mehanizam raspodjele rizika. Dodatno, pravna regulacija AI u poslovanju mora uzeti u obzir i pitanja zaštite potrošača, tržišne konkurencije i intelektualne svojine, s obzirom na to da AI sistemi mogu uticati na način na koji se proizvodi i usluge nude i distribuiraju, kao i na stvaranje novih oblika tržišne dominacije zasnovane na kontroli podataka i algoritama. U tom kontekstu, regulatorni organi suočavaju se sa izazovom prilagođavanja postojećih pravila novim tehnološkim realnostima, kako bi se spriječile zloupotrebe i obezbijedili fer uslovi poslovanja.

Kada je riječ o Bosni i Hercegovini i zemljama regiona, pravni okvir u oblasti vještačke inteligencije još uvijek je u fazi razvoja, pri čemu se u velikoj mjeri oslanja na evropske standarde i praksu, što je posebno izraženo u oblasti zaštite podataka, gdje su usvojeni zakoni koji su u određenoj mjeri usklađeni sa GDPR-om. Međutim, nedostatak specifične regulative koja se direktno odnosi na AI sisteme predstavlja izazov za pravnu sigurnost i može otežati odgovornu primjenu ovih tehnologija u poslovnom okruženju. Imajući u vidu

navedeno, jasno je da pravni okvir za regulaciju AI sistema u poslovanju mora biti dinamičan i prilagodljiv, kako bi mogao odgovoriti na brze tehnološke promjene, ali i dovoljno precizan da obezbijedi zaštitu osnovnih prava i pravnu sigurnost, što zahtijeva kontinuiranu saradnju između zakonodavaca, poslovnih subjekata i stručnjaka iz različitih oblasti. Ova pitanja posebno dolaze do izražaja u kontekstu odgovornog poslovanja, koje podrazumijeva ne samo formalno poštovanje pravnih normi, već i aktivno nastojanje da se etički principi integrišu u poslovne prakse.

V. ODGOVORNO POSLOVANJE I KORPORATIVNA ETIKA U KONTEKSTU AI

Savremeni koncept odgovornog poslovanja, koji se razvijao paralelno sa procesima globalizacije i jačanja uloge korporacija u društvu, danas dobija novu dimenziju u kontekstu primjene vještačke inteligencije, pri čemu se od poslovnih subjekata više ne očekuje isključivo ostvarivanje profita, već i aktivno upravljanje društvenim, etičkim i pravnim implikacijama tehnologija koje razvijaju i koriste. U tom smislu, integracija AI sistema u poslovne procese zahtijeva redefinisanje tradicionalnih pristupa korporativnoj etici i društvenoj odgovornosti, kako bi se obezbijedilo da tehnološke inovacije budu usklađene sa širim društvenim interesima i principima održivog razvoja [11].

Koncept korporativne društvene odgovornosti (CSR) podrazumijeva dobrovoljno uključivanje kompanija u rješavanje društvenih i ekoloških pitanja, izvan minimalnih zakonskih zahtjeva, pri čemu se u kontekstu AI ovaj koncept proširuje na odgovorno upravljanje podacima, transparentnost algoritama i zaštitu prava korisnika. Naime, kompanije koje implementiraju AI sisteme suočavaju se sa potrebom da razviju interne politike i procedure koje će osigurati etičku upotrebu tehnologije, uključujući uspostavljanje mehanizama nadzora, procjene rizika i kontinuiranog praćenja uticaja AI na različite grupe zainteresovanih strana [7]. Ovakav pristup podrazumijeva prelazak sa reaktivnog na proaktivni model upravljanja, u kojem se potencijalni etički i pravni problemi identifikuju i adresiraju već u fazi dizajna sistema.

U posljednje vrijeme, sve veći značaj dobija i koncept ESG (Environmental, Social, Governance) standarda, koji predstavljaju okvir za procjenu održivosti i etičkog uticaja poslovanja kompanija, pri čemu primjena AI sistema direktno utiče na sve tri dimenzije ovog okvira. Sa aspekta društvene dimenzije (Social), AI može doprinijeti unapređenju usluga i pristupa informacijama, ali i generisati rizike u pogledu diskriminacije i nejednakosti, dok sa aspekta upravljanja (Governance) postavlja pitanja transparentnosti, odgovornosti i kontrole nad algoritamskim procesima. U tom kontekstu, odgovorno poslovanje podrazumijeva integraciju AI etike u ESG strategije kompanija, čime se obezbjeđuje sistemski pristup upravljanju rizicima i uticajima tehnologije.

Pored internih mehanizama, značajnu ulogu u promociji odgovorne primjene AI imaju i međunarodne organizacije i inicijative koje razvijaju principe i standarde za etičku upotrebu tehnologije. Među njima se posebno ističu principi Organizacije za ekonomsku saradnju i razvoj (OECD), koji naglašavaju potrebu za inkluzivnim rastom, održivim razvojem i poštovanjem ljudskih prava u kontekstu AI [12]. Ovi principi, iako pravno neobavezujući, imaju značajan uticaj na oblikovanje nacionalnih politika i korporativnih praksi, te predstavljaju važan referentni okvir za kompanije koje nastoje uskladiti svoje poslovanje sa međunarodnim standardima. Međutim, implementacija principa odgovornog poslovanja u praksi suočava se sa brojnim izazovima, uključujući nedostatak jasnih smjernica za operacionalizaciju etičkih principa, ograničene resurse, kao i potencijalni sukob između ekonomskih interesa i etičkih obaveza. Naime, kompanije se često nalaze u situaciji da balansiraju između potrebe za inovacijama i konkurentnošću, s jedne strane, i zahtjeva za transparentnošću i odgovornošću, s druge strane, što može dovesti do kompromisa koji nisu uvijek u skladu sa najvišim etičkim standardima.

U tom kontekstu, pravna regulacija i etičke smjernice ne treba posmatrati kao suprotstavljene, već kao komplementarne mehanizme koji zajedno doprinose odgovornoj primjeni AI sistema. Dok pravni okvir postavlja minimalne standarde i obaveze, etički pristupi omogućavaju kompanijama da idu korak dalje i razviju poslovne modele koji su ne samo zakoniti, već i društveno prihvatljivi i održivi. Upravo ova sinergija između prava i etike predstavlja ključni element savremenog odgovornog poslovanja. Konačno, odgovorno upravljanje AI sistemima zahtijeva i razvoj odgovarajuće organizacione kulture, koja podstiče etičko razmišljanje, interdisciplinarnu saradnju i kontinuirano učenje, pri čemu posebnu ulogu imaju lideri organizacija koji svojim odlukama i primjerom oblikuju vrijednosti i standarde ponašanja unutar kompanije. U tom smislu, etika u primjeni AI ne može se svesti samo na formalne politike i procedure, već mora biti integrisana u svakodnevne poslovne prakse i odluke.

