Đorđević S. Aleksandar[*]
https://orcid.org/0009-0001-4513-0250
Jevtić Boris[**]
https://orcid.org/0009-0005-8261-2047
Deđanski Stevica[***]
https://orcid.org/0000-0002-5144-3675

UDC: 343.53:004.9(497.11)
Original scientific paper
DOI: 10.5937/ptp2404048D
Received on: October 15, 2024
Approved for publication on:
October 29, 2024
Pages: 48–68

INTERACTIONS BETWEEN REGULATIONS, LAW, NEW TECHNOLOGIES, AND ORGANIZATIONAL POLICIES IN FINANCIAL FRAUD DETECTION – A CASE STUDY OF SERBIA

ABSTRACT: Digitization has led to the emergence of increasingly sophisticated forms of financial fraud, necessitating more advanced and integrated approaches for their rapid detection and prevention. This challenge prompted the authors to examine relevant literature and analyze current policies and measures for detecting financial fraud within the digital environments of organizations, with the aim of enhancing proactive prevention strategies. To this end, an online empirical survey was conducted with 118 executives and managers from Serbia during the first half of 2024, supported by the Association of Employers of Serbia and the Association of Managers. The research focused on the impact of new technologies, particularly AI, on the regulations and organizational policies related to financial fraud detection. Qualitative research, which

[*] PhD, Research Associate, Institute of Comparative Law, Belgrade, Serbia, e-mail: dradjordjevic8@gmail.com

[**] PhD student, Union University, Faculty of Computing RAF, Belgrade, Serbia, e-mail: boris.jevtic10@gmail.com

[***] PhD, Associate Professor, University Business Academy in Novi Sad, Faculty of Social Sciences, Belgrade, Serbia, e-mail: dedjanskis@gmail.com

utilized 12 predefined statements within each impact group using a five-point Likert scale, provided insights into the actual experiences and perspectives of participants concerning financial fraud as a distinct business, social, and economic issue. Multiple correlation approaches were employed to analyze the data. The outcomes suggest that all analyzed factors contribute to addressing financial fraud, with new technologies – especially those based on artificial intelligence – and corporate policies and strategies playing significant roles. Conversely, regulations have a lesser impact, attributed to their correctness, implementation, and enforcement. These findings enhance the understanding of the significance of taking a comprehensive approach to combating fraud, corruption, and financial crime, and highlight the roles of continuous technological advancements, employee digital education, and enhanced communication with the public and investors in building trust and maintaining a company's reputation.

Keywords**:** *Digitization, legal framework, financial fraud, artificial intelligence, company policy.*

1. Introduction

Fraud detection within the financial services sector has evolved significantly over time. The historical narrative indicates a transformation from manual, rules-oriented methods to more advanced technological solutions, motivated by the escalating complexity associated with financial wrongdoing. In the foundational period of the financial sector, fraud detection predominantly entailed human supervision and structured regulatory systems, relying heavily on human expertise to identify suspicious patterns, inconsistencies, or deviations from typical behavior. While these proven methods yielded some results, their limitations became clearer as financial systems grew more extensive and complex. Established fraud detection approaches struggled with various obstacles that hindered their effectiveness in addressing advanced financial crimes. These systems relied on pre-set rules, which could only handle fraud patterns that were already known. In response, fraudsters promptly adapted to these regulations, crafting new tactics to evade established detection mechanisms. Additionally, the hands-on method turned the process into a slow and mistake-prone endeavor, impeding the organization's capability to react promptly to new risks. Another considerable constraint was the inability to conduct real-time analysis of large data sets. As the volume of financial transactions increased, traditional methods struggled to adapt, resulting in slower identification and resolution of fraudulent activities. The inability to scale and adapt made a paradigm shift essential for enhancing fraud detection capabilities.

From a practical business management perspective, an organization's fraud policy, particularly regarding the early detection and prevention of false reporting, is becoming increasingly important. Reducing the potential for illegal profits (Ahmed, Mahmood, & Islam, 2016) and addressing fraud in financial statements are subjects of extensive research (Abdallah, 2016). Fraud is defined as a willful act that is considered illegal or unethical and takes place during the course of employment, which can distort how an organization's profitability is perceived (Apostolou & Apostolou, 2012). The effectiveness of internal controls in preventing fraud depends on both the robustness of these controls and the ethical environment cultivated by the organization, which couold be determined by the conduct and communication of its leadership (Sengur, 2012). Some frauds in statements can evade detection by standard audit procedures (Dai & Handley-Schachler, 2015). A clearly articulated global network of ideas and processes impacts future outcomes through the actions of organizations today, heightening the responsibility of senior leadership. This accountability is enforced through internal rules, employee and management behavior, monitoring mechanisms, and a board dedicated to safeguarding the accuracy and reliability of financial reporting while also upholding the integrity of internal and external audit evaluations. Features of corporate culture play a more crucial role in uncovering and deterring financial deception (Lewis-Beck, Bryman & Futing Liao, 2004). Corporate culture comprises a series of shared social and ethical traits, along with business behaviors that are shaped by the organization's history and goals, and are reflected in the values established in its policies (Rockness & Rockness, 2005; Naqshbandi, 2017). Many authors emphasize the importance of long-term thinking in loss prevention for organizational policy (Servaes, Tamayo & Tufano 2009; Snider, 1991). Establishing clear objectives in fraud risk management, alongside fostering adaptability in response to the continuous changes in the environment, is essential for modern organizations (Lister, 2007; Crockford, 2005; Mehr & Forbes, 1973; Maynard, 1999). The development of organizations is increasingly influenced by the broader institutional ecosystem, making the regulations and legal frameworks surrounding fraud more prominent.

