THE USE OF AI IN TAX ADMINISTRATION, A SECURITY RISK OR AN OPPORTUNITY FOR ROMANIA'S DEVELOPMENT?

Cristina ONEȚ[1]

https://doi.org/10.54989/stusec.2025.19.02.15

Abstract

This article examines the impact of implementing artificial intelligence (AI) technologies within Romania's tax administration, assessing both the potential benefits and the associated risks. It explores how AI can streamline administrative processes by automating routine tasks, improving data accuracy, and enabling faster analysis of large-scale financial information. These developments have the potential to significantly enhance revenue collection and reduce tax evasion through more effective detection of irregularities, predictive analytics, and real-time monitoring of taxpayer behaviour.

At the same time, the article highlights several challenges that must be addressed to ensure responsible and trustworthy use of AI in the fiscal sector. Key concerns include cybersecurity vulnerabilities arising from the increased reliance on digital infrastructures, the protection of personal data in compliance with EU standards, and the need to preserve transparency in automated decision-making systems. Without clear safeguards, the use of AI could undermine public trust or lead to discriminatory outcomes.

Drawing on international examples as well as Romania's specific institutional and legislative context, the study offers practical recommendations for implementing AI in a balanced and legally compliant manner. These insights aim to support policymakers in designing a modern, efficient, and secure tax administration.

Keywords: artificial intelligence; tax administration; digitalization; cybersecurity; transparency

Introduction

Artificial intelligence (AI) represents one of the most significant technologies of the digital era, exerting a substantial impact on the way public services are designed and delivered. In the context of tax administration, the use of AI can contribute to streamlining processes, improving the collection of budgetary revenues, and reducing tax evasion by enabling the rapid and accurate analysis of large data volumes and by automating routine activities. However, the implementation of such technologies raises complex issues related to data security, the confidentiality of taxpayers' information, and the risks associated with algorithmic errors or the improper use of sensitive data. As a result, tax authorities face the challenge of harnessing the innovative potential of AI without compromising safety and public trust. In Romania, the digitalization of tax administration is undergoing an accelerated transformation, driven by European initiatives on digital governance and the need to modernize public infrastructure. Within this context, analysing how artificial intelligence can be integrated into the national fiscal system becomes essential for establishing a balance between efficiency, security, and transparency.

[1] Cristina Oneț, Associate Professor (Habil.), Faculty of Law, Lucian Blaga University of Sibiu, Romania, https://ORCID.org/0000-0002-6785-5025, cristina.onet@ulbsibiu.ro

This paper aims to examine the main benefits and risks of using AI in tax administration by referencing international best practices and the specific features of Romania’s legislative and institutional framework. It also identifies development opportunities that may arise from the responsible and ethical implementation of these technologies, with a view to strengthening institutional capacity and enhancing citizens’ trust in the Romanian fiscal system. The research methods used are those specific to public law, as the analysis begins with the normative framework established by the European Regulation on AI, which sets the conceptual foundations of this study. Therefore, the research methodology relies on theoretical, descriptive, and analytical approaches. A documentary and legislative analysis was carried out, examining European regulations on AI (Regulation EU 1689/2024 and proposals of the European Commission).

The first part of the paper analyses the official definitions of “AI systems” and the classification of risks. The legal obligations and compliance requirements for AI systems of various risk levels are identified. Subsequently, a theoretical and conceptual analysis was conducted. The paper classifies types of AI (General vs. Narrow AI) and associated risks, describes how different AI technologies operate and are applied (such as chatbots and machine learning), offers a predictive assessment of fiscal risks, and identifies broader challenges related to AI, such as cybersecurity, algorithmic transparency, errors, algorithmic discrimination, institutional resistance, ethical issues, and of course, legal concerns.

Another important part of the work includes a risk assessment and proposals for best practices. The main risks are enumerated and categorized (cybersecurity, data loss, internal and external attacks, interoperability, etc.), accompanied by recommended best practices for infrastructure and data protection, such as authentication, encryption, monitoring, specialized training, backups, and audits. Furthermore, theoretical concepts are related to the current status of Romania’s fiscal administrative IT systems. In this context, the study examines the concept of AI-driven attacks and relates it to the specific digital vulnerabilities of fiscal systems. At the same time, it analyzes the specific implementation of AI within National Agency for Fiscal Administration, including detailed references to systems such as e-Factura, RO e-Transport, SAF-T, and the APIC project, presenting the advantages and limitations of these systems within Romania’s current fiscal context.