VI. IZAZOVI I RIZICI PRIMJENE AI U POSLOVANJU

Iako primjena vještačke inteligencije u poslovanju donosi brojne prednosti, uključujući povećanje efikasnosti, smanjenje operativnih troškova i unapređenje donošenja odluka, njena implementacija istovremeno otvara niz složenih izazova i rizika koji se ne mogu adekvatno adresirati isključivo tehničkim rješenjima, već zahtijevaju interdisciplinarni pristup koji obuhvata pravne, etičke i organizacione dimenzije. Ovi izazovi posebno dolaze do izražaja u kontekstu sve veće autonomije AI sistema, njihove široke primjene i potencijalno značajnog uticaja na pojedince i društvo u cjelini, što dodatno naglašava potrebu za pažljivim upravljanjem rizicima i uspostavljanjem odgovarajućih mehanizama kontrole [6].

Jedan od ključnih izazova odnosi se na problem nedostatka transparentnosti i objašnjivosti AI sistema, posebno onih zasnovanih na kompleksnim modelima mašinskog učenja, koji često funkcionišu kao „crne kutije“, čime se otežava razumijevanje načina na koji dolaze do određenih odluka. Ovaj problem ima direktne implikacije na povjerenje korisnika i legitimnost poslovnih odluka, budući da nemogućnost objašnjenja algoritamskih odluka može dovesti do percepcije

nepravičnosti i arbitrarnosti, čak i u situacijama kada sistem funkcioniše u skladu sa zadatim parametrima [10]. U poslovnoj praksi, ovo može rezultirati reputacionim rizicima, ali i pravnim sporovima, posebno kada su pogođena prava pojedinaca.

Pored toga, značajan rizik predstavlja i algoritamska pristrasnost, koja može nastati usljed korištenja neadekvatnih, nepotpunih ili historijski opterećenih podataka, što dovodi do sistematskog favorizovanja ili diskriminacije određenih grupa. Ovaj problem je posebno izražen u sektorima kao što su zapošljavanje, finansije i osiguranje, gdje AI sistemi mogu donositi odluke koje direktno utiču na socio-ekonomski status pojedinaca, pri čemu čak i nenamjerne greške u dizajnu sistema mogu imati ozbiljne posljedice [13]. Izazov se dodatno komplikuje činjenicom da pristrasnost često nije lako detektovati, posebno u kompleksnim modelima, što zahtijeva razvoj sofisticiranih metoda za njeno prepoznavanje i ublažavanje.

Sigurnosni rizici predstavljaju još jednu važnu dimenziju primjene AI sistema u poslovanju, s obzirom na to da ovi sistemi mogu biti meta različitih oblika napada, uključujući manipulaciju podacima, napade na modele i eksploataciju ranjivosti u sistemima, što može dovesti do pogrešnih odluka, gubitka podataka ili narušavanja integriteta poslovnih procesa. U tom kontekstu, osiguranje tehničke robusnosti i otpornosti AI sistema postaje ključno pitanje, koje zahtijeva kontinuirano ulaganje u sigurnosne mehanizme i razvoj standarda zaštite. Dodatno, implementacija AI sistema u poslovanju često je praćena organizacionim izazovima, uključujući nedostatak stručnog kadra, ograničene kapacitete za upravljanje kompleksnim tehnologijama, kao i otpor zaposlenih prema promjenama koje donosi automatizacija. Ovi faktori mogu značajno uticati na uspješnost implementacije AI projekata, ali i generisati dodatne rizike u pogledu neadekvatne upotrebe sistema ili pogrešnog tumačenja rezultata koje AI generiše.

Sa pravnog aspekta, značajan izazov predstavlja i fragmentiranost regulatornih okvira na globalnom nivou, pri čemu različite države i regioni razvijaju različite pristupe regulaciji AI, što može otežati poslovanje kompanija koje djeluju na međunarodnom tržištu. Ova situacija dovodi do pravne neizvjesnosti i povećava troškove usklađivanja, ali i otvara prostor za regulatorni arbitrage, gdje kompanije mogu birati jurisdikcije sa blažim pravilima, što može imati negativne posljedice po zaštitu prava i standarde poslovanja. Posebno je važno istaći i reputacione rizike koji proizlaze iz neetičke ili neodgovorne primjene AI sistema, budući da negativni slučajevi iz prakse mogu značajno narušiti povjerenje korisnika i javnosti, što se direktno odražava na poslovne rezultate kompanija. U eri digitalne transparentnosti i brzog širenja informacija, reputacioni rizici mogu imati dugoročne posljedice koje nadilaze neposredne finansijske gubitke.

Uprkos navedenim izazovima, važno je naglasiti da oni ne predstavljaju nepremostivu prepreku za primjenu AI u poslovanju, već ukazuju na potrebu za sistemskim i odgovornim pristupom koji podrazumijeva identifikaciju, procjenu i upravljanje rizicima kroz kombinaciju tehničkih, pravnih i organizacionih mjera. U tom smislu, ključni zadatak savremenih poslovnih subjekata jeste da razviju kapacitete za upravljanje kompleksnošću AI sistema, uz istovremeno poštovanje etičkih principa i pravnih normi. Polazeći od navedenog, jasno je da izazovi i rizici primjene AI sistema u poslovanju predstavljaju integralni dio procesa digitalne transformacije, te da njihovo adekvatno adresiranje zahtijeva koordinisano djelovanje različitih aktera, uključujući kompanije, zakonodavce, regulatorna tijela i akademsku zajednicu, što će u narednom poglavlju biti razmotreno kroz konkretne preporuke za unapređenje etičke i pravno usklađene primjene AI sistema.

VII. PREPORUKE ZA ETIČKU I PRAVNO USKLAĐENU PRIMJENU AI SISTEMA

Polazeći od prethodno analiziranih etičkih dilema, pravnih izazova i praktičnih rizika, jasno je da odgovorna primjena vještačke inteligencije u poslovanju zahtijeva sistemski i proaktivan pristup koji nadilazi parcijalna rješenja i fragmentirane inicijative, te podrazumijeva uspostavljanje koherentnog okvira koji integriše pravne norme, etičke principe i organizacione mehanizme upravljanja. U tom smislu, preporuke koje se iznose u ovom poglavlju imaju za cilj da ponude smjernice za unapređenje postojećih praksi i razvoj novih modela upravljanja AI sistemima koji će biti u skladu sa principima odgovornog poslovanja.