Financial services are subject to multiple regulatory frameworks that dictate standards for privacy of information, consumer safeguards, and fair borrowing procedures. While existing laws have been employed to combat fraud since the beginning, gaps in oversight and overlapping jurisdictions have persisted. Additionally, the enforcement of laws and regulations is often inconsistent. The economic environment, characterized by high competitive pressure and innovations that heighten information asymmetry, has further influenced the prevalence of questionable practices. Consequently, management and control mechanisms have generally proven inadequate to prevent fraud. This circumstance underscores the need for AI-enabled fraud detection systems to meet regulatory compliance, ensuring their responsible and ethical use. Organizations should consistently monitor the changing regulatory environment regarding artificial intelligence in relation to financial fraud. It is crucial for compliance efforts to emphasize data protection laws (Blanke, 2020), anti-discrimination regulations, and other financial guidelines to uphold ethical and legal compliance in AI-powered fraud detection. Addressing prejudices, advancing model transparency, and conforming to compliance regulations, are key factors in the ethical deployment of artificial intelligence technologies for fraud detection. Nonetheless, the growing complexity of financial crime, fueled by technological progress, requires a shift away from conventional methods. Sophisticated tactics like identity theft, phishing, and malware attacks exploit weaknesses in financial systems. In the last two decades, modern technologies, particularly those based on artificial intelligence, have significantly enhanced the performance of both production and service systems. The challenges posed by artificial intelligence in the 21st century, alongside the rapid rise of information technologies globally, have influenced organizational development (Deđanski & Jevtić, 2024; Špiler et al., 2023; Miškić, Srebro, Rašković, Vrbanac & Jevtić, 2024). The proliferation of artificial intelligence has brought about a significant transformation in the identification of fraud. Algorithms based on machine learning can independently derive insights from data and discern patterns, offering solutions that are both dynamic and adaptive. These AI solutions have the ability to analyze vast datasets, detect minor discrepancies, and continually adjust to address emerging fraud schemes. The historical narrative emphasizes the immediate need and significance of integrating cutting-edge technologies, including artificial intelligence, into fraud detection, cultivating a more proactive and effective strategy for mitigating financial misconduct. The latest literature increasingly centers on fraud, techniques for its identification, the presentation and evaluation of fraud detection methods in financial documents, and fraud risk models that consider the elements of the fraud triangle (Srivastava, Mock & Gao, 2011).

In light of these trends, the authors were motivated to conduct this study to address the specified research inquiry: How significant and mutual is the influence of new digital technology methods, regulations, and company policies on the detection of financial fraud? Drawing on existing literature as well as their own prior works (Jevtić, Beslać, Janjušić & Jevtić, 2024; Jevtić, Deđanski, Beslać, Grozdanić & Damnjanović, 2013; Stake, 2006), the authors formulated an empirical study to assess the attitudes of representatives (managers and executives from financial and IT departments) from 118 companies in Serbia. In the first half of 2024, these representatives provided their insights in an anonymous online survey regarding the influence of 12 statements—three for each group of selected factors impacting financial fraud detection: modern technologies based on artificial intelligence, regulations, and company policies. The Employers' Union and the Association of Managers of Serbia assisted in selecting participants and establishing contacts. The outcomes of this investigation seek to enhance both scholarly literature and tangible uses within the domain through trend analysis that influence the role of artificial intelligence in maintaining security within the financial services industry. The structure of the paper includes an abstract, an introduction, a review of the literature, a detailed description of the methodology for the empirical research, data analysis, and discussion. The paper concludes with the results and accompanying references.

2. Literature Framework

New technologies, particularly those rooted in artificial intelligence, offer numerous opportunities for detecting and preventing financial fraud in modern organizations. However, these opportunities need to be better understood (Akindote et al., 2023). The following areas are noteworthy:

- Case-Based Reasoning: This approach uses a database of stored cases as the primary knowledge source, incorporating models from non-monotonic reasoning, qualitative analysis, automation, and spatiotemporal dimensions. The theory and practice of reasoning in artificial intelligence involve developing axioms that provide a sound and complete logical framework, understanding the theoretical properties of algorithms used for qualitative reasoning, and ensuring relevance to specific reasoning problems (e.g., independence), as well as methods for qualitative reasoning.
- Automated and Expert Systems: These systems have contributed to greater efficiency, faster processing, and improved scalability in fraud

detection. In particular, artificial intelligence significantly contributes to automating transaction data analysis, enabling financial institutions to efficiently detect irregularities and patterns that suggest fraudulent activities.

- Systemic Bias in AI: AI algorithms gain insights from historical data and assess whether it contains inherent biases; however, the models may unintentionally reproduce or magnify those biases in their decisions and predictions. Organizations must take action to recognize and alleviate biases during the creation and execution of these models to address this concern. This encompasses routinely analyzing the models for bias, ensuring that the training data is diverse and inclusive, and employing fairness metrics to measure the models' influence across different demographics. Several AI models, particularly neural network-based ones, operate in a "black box" manner, making it hard to discern the rationale for their decisions.
- Genetic Algorithms: These algorithms, based on natural selection and genetics, utilize knowledge representation, a structured approach to problem-solving, content-based image retrieval, and description logic for semantic indexing. Simple conceptual graphs form the core of most formalisms and represent another area of potential AI application in the issues being investigated.
- Directed and Non-Directed Learning: In directed learning, AI technologies are developed on classified datasets to identify associations with both legitimate and fraudulent transactions, facilitating forecasts for novel, unobserved data. However, data-driven learning, does not rely on labeled datasets; instead, it identifies patterns or anomalies by exploring the natural structures within the data. The transformation of artificial intelligence in fraud detection highlights a shift from traditional rule-based systems to innovative, learning-based approaches. Leveraging vast datasets, these models evolve with emerging threats, empowering financial institutions to stay ahead of increasingly complex fraud tactics. The integration of directed and undirected learning, advanced multi-layered learning methods, and language technology establishes a robust set of tools in the ongoing pursuit of combating financial wrongdoing.
- Machine Learning Methods: Learning agents (Ha, Xu, Ren, Mitchell & Ou, 2020) focusing on the syntax and semantics of user information represent a valuable area of artificial intelligence for detecting and preventing financial fraud. This includes inductive bias learning