In essence, this study offers an integrated analysis of the technical, legal, and operational implications of introducing AI in Romania’s tax administration.

Brief History and Definition of the Concept of Artificial Intelligence

The concept of artificial intelligence (AI) began to take shape in the early 1950^{s}, when Alan Turing published the paper *Computing Machinery and Intelligence*, in which he proposed the Turing Test to evaluate machine intelligence.[1] This milestone was followed by the Dartmouth College Conference in 1956, which officially introduced the term “artificial intelligence” and established AI as a branch of computer science.[2] After 1956, there was a period of great optimism regarding the idea that machines could possess their own intelligence within just a few years. However, the lack of spectacular results, as expected, led to a significant reduction in funding, followed by pronounced scepticism about the chances of success of this idea.[3]

[1] Alan Turing, *Computing Machinery and Intelligence,* Mind, 59 (236), 1950, pp. 433–460

[2] John McCarthy, Marvin Minsky, Nathaniel Rochester, Claude Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, Dartmouth College Archives, 1956, pp. 1

[3] Daniel Crevier, *AI: The Tumultuous History of the Search for Artificial Intelligence*, Basic Books, New York, 1993, pp. 1-8

Nevertheless, between the 1980^s and 1990^s, so-called expert systems emerged, which began to use knowledge from databases to solve specific problems, such as medical diagnosis or financial analyses. The increase in computing power and the development of databases led, between 1990 and 2010, to the creation of the first machine learning algorithms,[1] marking a step toward artificial intelligence. After 2010, humanity entered the era of the deep learning revolution (deep neural networks), which enables progress in speech recognition, natural language processing, and computer vision.[2] Recent applications include generative AI (capable of generating new content through machine learning algorithms) autonomous robots, and sophisticated recommendation systems.[3]

Accordingly, definitions of artificial intelligence (AI) have naturally emerged in line with these developments. It is considered a set of computing technologies capable of imitating human cognitive processes, such as learning, reasoning, pattern recognition, and decision-making.[4] In the European Commission's proposed Artificial Intelligence Regulation, AI was defined as "a software system (and, in some cases, hardware) designed to receive data, interpret it, and make decisions or recommend actions to achieve a specific objective." In the final version of the Regulation approved by the European Parliament and the Council, the concept of an "AI system" is defined as a machine-based system designed to operate with different levels of autonomy and capable of exhibiting adaptability after deployment, which, while pursuing explicit or implicit objectives, deduces from the input data it receives how to generate results such as predictions, content, recommendations, or decisions that may influence physical or virtual environments.[5] There are two main categories of AI systems:

- General AI systems, which express a theoretical concept aimed at developing systems capable of reproducing human intelligence in a broad sense.
- Narrow AI systems, which are used for specific tasks, such as data analysis, speech recognition, or fraud detection.[6]

General Risks and Challenges of Using Artificial Intelligence

Regulation (EU) No. 1689 of 13 June 2024 on AI classifies the risks associated with certain uses of AI into four levels of risk and establishes corresponding rules for each. The four risk levels under the AI Regulation and their respective requirements are as follows:

[1] Murray Campbell, Joseph J. Hoane, Feng-hsiung Hsu, *Deep Blue*", "Artificial Intelligence", 134(1–2), 2002, pp. 57–83

[2] David Silver, Aja Huang, Cristopher J. Maddison, et al., *Mastering the game of Go with deep neural networks and tree search,* "Nature", 529, 2016, pp. 484–489

[3] Recommendation systems are software applications designed to filter information and provide users with suggestions about items that might be of interest to them, based on certain criteria. Roditis, M., Tabacariu, A., Trăușan-Matu, S., 2011, *Image recommendation system based on social, semantic, and visual aspects*, in "*Romanian Journal of Human-Computer Interaction"*, 4(1), pp. 23–50

[4] David Poole, Alan Mackworth, Randy Goebel, *Computational Intelligence: A Logical Approach,* Oxford University Press., 1998, pp. 1-2.; Nils Nilsson, *Artificial Intelligence: A New Synthesis*. Morgan Kaufmann, 1998, pp. 1-15; George F. Luger, *Artificial Intelligence: Structures and Strategies for Complex Problem Solving* (5th Ed.). Pearson, 2005, pp 1-3

[5] Art. 3(1) of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144, and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Regulation) https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

[6] Stuart Russell, Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th Ed.). Pearson, 2021, p.21

a) Minimal or Non-existent Risks. Most AI systems pose no significant risks, so systems such as AI-based games or spam filters can be used without restrictions. These are not regulated or targeted by the provisions of the EU AI Regulation.