Prije svega, od ključnog značaja je uspostavljanje jasnih i preciznih regulatornih okvira koji će omogućiti pravnu sigurnost i predvidivost u primjeni AI sistema, uz istovremeno očuvanje prostora za inovacije. U tom kontekstu, pristup zasnovan na procjeni rizika, kakav je predviđen u okviru evropskog Akta o vještačkoj inteligenciji, može poslužiti kao adekvatan model za diferencijaciju regulatornih zahtjeva u zavisnosti od potencijalnog uticaja AI sistema na prava i interese pojedinaca [9]. Međutim, kako bi takav pristup bio efikasan, neophodno je obezbijediti jasne kriterijume za klasifikaciju sistema, kao i mehanizme nadzora i sankcionisanja koji će osigurati njegovu dosljednu primjenu u praksi.

Istovremeno, kompanije koje razvijaju i koriste AI sisteme treba da uspostave interne okvire upravljanja koji će omogućiti identifikaciju i ublažavanje etičkih i pravnih rizika u svim fazama životnog ciklusa sistema, od dizajna i razvoja do implementacije i evaluacije. Ovi okviri treba da obuhvate procedure procjene uticaja na prava pojedinaca, posebno u slučajevima kada se radi o sistemima visokog rizika, kao i mehanizme za osiguranje transparentnosti i objašnjivosti algoritamskih odluka. U tom smislu, primjena koncepta „etike po dizajnu“ (ethics by design) i „privatnosti po dizajnu“ (privacy by design) može značajno doprinijeti integraciji etičkih principa u tehničke aspekte razvoja AI sistema [2]. Dalje, neophodno je unaprijediti mehanizme odgovornosti i pravne zaštite u kontekstu primjene AI sistema, kako bi se obezbijedila adekvatna zaštita pojedinaca u slučajevima kada

algoritamske odluke proizvode štetne posljedice. To podrazumijeva ne samo prilagođavanje postojećih pravnih instituta, već i razmatranje uvođenja novih modela odgovornosti koji će uzeti u obzir specifičnosti autonomnih sistema, uključujući njihovu sposobnost učenja i prilagođavanja [7]. U tom kontekstu, posebnu pažnju treba posvetiti razvoju mehanizama za efikasno ostvarivanje prava na pravni lijek, uključujući mogućnost osporavanja automatizovanih odluka i pristupa relevantnim informacijama.

Pored regulatornih i pravnih mjera, od suštinskog značaja je i razvoj standarda i smjernica na međunarodnom nivou, koji će omogućiti harmonizaciju pristupa i olakšati poslovanje u globalnom okruženju. Principi Organizacije za ekonomsku saradnju i razvoj, koji naglašavaju transparentnost, odgovornost i poštovanje ljudskih prava, predstavljaju važan korak u tom pravcu, ali njihova efikasnost zavisi od spremnosti država i kompanija da ih implementiraju u konkretne politike i prakse [12]. Takođe, značajnu ulogu u unapređenju etičke primjene AI imaju edukacija i razvoj kapaciteta, kako unutar organizacija, tako i na nivou društva u cjelini. Naime, razumijevanje načina na koji AI sistemi funkcionišu, kao i njihovih potencijalnih rizika i ograničenja, ključno je za donošenje informisanih odluka i odgovorno upravljanje tehnologijom. U tom smislu, potrebno je ulagati u razvoj interdisciplinarnih znanja koja povezuju tehničke, pravne i etičke aspekte AI, čime se omogućava sveobuhvatno sagledavanje problema i razvoj adekvatnih rješenja.

Konačno, važno je naglasiti da odgovorna primjena AI sistema nije statičan cilj, već kontinuirani proces koji zahtijeva stalno praćenje, evaluaciju i prilagođavanje u skladu sa razvojem tehnologije i promjenama u društvenim očekivanjima. U tom kontekstu, kompanije i regulatorna tijela treba da uspostave mehanizme za kontinuirano praćenje uticaja AI sistema, uključujući prikupljanje povratnih informacija od korisnika i drugih zainteresovanih strana, kao i redovno ažuriranje politika i procedura. Efikasna i odgovorna primjena vještačke inteligencije u poslovanju zahtijeva koordinisano djelovanje različitih aktera, uključujući zakonodavce, poslovne subjekte, akademsku zajednicu i civilno društvo, pri čemu se ključ uspjeha nalazi u uspostavljanju ravnoteže između tehnološkog razvoja i zaštite osnovnih vrijednosti savremenog društva, što ujedno predstavlja i osnov za zaključna razmatranja koja slijede u narednom poglavlju.

VIII. ZAKLJUČAK

U savremenom poslovnom okruženju, obilježenom intenzivnom digitalnom transformacijom i sveprisutnom primjenom vještačke inteligencije, pitanje etike i pravne regulacije AI sistema nameće se kao jedno od ključnih pitanja za održivo i odgovorno poslovanje, pri čemu analiza sprovedena u ovom radu ukazuje na to da tehnološki napredak, iako donosi značajne koristi u pogledu efikasnosti, inovacija i konkurentnosti, istovremeno generiše kompleksne izazove koji zahtijevaju sistemski i interdisciplinarni pristup. Posebno se ističe činjenica da AI sistemi sve češće učestvuju u donošenju odluka koje imaju direktne implikacije na prava i interese pojedinaca, što dodatno naglašava potrebu za njihovim etičkim i pravnim utemeljenjem.

Analiza teorijskog okvira pokazala je da vještačka inteligencija, kao skup tehnologija zasnovanih na obradi podataka i algoritamskom učenju, ima transformativni potencijal u poslovanju, ali da njena primjena nije neutralna, već duboko utiče na način organizacije rada, raspodjelu resursa i odnose između različitih aktera u ekonomiji. U tom kontekstu, etički aspekti, uključujući transparentnost, odgovornost, pravičnost i zaštitu privatnosti, predstavljaju ključne elemente za procjenu prihvatljivosti i legitimnosti AI sistema, pri čemu njihova implementacija u praksi ostaje izazovna zbog kompleksnosti tehnologije i nedostatka jasnih operativnih smjernica.