models, approximation algorithms, and experiments on inducing interpretable vote classifiers without trading. Machine learning algorithms, particularly those utilizing unsupervised learning methods, are designed to detect subtle irregularities and deviations from typical patterns within extensive datasets. These discrepancies may involve unusual transaction patterns, odd spending locations, or behaviors that deviate from typical user activity. The aspect of continuous learning ensures that the system develops in tandem with emerging threats, delivering an adaptable defense against evolving fraud tactics. Natural language processing, a branch of AI, has become instrumental in fraud detection by examining written data, including correspondence logs and transaction summaries, to uncover linguistic patterns that suggest dishonest activity.

- Neural Networks: Neural networks have been instrumental in improving fraud detection by enabling systems to independently learn and identify hierarchical structures within datasets, thereby enhancing their ability to detect complex fraud schemes.. Due to their capacity to handle complex and non-linear relationships, neural networks are skilled at recognizing sophisticated patterns associated with fraud. Their capability to independently extract features from data has resulted in a considerable enhancement in the accuracy of fraud detection algorithms.
- Precision in Envelope Maintenance Problems: The employment of machine learning frameworks to achieve precision in envelope maintenance problems (Singh et al., 2002) is another intriguing area of study for application in fraud detection.
- Developing a Partnership Strategy: Developing a partnership strategy that leverages the advantages of artificial intelligence algorithms alongside human skills enhances the overall success of fraud prevention activities (Srebro, Paunović & Jevtić, 2024). Successful fraud detection using artificial intelligence is shaped by the quality and range of training data made available. This includes utility and solution, distributed artificial intelligence, theorem proving, constraint satisfaction, theory of computation, and techniques like Monte Carlo methods, belief revision, and data mining.

Forecasting future trends and innovations in this area includes the potential application of the latest technologies, such as:

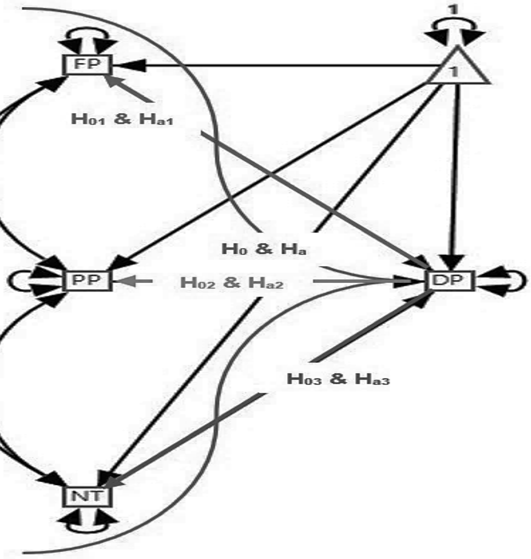
- Advancement of Interpretable AI: This endeavor focuses on boosting transparency and clarity in AI algorithms. In response to growing regulatory scrutiny, organizations are leveraging these systems to ensure clear rationales for the decisions generated by AI algorithms. This degree of transparency is crucial for building trust among stakeholders, complying with regulatory requirements, and fostering productive cooperation between human specialists and automated technologies. Anticipated innovations in explainable AI are poised to improve the comprehensibility and usability of AI models, including advancements in visualization techniques, interactive dashboards, and more straightforward explanations of complex AI choices.

- Joint Learning: A decentralized machine learning approach promises to enhance collaboration between organizations while safeguarding personal data security. In this approach, AI models undergo training directly at each organization, utilizing data specific to that entity and exchanging only the updates to the models. This facilitates joint learning across a consortium of entities while safeguarding confidential, site-specific data.
- Integration of Advanced Biometric Authentication Methods: Incorporating biometrics – such as facial recognition, fingerprint scanning, and behavioral biometrics – into AI-driven fraud detection systems provides an added level of protection by specifically identifying individuals according to their physical and behavioral characteristics. Real-time analysis of biometric traits by AI algorithms helps uncover and prevent instances of unauthorized access or fraud.
- Network Graph Analysis: This serves as a robust approach for uncovering intricate Deceptive schemes that encompass various interrelated parties. By modeling the relationships and dynamics within extensive datasets, AI systems can identify unusual patterns that suggest organized fraudulent behavior. This method greatly enhances the capability to identify and prevent fraud that could be overlooked by conventional techniques. Many authors highlight the increasingly active role that regulatory bodies will play in shaping fraud detection through artificial intelligence methods.
- Trends in Addressing Financial Fraud: Trends in addressing financial fraud are shifting towards greater collaboration among modern organizations, encouraging the transfer of threat intelligence and industry best practices. These joint initiatives promote an anticipatory response to new fraud patterns, facilitating the exchange of knowledge gained by one entity across the broader industry network. It is crucial for regulatory bodies to continuously adjust to the evolving landscape of AI and fraud, which requires monitoring progress in technology, assessing the ethical impact of AI

systems, and maintaining regulatory compliance to adequately safeguard consumers and contemporary organizations. Building collaborations involving regulatory entities and corporate sector participants will promote continuous communication and adaptable regulatory structures.

Based on a review of the authors' numerous studies and relevant literature in the field of research, the following research variables (categories influencing the detection of financial fraud) were defined: three independent variables: Organizational Policies Regarding Financial Fraud (FP), Legal Framework and Regulations Concerning Financial Fraud (PP), and New Technologies and Methods for Detecting Financial Fraud (NT); as well as one dependent variable: Detection of Financial Fraud (DP). Consequently, the research model for this study was defined (Graph 1):

Graph 1. Conceptual model



Source: Author’s research

3. Materials and Methods

For this research, a web-based empirical assessment was conducted involving a sample of 118 companies (executives and managers) based in Serbia during the first half of 2024. The study was facilitated by Serbia's Employers' Association and the Association of Managers. It focuses on the impact of new technologies, particularly those based on artificial intelligence, as well as regulations and company policies related to the detection of financial fraud. Online data were collected regarding the views of representatives from the companies on 12 statements (3 for each impact category) as defined in Table 1:

Table 1: Statements

Statements	
FP: **Organizational Policies Towards Financial Fraud**	
FP_1	The company develops long-term financial fraud prevention strategies that are integrated into broader business goals.
FP_2	Addressing financial fraud helps preserve a company’s integrity and reputation, which is critical to its long-term success.
FP_3	Organizations should educate employees about potential sources of fraud, relevant legislation, and new technologies to enhance the effectiveness of risk management in recognizing potential fraud.
PP: **Regulations Relating to Financial Fraud**	
PP_1	Regulatory changes and tightening legal requirements increase the need for compliance with standards and the implementation of stricter control measures.
PP_2	Financial fraud can lead to legal issues, including fines, litigation, and damage to an organization’s reputation.
PP_3	The creation and implementation of modern laws and regulations to maintain ethical business practices, minimize the likelihood of fraud, and build investor confidence among employees and the public are increasingly important in Serbia.
NT: **New Technologies Based on Artificial Intelligence**	
NT_1	As digitization and the use of new technologies increase, financial fraud becomes more sophisticated.
NT_2	The integration of digital technologies with existing audit and control systems augments the capability to detect and mitigate financial fraud.
NT_3	Utilizing artificial intelligence, machine learning, and advanced algorithms for document analysis allows for accurate tracking and recognition of fraud patterns in large data sets.
DP: **Financial Fraud Detection**	
DP_1	Financial fraud, defined as a dishonest and illegal act, includes the manipulation of financial data and documentation, identity theft, and corruption, all aimed at concealing the true financial condition of the organization for personal gain.
DP_2	The disclosure and prevention of financial fraud are key to maintaining the trust of investors, clients, and other stakeholders.
DP_3	Preventing financial fraud improves internal management and control, thereby reducing the risk of future fraud and irregularities.

Source: Author’s research

Respondents expressed their views on their agreement with the defined statements using a weighted Pearson scale ranging from 5 to 1, where 5 represents the highest value. This research seeks to identify the possible effects: Does FP affect DP? Does PP affect DP? Does NT affect DP? Do FP, PP, and NT collectively affect DP? Based on the established research model and defined objectives, the following hypotheses were formulated:

- H01: FP does not affect DP; Ha1: FP affects DP.
- H02: PP does not affect DP; Ha2: PP affects DP.
- H03: NT does not affect DP; Ha3: NT affects DP.
- H0: FP, PP, and NT do not affect DP; Ha: FP, PP, and NT affect DP.

The following statistical methods were used to analyze the obtained data: multiple correlation and regression analyses, along with the ANOVA test. All calculations were performed using the statistical software SAS JMP Pro 17.

3.1 Key findings

In this segment of the document, the significant outcomes of the applied research are detailed. Table 2 displays the frequencies and probabilities for each statement related to all the variables in the research model.

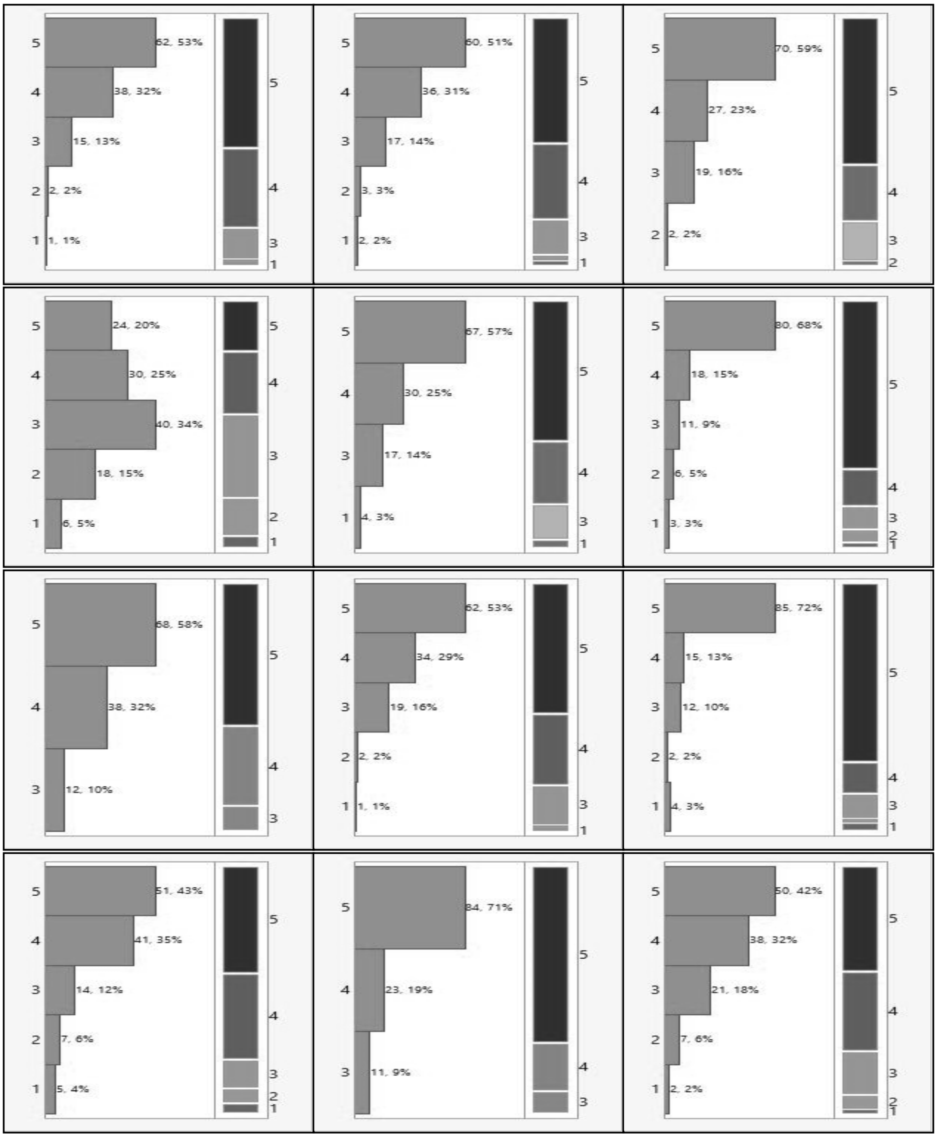
It can be concluded that the highest frequency for the attitude is: 1 – Not at all accurate PP1 – 6,2 – Largely inaccurate statement PP1 – 18, 3 – Undecided on statement PP3 – 40, 4 – Largely accurate statement DP1 – 41 and 5 – Completely correct statement NT3 – 85. It can be concluded that the lowest frequency for the attitude is: 1 – Not at all accurate FP3, NT1, DP2 – 0, 2 – Largely inaccurate statement PP2, NT1, and DP2 – 0, 3 – Undecided about statement NT1 – 0, 4 – Largely accurate NT3 – 15 and 5 – Fully accurate statement PP1 – 24. In (Graph 2) graphical frequencies and probabilities are given for each statement of all set variables of the research model.