Sa pravnog stanovišta, utvrđeno je da postojeći normativni okviri, iako pružaju određeni stepen zaštite, nisu u potpunosti prilagođeni specifičnostima AI sistema, posebno u pogledu pitanja odgovornosti, objašnjivosti i automatizovanog donošenja odluka. Inicijative poput evropskog Akta o vještačkoj inteligenciji predstavljaju značajan korak ka uspostavljanju sveobuhvatnog regulatornog sistema, ali njihova efikasnost zavisiće od načina implementacije i sposobnosti da odgovore na dinamične promjene u tehnološkom razvoju. U tom smislu, pravna regulacija mora biti fleksibilna, ali istovremeno dovoljno precizna da obezbijedi pravnu sigurnost i zaštitu osnovnih prava.

Dalje, razmatranje koncepta odgovornog poslovanja ukazalo je na to da etička primjena AI sistema ne može biti isključivo rezultat regulatornih zahtjeva, već zahtijeva aktivno uključivanje kompanija kroz razvoj internih politika, procedura i organizacione kulture koja promoviše odgovornost, transparentnost i poštovanje društvenih vrijednosti. Integracija etičkih principa u poslovne strategije, uključujući kroz CSR i ESG okvire, predstavlja važan korak ka uspostavljanju održivih modela poslovanja u eri digitalne ekonomije.

Identifikovani izazovi i rizici, uključujući algoritamsku pristrasnost, nedostatak transparentnosti, sigurnosne prijetnje i regulatornu fragmentiranost, dodatno potvrđuju potrebu za koordinisanim djelovanjem različitih aktera, kako bi se obezbijedila odgovorna primjena AI sistema. U tom kontekstu, preporuke iznesene u radu naglašavaju značaj kombinacije pravnih, etičkih i organizacionih mjera, uključujući razvoj regulatornih okvira zasnovanih na procjeni rizika, unapređenje mehanizama odgovornosti, kao i ulaganje u edukaciju i razvoj kapaciteta.

Budućnost primjene vještačke inteligencije u poslovanju zavisi od sposobnosti društva da uspostavi ravnotežu između tehnološkog napretka i zaštite temeljnih vrijednosti, pri čemu etika i pravo imaju ključnu ulogu u oblikovanju tog procesa. U tom smislu, dalja istraživanja treba da budu usmjerena na razvoj konkretnih modela implementacije etičkih principa i pravnih normi u praksi, kao i na praćenje efekata postojećih regulatornih inicijativa, kako bi se obezbijedio održiv i inkluzivan razvoj AI tehnologija.

LITERATURA

[1] S. Russell i P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Pearson, 2020.

[2] European Commission, "Ethics Guidelines for Trustworthy AI," 2019.

[3] N. Bostrom, *Superintelligence: Paths, Dangers, Strategies*. Oxford University Press, 2014.

[4] E. Brynjolfsson i A. McAfee, *The Second Machine Age*. W.W. Norton & Company, 2014.

[5] T. Davenport i J. Ronanki, "Artificial Intelligence for the Real World," *Harvard Business Review*, 2018.

[6] L. Floridi et al., "AI4People – An Ethical Framework for a Good AI Society," *Minds and Machines*, 2018.

[7] V. Dignum, *Responsible Artificial Intelligence*. Springer, 2019.

[8] European Parliament, "General Data Protection Regulation (GDPR)," 2016.

[9] European Commission, "Proposal for a Regulation on Artificial Intelligence (AI Act)," 2021.

[10] F. Pasquale, *The Black Box Society*. Harvard University Press, 2015.

[11] B. Carroll, "Corporate Social Responsibility: Evolution of a Definitional Construct," *Business & Society*, 1999.

[12] OECD, "OECD Principles on Artificial Intelligence," 2019.

[13] Mittelstadt et al., "The Ethics of Algorithms: Mapping the Debate," *Big Data & Society*, 2016.

UDK 811.111(100):[316.772.4:339.92
DOI 10.7251/ZRSNG2526105D

Globalni engleski i interkulturalna komunikacija: između integracije i lingvističkog imperijalizma

Global English and Intercultural Communication: Between Integration and Linguistic Imperialism

Anja Đuranović, Ekonomski fakultet Pale, Univerzitet u Istočnom Sarajevu

***Sažetak* – Ovaj rad analizira ulogu engleskog jezika kao lingua franca u savremenoj globalnoj i interkulturalnoj komunikaciji, posebno se osvrćući na tenziju koja postoji između engleskog i ostalih jezika, odnosno na njegovu integrativnu sposobnost naspram potencijalnog lingvističkog imperijalizma. U doba globalizacije i digitalizacije, engleski je postao dominantno sredstvo međunarodne komunikacije u oblastima obrazovanja, nauke, medija, mreža i ekonomije. On omogućava govornicima različitih jezika da lakše komuniciraju, globalno sarađuju i umrežavaju se. Međutim, pored integrativne uloge, brojni lingvisti ukazuju na opasnosti koje prate globalnu dominaciju engleskog jezika. Otuda se nameće koncept lingvističkog imperijalizma i pitanje jezičke hegemonije i marginalizacije ostalih jezika i kultura, naročito u digitalnom okruženju gdje se većina sadržaja plasira na engleskom jeziku. Dakle, stvara se dilema da li engleski podstiče interkulturalno razumijevanje ili podstiče homogenizaciju kulturnih obrazaca. Rad predstavlja preglednu teorijsku analizu stručne literature iz oblasti socio i primijenjene lingvistike. Cilj rada je da kritički sagleda prirodu globalnog engleskog jezika i ukaže na potrebu da se očuvaju manji jezici, a prepoznaju komunikacijske funkcije globalnog jezika.**

***Ključne riječi* – globalni engleski; interkulturalna komunikacija; lingvistički imperijalizam; digitalni svijet; jezička raznolikost.**

***Abstract* – This paper analyses the role of English as a lingua franca in contemporary global and intercultural communication, focusing in particular on the tension that exists between English and other languages, or rather on its integrative capacity in the face of potential linguistic imperialism. In the era of globalisation and digitalisation, English has become the dominant means of international communication in the fields of education, science, media, networks and economics. It allows speakers of different languages to communicate more easily and collaborate globally. Nevertheless, in addition to its integrative role, numerous linguists point to the dangers that accompany the global dominance of the English language. Hence, the concept of linguistic imperialism and the issue of linguistic hegemony and marginalisation of other languages and cultures arise, especially in the digital environment, where most content is in English. Therefore, a dilemma arises as to whether English encourages intercultural understanding or the homogenisation of cultural patterns. The paper presents a comprehensive theoretical analysis of professional literature in the field of socio- and applied linguistics. The paper critically examines the nature of global English and highlights the need to preserve smaller languages while acknowledging the communicative functions of global language.**