Table 2: Frequencies and probability of representation of attitudes to the set research statements of all variables

Statement **FP**	FP_1		FP_2		FP_3	
Attitudes/scale	**Frequency**	**Probability**	**Frequency**	**Probability**	**Frequency**	**Probability**
1 – Not at all accurate	1	0.00847	2	0.01695	0	0
2 – Largely inaccurate	2	0.01695	3	0.02542	2	0.01695
3 – Undecided	15	0.12712	17	0.14407	19	0.16102
4 – Largely accurate	38	0.32203	36	0.30508	27	0.22881
5 – Fully **accurate**	62	0.52542	60	0.50847	70	0.59322
Total	118	1.00000	118	1.00000	118	1.00000
Statement **PP**	**PP_1**		**PP_2**		**PP_3**	
Attitudes/scale	**Frequency**	**Probability**	**Frequency**	**Probability**	**Frequency**	**Probability**
1 – Not at all accurate	6	0.05085	4	0.03390	3	0.02542
2 – Largely inaccurate	18	0.15254	0	0	6	0.05085
3 – Undecided	40	0.33898	17	0.14407	11	0.09322
4 – Largely accurate	30	0.25424	30	0.25424	18	0.15254
5 – Fully **accurate**	24	0.20339	67	0.56780	80	0.67797
Total	118	1.00000	118	1.00000	118	1.00000
Statement **NT**	**NT_1**		**NT_2**		**NT_3**	
Attitudes/scale	**Frequency**	**Probability**	**Frequency**	**Probability**	**Frequency**	**Probability**
1 – Not at all accurate	0	0	1	0.00847	4	0.03390
2 – Largely inaccurate	0	0	2	0.01695	2	0.01695
3 – Undecided	0	0	19	0.16102	12	0.10169
4 – Largely accurate	38	0.32203	34	0.28814	15	0.12712
5 – Fully **accurate**	68	0.57627	62	0.52542	85	0.72034
Total	118	1.00000	118	1.00000	118	1.00000
Statement DP	DP_1		DP_2		DP_3	
Attitudes/scale	**Frequency**	**Probability**	**Frequency**	**Probability**	**Frequency**	**Probability**
1 – Not at all accurate	5	0.04237	0	0	2	0.01695
2 – Largely inaccurate	7	0.05932	0	0	7	0.05932
3 – Undecided	14	0.11864	11	0.09322	21	0.17797
4 – Largely accurate	41	0.34746	23	0.19492	38	0.32203
5 – Fully **accurate**	51	0.43220	84	0.71186	50	0.42373
Total	118	1.00000	118	1.00000	118	1.00000

Source: Author's research

Graph 2. Frequency and Probability Analysis of Attitudes Toward All Variable Statements



Source: Author's research

The highest average score for the statements of the variable **FP** is **4.40** for statement **FP3**. The highest standard deviation for the statements of the variable **FP** is **0.92** for statement **FP2**. For the variable **PP**, the highest mean value is **4.41** for statement **PP3**, while the highest standard deviation is **1.13** for statement **PP1**. For the variable **NT**, the highest mean value is **4.83** for statement **NT3**, which also has the highest standard deviation at **0.98**. The highest average score for the **DP** variable is **4.62** for statement **DP2**, while the highest standard deviation is **1.08** for statement **DP3**. Table 3 provides the standard deviations for all variables in the research model. Among the variables, the highest mean value is **4.42** for **NT**, and the highest standard deviation is **0.69** for **DP**. The lowest mean value is **4.05** for the variable **PP**, and the lowest standard deviation is **0.62** for the variable **NT**.

Table 3. Mean scores and dispersion of the research model variables

Variables	Mean Value	Dispersion
FP	4.333	0.6595057
PP	4.045	0.6875852764
NT	4.421	0.6200633581
DP	4.254	0.6913905035

Source: Author's research

Analysis of the relationship between the FP and DP variables: The statistical significance assessment from the ANOVA test for FP and DP is [F(1,116) = 71.8920, p < 0.0001]. The H01 hypothesis has no assumed premise, but there is an agreed-upon Ha1 as the alternative.***: FP affects DP.*** The linear regression equation for the variables FP and DP (Formula 1) is as follows:

$$DP = 1{,}444 + 0{,}648 \cdot FP \tag{1}$$

The intercept of 1.444 represents the baseline value of DP which occurs when FP is 0, and the coefficient of 0.648 shows how variations in FP influence DP.