***Keywords* – global English; intercultural communication; linguistic imperialism; digital world; linguistic diversity.**

I. UVOD

Globalizacija, tehnologija i digitalna transformacija su u ogromnoj mjeri promijenili svijet u kojem živimo. Komunikacija preko interneta prevazilazi i geografske i političke granice, pa narodi iz različitih kultura lakše stupaju u interakcije. Nije čudo što se javila potreba da se stvori novi, zajednički jezik, da preuzme ulogu koju je latinski imao u vijekovima iza nas. Ta uloga pripala je engleskom jeziku koji je postao sredstvo međunarodne komunikacije, obrazovanja, nauke, medija i interneta. O tome kako je došlo do toga da engleski postane *lingua franca*, biće riječi u nastavku rada. Osim istorijskih okolnosti, tu poziciju dodatno su učvrstile digitalne tehnologije, s obzirom da je većina online i softverskog sadržaja na engleskom jeziku. Dakle, on postaje jezik koji nije važan samo za komunikaciju već i bitan socijalni faktor.

Upravo ta dominacija jednog jezika otvara niz pitanja koja se ne tiču samo njegove komunikacijske uloge. Javlja se dilema da li njegova upotreba doprinosi kulturnoj integraciji i razumijevanju ili pak izaziva asimetriju moći, ugnjetavanje manjih jezika i homogenizaciju društva - da li se radi o lingvističkoj raznolikosti ili lingvističkom ugnjetavanju. Takvim pitanjima bavili su se Filipson i Kristal (eng. Phillipson and Crystal), a Filipson je uveo termin *lingvistički imperijalizam* i ukazao na činjenicu da dominacija engleskog jezika predstavlja prijetnju drugim jezicima, jer održava nejednak status među jezicima, a samim tim i među državama i kulturama [1].

Cilj ovoga rada je da teorijski sagleda tu dvojaku prirodu globalnog engleskog, pa ćemo se osvrnuti i na njegove ekonomske, obrazovne i kulturne implikacije koje najčešće srećemo u medijima. Da li je engleski sredstvo integracije i povezivanja kultura ili samo instrument lingvističke dominacije u rukama velikih sila. Kroz pregled značajnih teorijskih pristupa i ideja, rad nastoji da ponudi objektivan

pogled na mjesto i ulogu engleskog jezika u modernom, digitalnom dobu.

najprije da sagledamo istorijske, političke i tehnološke okolnosti koje su dovele do njegovog globalnog širenja i sticanja statusa lingua franca (engleski kao lingua franca – ELF). Sajdlhofer navodi da se taj termin pojavio kao način označavanja komunikacije na engleskom između govornika sa različitim maternjim jezicima.[2] Svoju dominaciju ne duguje svojoj jezičkoj strukturi niti superiornosti, već složenom spletu društvenih okolnosti i globalnih političkih, kao i tehnoloških promjena.

Engleski je počeo da se širi u periodu britanske kolonijalne ekspanzije koja je svoj vrhunac imala od XVII do XIX vijeka. Na taj način engleski je stigao na mnoge kontinente, uključujući Sjevernu Ameriku, Afriku, Aziju i Australiju. Kao velika kolonijalna sila, Britanija je prodrla u obrazovne sisteme i širila se trgovačkim putevima i mrežama, postajući tada jezik elite koji su govorili viši slojevi društva. Na taj način su postavljeni temelji njegove globalne upotrebe. Od tada pa do danas njegova ekspanzija je bivala sve veća, a broj govornika rastao je iz dana u dan.

Uloga engleskog u svijetu nije slabila ni nakon svjetskih ratova, a vodeću ulogu u njegovom daljem širenju nakon Drugog svjetskog rata preuzele su Sjedinjene Američke Države, čiji su ekonomski i politički uticaj oblikovali savremeni međunarodni poredak. Razvoj ove velesile, globalne ekonomije, širenje međunarodnih organizacija i popularne kulture odredio je engleski kao dominantan jezik poslovanja, diplomatije i akademske razmjene. Razvoj međunarodnog saobraćaja i mobilnosti dodatno je učvrstio njegov status univerzalnog komunikacijskog sredstva.

Simboličku dimenziju te dominacije ilustruje citat kojim Filipson otvara svoju knjigu *English-Only Europe*:

„*Niko ne obraća pažnju na ono što govorite ukoliko ne govorite engleski, jer je engleski jezik moći*.“ (Ombudsman za ljudska prava u Bosni i Hercegovini, Gret Haller, 1999) [3]

Ova izjava jasno ukazuje na percepciju engleskog kao jezika političke i društvene moći, što prevazilazi njegovu isključivo komunikacijsku funkciju.

Naročito značajnu ulogu imao je u globalizaciji i razvoju informaciono-komunikacionih tehnologija krajem XX i početkom XXI vijeka. Internet, društvene mreže, softverska industrija razvijaju se isključivo u anglofonom okruženju, te kao rezultat imamo to da je najveći dio digitalnog sadržaja dostupan na engleskom jeziku, a poslovi vezani za programiranje su neizvodivi na bilo kom drugom jeziku.

Poznavanje engleskog postalo je ključni faktor prilikom zapošljavanja, a neophodan je i za pristup informacijama i svaki oblik profesionalne komunikacije. Lukianenko je kroz kvantitativne analize podataka sa tržišta rada ukazala da postoji snažna povezanost između jezičke kompetencije i ekonomskih prilika. Pojedinci koji tečno govore dominantne jezike, imaju bolje izglede za zaposlenje, više plate i veće

II. NASTANAK I RAZVOJ ENGLESKOG JEZIKA KAO LINGUA FRANCA

Kako bismo bolje razumjeli savremenu ulogu engleskog jezika u svijetu i interkulturalnoj komunikaciji, potrebno je

mogućnosti za napredovanje u karijeri u poređenju s onima koji govore manje zastupljene jezike. [4] Na taj način jezičke vještine postaju oblik lingvističkog kapitala, koji utiče na društvenu i ekonomsku stratifikaciju.

Upotreba engleskog jezika često prevazilazi nacionalne i kulturne identitete, produbljuje se međunarodna saradnja, razmjenjuju se znanja i povezuju se kulture. Međutim, ta njegova univerzalnost i globalna upotreba predstavljaju osnovu za strah i dalju raspravu o njegovim društvenim implikacijama i posljedicama po druge kulture i jezike, o čemu će biti govora u narednim poglavljima rada.