Analysis of the relationship between the PP and DP variables: After completing the basic standard and non-standard assessments, an evaluation of the derived research model for PP and DP was supported. According to the multiple R-squared value of 0.2333, 23.33% of the variation in the DP can be traced to PP. The correlation between the variables is relatively weak, at 0.483. The statistical significance of the ANOVA test for PP and DP is [F(1,116) = 35.3008, p < 0.0001]. Based on these results, The H02 hypothesis has no assumed premise, but there is an agreed-upon Ha2 as the alternative***: PP affects DP. The linear regression equation for the variables PP and DP*** (Formula 2) is as follows:

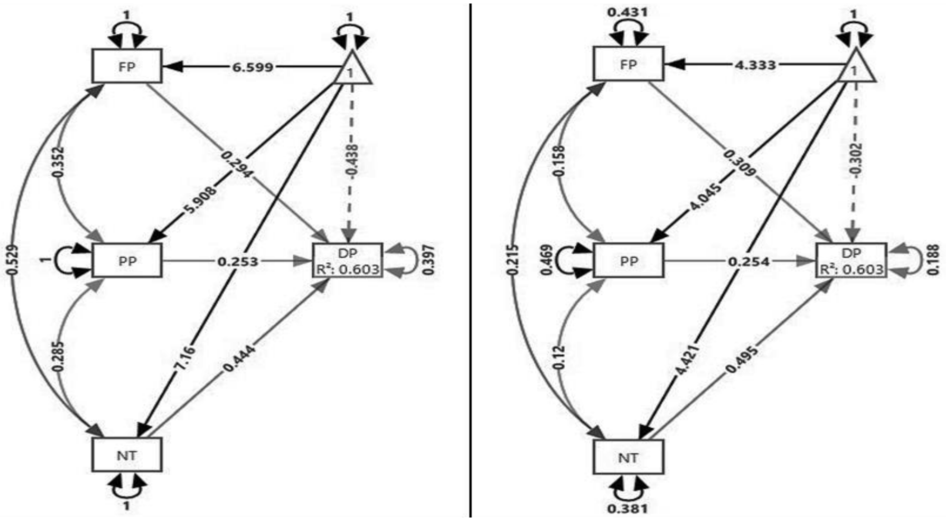
$$DP = 2{,}289 + 0{,}486 \cdot PP \tag{2}$$

The intercept of 2,289 represents the baseline value of DP which occurs when PP is 0, and the coefficient of 0,486 shows how variations in PP influence DP.

Analysis of the relationship between the NT and DP variables: After evaluating the derived research model for NT and DP, a coefficient of determination of 0.4515 was gathered, signifying that 45.15% of the variability in the DP can be attributed the variable NT. The association between the variables is moderately strong, at 0.672. The statistical significance of the ANOVA test for NT and DP is [F(1,116) = 95.5145, p < 0.0001]. The H03 hypothesis has no assumed premise, but there is an agreed-upon Ha3 as the alternative: NT affects DP. The linear regression equation formed for the variables NT and DP (Formula 3) is as follows:

$$DP = 0{,}942 + 0{,}749 \cdot NT \tag{3}$$

Graph 3. Standardized (left) and raw (right) contribution sizes for the variables FP, PP, NT, and DP



Source: Author's research

The greatest contribution to DP comes from the NT variable (0.444), followed by FP (0.294), with the smallest contribution from PP (0.253). The assessment of the statistical significance of the ANOVA test for the variables

FP, PP, NT, and DP is [F(3,114) = 57.6580, p < 0.0001]. The H0 hypothesis has no assumed premise, but there is an agreed-upon Ha as the alternative: ***FP, PP, and NT have an effect on DP***. A multiple linear regression equation was developed for the variables FP, PP, NT, and DP (formula 4), which is as follows:

$$DP = -0{,}302 + 0{,}309 \cdot FP + 0{,}254 \cdot PP + 0{,}495 \cdot NT \tag{4}$$

This formula enables the prediction of the DP variable using the values of further three: FP, PP, and NT. The intercept (-0.302) represents the baseline value of DP when all independent variables are zero. The coefficients (0.309 for FP, 0.254 for PP, and a value of 0.495 for NT indicates the expected change in the dependent variable, DP, with a single increment in NT, holding other variables constant.

3.2 Disccusion

Acceptance of the alternative hypothesis **Ha1** indicates that the independent variable **FP** is an important predictor of the dependent variable **DP**. This means that when modeling or predicting **DP**, the independent variable **FP** should be considered, as it has a significant and measurable impact on the values of **DP**. Similarly, acceptance of the alternative hypothesis **Ha2** indicates that the independent variable **PP** is also an important predictor of **DP**. This implies that when modeling or predicting **DP**, the independent variable **PP** should be taken into account, given its significant and measurable impact on **DP**'s values. Acceptance of the alternative hypothesis **Ha3** indicates that the independent variable **NT** is likewise an important predictor of **DP**. Thus, when modeling or predicting **DP**, the independent variable **NT** should be considered due to its significant and measurable impact on **DP**.