III. ENGLESKI KAO SREDSTVO INTERKULTURALNE KOMUNIKACIJE

U savremenom svijetu engleski jezik predstavlja most koji povezuje različite kulture i omogućava pojedincima različitog porijekla da upoznaju druge kulture, sarađuju, zajedno uče i druže se. Engleski kao lingua franca (ELF) dozvoljava komunikaciju među govornicima koji nemaju zajednički maternji jezik i tako prevazilazi jezičke i kulturne barijere koje su nekada predstavljale ozbiljnu prepreku međunarodnoj saradnji, pa čak dovodile i do ratova.

Jedno istraživanje pokazuje da je engleski najpoznatiji jezik nakon maternjih jezika, što je naročito izraženo u Švedskoj (89%), Malti (88%) i Holandiji (87%). Ukupno 51% građana EU tvrdi da može voditi razgovor na engleskom jeziku. Istraživanje takođe ukazuje na to da građani EU smatraju da govore engleski na boljem nivou nego bilo koji drugi strani jezik. Sedamdeset sedam posto građana EU vjeruje da bi njihova djeca trebalo da uče engleski jezik. Engleski se pokazao kao najpoželjniji jezik za učenje u svim zemljama u kojima je istraživanje sprovedeno, osim u Ujedinjenom Kraljevstvu, Republici Irskoj i Luksemburgu. [5]

Postoji mnogo načina da se definiše riječ kultura, pri čemu se ona ne odnosi samo na književnost, muziku i umjetnost, već na zajednički sistema stavova, uvjerenja, vrijednosti i ponašanja – jednostavno je to način na koji mi ovdje radimo stvari. Kultura se ispoljava kako u obrascima jezika i mišljenja, tako i u oblicima djelovanja i ponašanja. Ti obrasci postaju modeli za zajedničke prilagodljive postupke i stilove izražajnog ponašanja koji omogućavaju ljudima da žive u društvu, unutar određenog geografskog okruženja i na određenom stepenu tehničkog razvoja. [6] Uloga engleskoga je da prevaziđe i pomiri razlike koje postoje i uspostavi interakciju između kultura. Danas, čak i zajednice gdje engleski nije maternji usvajaju engleske riječi, fraze, izraze i načine ponašanja, što stvara mješavinu koja prati globalne trendove i utiče na lokalne tradicije. Ovo jezičko prilagođavanje olakšava međukulturnu komunikaciju i podstiče osjećaj globalne povezanosti, jer ljudi iz različitih sredina međusobno komuniciraju putem zajedničkog jezičkog medija. [7]

Jedna od prvih prednosti globalne upotrebe engleskog jezika jeste razmjena znanja. On je postao dominantan jezik u oblasti nauke i visokog obrazovanja, pa pored maternjeg jezika je engleski drugi radni jezik mnogih konferencija i časopisa. Naučnici iz različitih dijelova svijeta koriste engleski da predstave rezultate istraživanja i tako se uključe u globalne naučne tokove. Engleski stvara zajednički prostor u kojem se dijele znanja i iskustva, prevazilazi granice i nacionalne okvire globalne akademske zajednice.

Slično je i u oblasti ekonomije i poslovanja. Velike multinacionalne kompanije i međunarodne organizacije posluju na engleskom jeziku. Zajednički jezik na tržištu rada olakšava sklapanje ugovora i mobilnost osoblja, te doprinosi saradnji između partnera iz različitih zemalja. Bolje jezičke vještine govora, pisanja i čitanja postale su i garant boljeg zaposlenja, viših primanja i unosnijih prilika za napredovanje. Na taj način, engleski postaje sredstvo integracije u ekonomske i poslovne prilike.

Društvene mreže, digitalne platforme, onlajn kursevi i međunarodni projekti dodatno su doprinijeli širenju engleskog jezika i ojačali njegovu integrativnu funkciju. Bez obzira na fizičku udaljenost, razmjenjuju se ideje, iskustva i kulturni sadržaji. Na taj način se razvijaju nove platforme digitalne interkulturalnosti, a različiti identiteti se iznova prepliću i nadopunjuju.

Dakle, komunikacija na ELF se ne zasniva isključivo na normama izvornih govornika. Mnoge situacije zahtijevaju da se jezik prilagodi nekoj kulturi i njenim govornicima čime se stvara međusobno razumijevanje, fleksibilan i funkcionalan oblik komunikacije. Dakle, engleski tada nije nacionalni jezik već globalno sredstvo sporazumijevanja koje pripada svim kulturama i njihovim narodima. To naravno otvara neka normativna pitanja i pitanja vezana za vlasništvo nad jezikom. Dombi navodi da prihvatanje engleskog kao jezika koji služi komunikativnim i zajedničkim potrebama različitih zajednica logično podrazumijeva njegovu raznolikost.[1] To opet nameće pitanje u kojoj mjeri se ELF razlikuje od engleskog kao stranog jezika (EFL), koji se kao predmet izučava u većini škola proširenog kruga[1]. Možda najveća razlika između ove dvije vrste engleskog jeste u njihovim ciljevima. ELF služi međusobnom sporazumijevanju pojedinaca čiji maternji jezici nisu isti, a EFL omogućava usvajanje standardnih normi i podstiče kompetenciju nalik izvornoj.

Dakle, engleski jezik se može tumačiti kao faktor povezivanja, dijaloga i kulturne razmjene. On olakšava pristup globalnim tokovima informacija, obrazovanju i poslovnim prilikama, te doprinosi većoj mobilnosti pojedinaca i zajednica. Baš zato mnogi lingvisti ističu njegovu integrativnu ulogu u modernom svijetu.

Ipak, iako njegova funkcija mosta među kulturama ima brojne prednosti, postavlja se pitanje da li ta integracija podrazumijeva ravnopravnost ili se iza nje kriju odnosi moći i lingvističkog imperijalizma. Ta problematika je predmet analize narednog poglavlja.

IV. LINGVISTIČKI IMPERIJALIZAM I PITANJE JEZIČKE DOMINACIJE

Iako engleski jezik ima jako važnu integrativnu ulogu i sredstvo je interkulturalne komunikacije, njegova dominacija otvara niz ozbiljnih društvenih, kulturnih, ekonomskih i političkih pitanja. U prethodnom poglavlju je bilo riječi o prednostima engleskog kao lingua franca u širem društvenom kontekstu, ali postoje lingvisti i društveni teoretičari koji tvrde da dominacija jednog jezika može imati negativne, pa i pogubne posljedice po druge jezike i kulture.

Jedno od najčešćih pitanja koje se postavlja jeste da li globalna i univerzalna upotreba samo jednog jezika zaista doprinosi ravnopravnosti između kultura ili stvara nove oblike neravnoteže i političke dominacije. Dakle, da li postojanje lingua franca predstavlja napredak ili kulturni gubitak? Kako jedan jezik postane dominantno sredstvo komunikacije, javlja se mogućnost da govornici drugih jezika budu u nezavidnom položaju. Takva situacija može dovesti do stvaranja novih društvenih hijerarhija u kojima poznavanje engleskog jezika može postati ključni faktor pristupa znanju i profesionalnim prilikama. Sa obrazovnog aspekta, za jedne to može biti prilika, a za druge prepreka. Qizi navodi da davanje prednosti engleskom jeziku u obrazovanju može dovesti do jezičke nejednakosti, pri čemu učenici iz urbanih i društveno privilegovanih sredina – koji su češće izloženi engleskom jeziku – imaju veće obrazovne i profesionalne mogućnosti u odnosu na one iz ruralnih ili marginalizovanih zajednica. [8] To bi značilo da engleski nije samo lingvistička vještina, već značajan faktor društvenih podjela.

Posmatrano iz te perspektive, jezik nije samo neutralno sredstvo komunikacije, već jedna vrsta simboličke moći. Jezik je instrument kojim se oblikuju društveni odnosi, status pojedinca, kulture i države. Poznavanje engleskog jezika je vrsta društvenog kapitala i globalna valuta koja stvara asimetrije u svjetskom sistemu, te olakšava pristup boljim ekonomskim i političkim prilikama. Kristal ističe da je status globalnog jezika prvenstveno posljedica političke i ekonomske moći njegovih govornika, a ne njegovih lingvističkih karakteristika. [9] Dakle, jezik ne postaje globalan zato što je lingvistički jednostavniji ili *bolji*, već zato što se govori u zajednicama koje su politički, vojno i ekonomski moćnije.

Malo ekstremniji pogled na ovo ima Robert Filipson koji je uveo pojam *lingvističkog imperijalizma***,** koji podrazumijeva da širenje jednog jezika potkopava opstanak drugih. Termin se pojavio početkom devedesetih godina XX vijeka i definiše se kao proces u kojem dominacija globalnog jezika doprinosi očuvanju ekonomske i kulturne moći samo pojedinih zemalja. Prema njegovoj teoriji, širenje engleskog jezika povezano je sa istorijskim procesom kolonijalizma i savremenim uticajem anglofonih zemalja. [10]

Filipson takođe upozorava da situacija u obrazovnim sistemima može dovesti do marginalizacije lokalnih jezika.

[1] Kachru (1992) je predstavio model svjetskih varijeteta engleskog jezika kroz tri koncentrična kruga. Prvi, unutrašnji krug (Inner Circle), odnosi se na zemlje u kojima je engleski maternji jezik. Drugi, spoljašnji krug (Outer Circle), obuhvata države u kojima engleski nije maternji, ali ima istorijski utemeljenu i institucionalnu ulogu. Treći, prošireni krug (Expanding Circle), uključuje zemlje u kojima engleski nema istorijski status, već se prvenstveno uči i koristi kao strani jezik.

Upotreba engleskog je vidljiva u svim sferama života, pa univerziteti širom svijeta uvode studijske programe na engleskom, a naučni radovi se sve češće objavljuju na engleskom kako bi bili vidljivi svjetskoj akademsko zajednici. Prema podacima baza Scopus i Web of Science, gotovo 95% indeksiranih naučnih časopisa objavljuje se na engleskom jeziku. [8] To je doprinijelo stvaranju globalne akademske elite koja privileguje naučnike koji objavljuju na engleskom, a istovremeno se smanjuje vidljivost istraživanja napisanih na drugim jezicima.

Poznavanje engleskog jezika postaje ključan faktor društvene stratifikacije. Pojedinci koji imaju pristup kvalitetnom obrazovanju i mogućnost učenja engleskog imaju veće šanse za profesionalni napredak, međunarodnu mobilnost i pristup svjetskim tržištima rada. Postoje i oni koji nemaju takve mogućnosti mogu i nalaze se u nepovoljnijem položaju, što dodatno produbljuje postojeće socijalne i ekonomske nejednakosti.

UNESCO izvještaji ukazuju na to da je 40% svjetskih jezika ugroženo, a mnogima prijeti i potpuno izumiranje dkaja XXI vijeka. Taj podatak ne čudi kada se uzme u obzir uticaj engleskog na druge jezike. Globalna upotreba engleskog dovela je do pojave velikog broja anglicizama – riječi i izraza preuzetih iz engleskog jezika. To se vidi i na primjeru srskog jezika – izdanje Srpskog rečnika novijih anglicizama (SRNA) iz 2001. sadržavalo je oko 950 odrednica, dok izdanje iz 2021. broji preko 4500 odrednica, što je čak pet puta više u odnosu na prvo. [11] Osim anglicizama, javljaju se i jezički hibridi u kojima se elementi lokalnog jezika kombinuju sa stranim izrazima. Sa jedne strane, takve promjene obogaćuju jezik, ali istovremeno postojii zabrinutost zbog potiskivanja domaće leksike, jezičke autentičnosti i identiteta. Tako jedna nacija ne gubi samo jezik, već onaj medijum kroz koji su se gradila njihiva načela, nasljeđe i kultura. Širenje jednog jezika na uštrb drugih dovodi do homogenizacije, jednoličnosti i tsvaranja globalnog identiteta oblikovanog zapadnim vrijednostima i normama.

Kroz svjetske medije i digitalnu dominaciju, engleski postaje *instrument kulturne i političke hegemonije*. Širenjem jezika šire se i kulturni i društveni obrasci, vrijednosti i stil života, te se oblikuju globalni kulturni tokovi i utiče se na način na koji različite zajednice percipiraju svijet.

Uprkos svim izazovima, mnogi lingvisti naglašavaju da dominacija engleskog jezika ne mora nužn da znači potpuno uništenje ili marginalizaciju drugih jezika. Mnoga društva njeguju i razvijaju modele višejezičnosti kojima se uspostavlja ravnoteža između globaliacije i očuvanja kulture i jezičkog identiteta. Baš taj prostor između integracije i očuvanja raznolikosti podstiče savremene i korisne rasprave o ulozi engleskog jezika u svijetu.