Overall, acceptance of the alternative hypothesis **Ha** indicates that the independent variables **FP**, **PP**, and **NT** are all important for predicting the dependent variable **DP**. This means that when modeling or predicting **DP,** all three independent variables—**FP, PP**, and **NT**—should be taken into account, as they have a significant and measurable impact on **DP**'s values. It can be said that the research model presented in Graph 1 is well-suited for predicting the dependent variable **DP.**

4. Conclusion

The paper analyzes a dynamic approach to detecting and averting fraud in organizations, highlighting the transformative impact of artificial intelligence (AI). It demonstrates that, in addition to bolstering security frameworks, AI encourages a forward-thinking and agile methodology to confront the continually shifting landscape of financial fraud. The paper indicates that gaining a thorough understanding of how AI can transform fraud detection in the financial sector necessitates the integration of historical insights, current applications, and future developments. The rationale for this paper's focus on better integrating AI into organizational fraud detection and prevention arises from the demand for sophisticated, flexible, and real-time detection capabilities. Since AI systems need to evolve persistently to keep pace with emerging fraudulent tactics and changing patterns, performing regular updates and organizational enhancements is key to maintaining the functionality of fraud mitigation platforms. Although AI offers remarkable possibilities for fraud detection, it is important to maintain human oversight. Combining AI algorithms with human expertise in a collaborative manner significantly enhances the overall success of anti-fraud initiatives. The capacity of AI technologies to evaluate vast amounts of data, detect nuanced patterns and adapt to changing fraud schemes, positioning them as critical allies in the battle against financial crime. The adoption of artificial intelligence is further determined by the demand to stay ahead of increasingly sophisticated fraud that traditional methods struggle to address. It is vital for organizations to prioritize AI models that provide clarity during strategic initiatives aimed at building trust with stakeholders and ensuring adherence to regulatory requirements. The tangible benefits of AI applications in combating fraud illustrate its performance in stopping dishonest practices, curtailing the number of false positives and negatives, and providing organizations with valuable intelligence. As organizations increasingly adopt AI-driven anti-fraud frameworks, the partnership between human skills and cutting-edge technology will be crucial for maintaining a resilient defense against evolving fraud threats. This research expands knowledge regarding financial fraud and highlights the need for anticipatory prevention strategies, particularly contributing to the literature in Southeast Europe. By building upon existing practices, researchers can design proactive models, and subsequent studies may use this foundation to establish new theories in proactive fraud prevention. This work may influence investments in AI models and the development of fraud prevention strategies, especially in a rapidly changing business environment. Social implications include the potential to enhance trust in corporate reporting, thereby improving corporate reputation. The limitations of this study involve a sample restricted to organizations within the economic sector and an analysis limited to a smaller set of factors affecting fraud detection. Given the high economic costs of fraud, gaining insight into existing fraud policies and practices is crucial for informing more proactive measures for early detection.

In conclusion, the findings highlight the need for further research on current trends and innovative solutions in automated financial fraud detection using AI, particularly in methods like explainable AI, joint learning, and continuous adaptation to emerging threats.

Đorđević S. Aleksandar
Institut za uporedno pravo, Beograd, Srbija

Jevtić Boris
Univerzitet Union, Računarski fakultet, Beograd, Srbija

Deđanski Stevica
Univerzitet Privredna akademija u Novom Sadu, Fakultet društvenih nauka, Beograd, Srbija

INTERAKCIJE ZAKONA, PROPISA, NOVIH TEHNOLOGIJA I POLITIKA ORGANIZACIJE U OTKRIVANJU FINANSIJSKIH PREVARA – PRIMER SRBIJE

APSTRAKT: Digitalizacija je dovela do pojave sve sofisticiranijih oblika finansijskih prevara, što zahteva naprednije i integrisane pristupe za njihovo brže otkrivanje i prevenciju. Ovaj izazov je podstakao autore da ispitaju relevantnu literaturu i analiziraju aktuelne politike i mere za otkrivanje finansijskih prevara u digitalnom okruženju organizacija, sa namerom unapređenja proaktivnih strategija prevencije. U tom cilju sprovedeno je online empirijsko istraživanje sa 118 rukovodilaca i menadžera iz Srbije tokom prve polovine 2024. godine, uz podršku Udruženja poslodavaca

Srbije i Udruženja menadžera. Istraživanje se fokusiralo na uticaj novih tehnologija, posebno onih zasnovanih na veštačkoj inteligenciji, propisa i politike firmi koje se odnose na otkrivanje finansijskih prevara. Kvalitativno istraživanje, koje je koristilo 12 unapred definisanih izjava unutar svake grupe uticaja peko Pirsonove skale od pet tačaka, pružilo je uvid u stvarna iskustva i perspektive učesnika u vezi sa finansijskim prevarama kao posebnim poslovnim, društvenim i ekonomskim pitanjem. Podaci su analizirani korišćenjem višestrukih korelacionih metoda. Nalazi sugerišu da svi analizirani faktori utiču na finansijske prevare, pri čemu nove tehnologije, posebno one zasnovane na veštačkoj inteligenciji, politike i strategije organizacije igraju značajnu ulogu. Nasuprot tome, propisi imaju manji uticaj, što se pripisuje njihovoj aktuelnosti, primeni i transparentnosti. Ovi rezultati doprinose dubljem razumevanju značaja sveobuhvatnog pristupa u borbi protiv prevara, korupcije i finansijskog kriminala i ističu ulogu kontinuiranog tehnološkog napretka, digitalnog obrazovanja zaposlenih i poboljšane komunikacije sa javnošću i investitorima u izgradnji poverenja i očuvanju ugleda kompanije.