Na osnovu svega navedenog da se zaključiti da je njegova uloga dvostruka. Sa jedne strane, on je korisno sredstvo međunarodne komunikacije i saradnje, a sa druge strane njegova sveprisutnost i dominacija mogu stvoriti nove oblike jezičke i kulturne nejednakosti i neravnopravnosti. Razumijevanje njegove kompleksne prirode i dinamike je značajno za dalje sagledavanje prilika i mjesto engleskog jezika u savremenom i interkulturalnom prostoru.

Ozbiljnost situacije shvataju i globalne sile pa je tako Generalna skupština UNa usvojila rezoluciju kojom je period od 2022. do 2032. godine proglašen *Međunarodnom dekadom autohtonih jezika (IDIL 2022–2032)*. Cilj ove inicijative je da se skrene globalna pažnja na kritičnu situaciju u kojoj se nalaze mnogi autohtoni jezici, kao i da se mobilišu različiti akteri i resursi za njihovo očuvanje, revitalizaciju i promociju. [12]

V. ZAKLJUČAK

U savremenom digitalnom svijetu engleski jezik se izborio za jedinstvenu poziciju kao sredstvo međunarodne komunikacije – lingua franca. Njegova rasprostranjenost i dominacija su rezultat viševjekovnih društvenih, političkih i tehnoloških dešavanja. Kao takav, on omogućava komunikaciju između ljudi različitih jezičkih i kulturnih pozadina, olakšava saradnju, razmjenu znanja i nastoji da integriše kulture.

S jedne strane, on predstavlja sredstvo interkulturalne integracije. Njegova upotreba olakšava prevazilaženje jezičkih i kulturnih barijera i omogućava pristup globalnim tokovima informacija, inovacija i obrazovanja. Engleski predstavlja centralni kanal komunikacije u digitalnom okruženju i doprinosi stvaranju globalnog komunikacijskog prostora u kojem različitosti djeluju, upoznaju se, prepliću i stupaju u interakciju.

Sa druge strane, dominacija samo jednog jezika otvara niz ozbiljnih pitanja koja se odnose na raznoslikost i ravnopravnost jezika i kultura. Mnogi lingvisti upozoravaju na problem marginalizacije manjih jezika, stvaranje jezičkih nejednakosti i produbljivanje društvenog jaza. Konept jezičkog imperijalizma ukazuje na to da jezik može postati moćan instrument u rukama svjetskih sila, dovoljno jak da uništi manje jezike i stvori nejednakosti između različitih društvenih grupa i država.

Zbog toga se uloga engleskog jezika u modernom svijetu ne može posmatrati jednostrano. On istovremeno i povezuje i razdvaja, obogaćuje i istovremeno uništava vokabulare manjih jezika. Budući izazov za međunarodne zajednice i pripadnike manjih nacija jeste pronalaženje ravnoteže između integrisanja i očuvanja jezičke raznolikosti i kulturne baštine. Jedino takav pristup može omogućiti da upotreba engleskog jezika doprinese međukulturnom razumijevanju i prihvatanju različitosti koje zapravo i čine ovaj svijet bogatijim i ljepšim.

LITERATURA

[1] J. Dombi, “English as a lingua franca in intercultural communication,” Bulletin of the Transilvania University of Brasov. Series IV: Philology and Cultural Studies, pp. 183–186, Jul. 2011, Accessed: Mar. 02, 2026. [Online].Available: https://webbut.unitbv.ro/index.php/Series_IV/article/view/6231

[2] B. Seidlhofer, “English as a lingua franca,” *ELT Journal*, vol. 59, no. 4, pp. 339–341, Oct. 2005, doi: 10.1093/elt/cci064.

[3] R. Phillipson, *English-Only Europe?*, 0 ed. Routledge, 2004. doi: 10.4324/9780203696989.

[4] N. Lukianenko, “Language and power: linguistic imperialism,” *ISJEL*, vol. 3, no. 5, pp. 41–49, Oct. 2024, doi: 10.46299/j.isjel.20240305.06.

[5] “Eurobarometer.” Accessed: Mar. 04, 2026. [Online]. Available: https://europa.eu/eurobarometer/surveys/detail/518

[6] N. Bakic-Miric, “Re-imaging Understanding of Intercultural Communication, Culture and Culturing,” *J. inc. comm*, vol. 8, no. 2, pp. 1–05, Jun. 2008, doi: 10.36923/jicc.v8i2.456.

[7] A. Nishat, “English as a Global Lingua Franca: Effects on Cultural Identity and Intercultural Communication,” [Online]. Available: https://api.semanticscholar.org/CorpusID:278691616

[8] Toxirjonova Kamola Dilshodbek Qizi, “THE IMPACT OF ENGLISH AS A GLOBAL LINGUA FRANCA ON LOCAL LANGUAGES,” Nov. 2025, doi: 10.5281/ZENODO.17586159.

[9] “Crystal, David. 2003. English as a Global Language. Second edition. Cambridge University Press,” *Per Linguam*, vol. 20, no. 1, 2011, doi: 10.5785/20-1-80.

[10] R. Phillipson, “Linguistic imperialism,” Oxford university press, Oxford [GB], 1992.

[11] A. Đuranović and M. Vuković , “Језички хибриди на друштвеним мрежама: утицај енглеског језика на комуникацију путем друштвених мрежа,” Nauka i stvarnost 2025 Pale. (U štampi)

[12] “Indigenous Languages Decade (2022-2032) | UNESCO.” Accessed: Mar. 05, 2026. [Online]. Available: https://www.unesco.org/en/decades/indigenous-languages

CIP - Каталогизација у публикацији
Народна и универзитетска библиотека
Републике Српске, Бања Лука

004.56:502.131.1]:17(0.034.2)

МЕЂУНАРОДНИ научни скуп "Синергија" (26 ; 2026 ; Бијељина)
Zbornik radova "Sinergija 2026". Inovacije, bezbjednost i etika u savremenom digitalnom i održivom poslovanju [Електронски извор] / XXVI međunarodni naučni skup sa međunarodnim učešćem, Bijeljina, 29. april 2026. godine ; [glavni urednik Saša Adamović]. - Onlajn izd. - El. zbornik. - Bijeljina : Univerzitet Sinergija, 2026. - (Zbornik radova Sinergija, ISSN 2490-3825)

Način pristupa (URL):
https://naucniskup.sinergija.edu.ba/zbornici/. - Насл. са насловног екрана. - Опис извора дана 21.07.2026. - Ел. публикација у ПДФ формату опсега 109 стр. - Радови на срп. и енгл. језику. - Напомене и библиографске референце уз текст. - Библиографија уз сваки рад. - Abstracts.

ISBN 978-99955-26-50-4

COBISS.RS-ID 144622849