Ključne reči: *digitalizacija, zakonski okvir, finansijska prevara, veštačka inteligencija, politika organizacije.*

References

1. Ahmed, M., Mahmood, A. N., & Islam, M. R. (2016). A survey of anomaly detection techniques in financial domain. *Future Generation Computer Systems*, *55*, pp. 278–288. https:// doi.org/10.1007/978-3-030-70713-2_60.
2. Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detecton system: A survey. Journal of Network and Computer Applications, *68*, pp. 90–113. https://doi.org/10.3390/app12199637
3. Akindote, O. J., Adegbite, A. O., Dawodu, S. O., Omotosho, A., Anyanwu, A., & Maduka, C. P. (2023). Comparative review of big data analytics and GIS in healthcare decision-making. *World Journal of Advanced Research and Reviews*, *20*(3), pp. 1293–1302 http://dx.doi.org/10.30574/wjarr.2023.20.3.2589
4. Apostolou, B., & Apostolou, N. (2012). The value of risk assessment: Evidence from recent surveys. The Forensic Examiner, *21*(3), Downloaded 2024, August 31 from http://www.theforensicexaminer.com/
5. Blanke, J.M. (2020). Protection for 'Inferences drawn': A comparison between the general data protection regulation and the California

consumer privacy act. *Global Privacy Law Review, 1*(2). http://dx.doi.org/10.54648/gplr2020080

6. Crockford, G. N. (2005). The changing face of risk management, *Geneva Papers on Risk & Insurance – Issues & Practice*, *30*(1), pp. 5–10. http://dx.doi.org/10.1057/palgrave.gpp.2510019
7. Dai, Y., & Handley-Schachler, M. (2015). A fundamental weakness in auditing: The need for a conspiracy theory. *Procedia Economics and Finance*, *28*, pp. 1–6. DOI: 10.1016/S2212-5671(15)01074-6.
8. Deđanski, S., & Jevtić, B. (2024). Uticaj veštačkom inteligencijom podržanih usluga na korisničko iskustvo – primer hotelske industrije Srbije [The impact of artificial intelligence-supported services on user experience – the example of the Serbian hotel industry], *Limes-plus,* 1-2, in press
9. Ha, N., Xu, K., Ren, G., Mitchell, A. & Ou, J.Z. (2020). Machine learning-enabled smart sensor systems. *Advanced Intelligent Systems*, *2*(9), pp. 2000063. http://dx.doi.org/10.1002/aisy.202000063
10. Jevtić, B., Deđanski, S., Beslać, M., Grozdanić, R., & Damnjanović, A. (2013). SME Technology Capacity Building for Competitiveness and Export – Evidence from Balkan Countries, *Metalurgija International*, *18*(spec.iss.4), pp. 162–170
11. Jevtić, B., Beslać, M., Janjušić, D., & Jevtić M. (2024). The effects of digital natives' expectations of tech hotel services quality on customer satisfaction, *International Journal for Quality Research*, *18*(1), pp. 1–10. DOI: 10.24874/IJQR18.01-01
12. Lewis-Beck, M. S., Bryman, A. & Futing Liao, T. (2004). *The SAGE encyclopedia of social science research methods*, SAGE Publications Ltd. DOI: 10.4135/9781412950589.
13. Lister, L. M. (2007). A practical approach to fraud risk. *Internal Auditor*, *64*(6), pp. 61–65. Downloaded 2022, January 21 from https://na.theiia.org/Pages/IIAHome.aspx
14. Maynard, G. R. (1999). Embracing risk. *Internal Auditor*, *56*(1), pp. 24–29. Downloaded 2022, March 21 from https://na.theiia.org/Pages/IIAHome.aspx
15. Mehr, R. I., & Forbes, S. W. (1973). The risk management decision in the total business setting. *Journal of Risk & Insurance*, *40*(3), pp. 389–401. http://dx.doi.org/10.2307/252226
16. Miškić, M., Srebro, B., Rašković, M., Vrbanac, M., & Jevtić, B. (2024). Key Challenges Hindering SMEs' full benefit from Digitalization – A

Case Study from Serbia, *International Journal for Quality Research*, *19*(2). DOI: 10.22874/IJQR1902-03.

17. Naqshbandi, K. M. A. (2017). Towards understanding corporate social responsibility. Pakistan & Gulf Economist. Downloaded 2024, April 15 from http://www.pakistaneconomist.com
18. Rockness, H., & Rockness, J. (2005). Legislated ethics: From Enron to Sarbanes-Oxley, the impact on corporate America. *Journal of Business Ethics*, *57*(1), pp. 31–54. DOI: 10.1007/s10551-004-3819-0
19. Sengur, E. D. (2012). Auditors' perception of fraud prevention measures: Evidence from Turkey. *Annales Universitatis Apulensis – Series Oeconomica*, *14*(1), pp. 128. http://dx.doi.org/10.29302/oeconomica.2012.14.1.11
20. Snider, H. W. (1991). Risk management: A retrospective view. *Risk Management* (00355593), 38(4), pp. 47–54. Downloaded 2024, April 10 from http://www.rmmag.com/
21. Servaes, H., Tamayo, A., & Tufano, P. (2009). The theory and practice of corporate risk management. *Journal of Applied Corporate Finance*, *21*(4), pp. 60–78. DOI:10.1111/j.1745-6622.2009.00250.x
22. Srivastava, R. P., Mock, T. J., & Gao, L. (2011). The Dempster-Shafer theory: An introduction and fraud risk assessment illustration. *Australian Accounting Review*, *21*(3), pp. 282–291. DOI:10.1111/j.1835-2561.2011.00135.x
23. Stake, R. E. (2006). *Multiple case study analysis*. New York: The Guilford Press.
24. Srebro, B., Paunović, L., & Jevtić, B. (2024). Unraveling Hospitality: Exploring Human, Digital, and External Forces in Marketing Communications. In: *XIX International symposium SymOrg, Zlatibor* (pp. 617–625). Belgrade: University of Belgrade, Faculty of Organizational Sciences
25. Špiler, M., Milošević, D., Miškić, M., Gostimirović, L., Beslać, M., & Jevtić, B. (2023). Investments in digital technology advances in textiles, *Industria Textila*, *74*(1), pp. 90–97, DOI: 10.35530/IT.074.01.202287