b) Limited Risks. AI systems that involve only limited risks, such as chatbots or AI systems generating content, are subject to transparency obligations, such as informing users that the content has been generated by AI, allowing them to make informed decisions regarding its continued use.

c) High Risks. High-risk AI systems, such as those used in disease diagnosis, autonomous vehicle operation, or biometric identification of individuals involved in criminal activities or investigations, must meet strict requirements to access the EU market. These obligations include rigorous testing, transparency, and human oversight.

d) Unacceptable Risks. The use of AI systems that pose a threat to human safety, rights, or livelihoods is prohibited in the EU. This includes behavioral-cognitive manipulation, predictive policing activities, emotion recognition in workplaces and educational institutions, and the assignment of social scores. The real-time remote use of biometric identification systems, such as facial recognition by law enforcement in public spaces, is also prohibited, with only limited exceptions.

The expansion of AI use has been a natural process, given the numerous advantages it can bring to both public and private spheres. However, the emerging risks have created a set of challenges that require appropriate and generally acceptable solutions. Among the challenges highlighted in the aforementioned European document, the following stand out:

a) Cybersecurity and Personal Data Protection. Implementing AI involves managing large volumes of sensitive data, so the absence of robust security measures can lead to information leaks or cyberattacks.

b) Algorithmic Transparency. Many AI systems function as “black boxes,” making it difficult to understand how decisions are made. This can generate concerns regarding the fairness and impartiality of the tax process.

c) Risk of Errors and Algorithmic Discrimination. If algorithms are trained on incomplete or biased datasets, classification errors and unfair treatment of taxpayers may occur.

d) Institutional Resistance and Lack of Digital Skills. Administrative staff must be trained to work effectively with new technologies; otherwise, the implementation process may be slow and inefficient.

e) Ethical and Legal Issues. In the absence of a clear legislative framework regarding responsibility for automated decisions, defining institutional accountability may be challenging.[1]

All these challenges require adequate solutions,[2] as the successful and efficient use of AI in public administration is not a solution in itself. AI can exponentially improve the relationship between public administration and citizens in all its aspects,[3] but only if

[1] Anca Florentina Vatamanu, Mihaela Tofan, *Integrating Artificial Intelligence into Public Administration: Challenges and Vulnerabilities*, in *„Administrative Sciences”,* vol. 15, no. 4, 2025, article 149 https://doi.org/10.3390/admsci15040149

[2] Yulia Petlenko, Lucian Tarnu, Bohdan Shchehliuk, Silviu Nate, *Enhancing the Effectiveness of Defence Planning through the Implementation of Capability-Based Budgeting and Civilian Control*, in ”*AJEE Journal”*, 2023, https://doi.org/10.33327/AJEE-18-6.4-n000477

[3] Andreea Nicoleta Dragomir, *The Role of Technology in Migration Management: Balancing Security, Ethics, and Human Rights*, in ”*Studia Securitatis”*, 18(2), 2024, pp. 25–34

implemented correctly, precisely, and in compliance with certain requirements. This makes the process neither simple nor accessible to everyone.

The Use of Artificial Intelligence in Romania's Tax Administration. Introductory Considerations

In its current activity, the tax administration primarily focuses on the use of general AI systems, with the main objectives of automating repetitive processes, supporting decision-making analysis, and improving the relationship between the tax authority and taxpayers. Over the past decade, AI has become an essential component of the digital transformation of the public sector. Tax, customs, and financial administrations in developed countries employ intelligent systems for operations such as predictive analysis of taxpayer behavior to identify potential cases of tax evasion; automation of administrative processes, including the validation of tax returns, document verification, and the processing of VAT refunds; optimization of taxpayer services through virtual assistants capable of providing personalized information; and monitoring of transactions as well as anomaly detection through machine learning algorithms.[1]

Successful examples of the expanded use of AI in the public sector can be observed in countries such as Estonia, Finland, Spain, and the Netherlands, where AI is integrated into national tax systems, contributing to the reduction of bureaucracy, the decrease of tax evasion, and the increase of voluntary compliance.

Potential Advantages of Using AI in Romania's Tax Administration

Faced with the enormous volume of information flowing from taxpayers to the fiscal authority, the use of AI appears to be the most effective response that public authorities can provide. AI can enable the collection, management, and processing of this information for the purpose of accurately determining each taxpayer's real fiscal situation. The use of AI in tax debt administration has significant potential to increase the efficiency of the tax authority, as it facilitates not only the structuring of collected information but also its analysis and processing in order to generate accurate and relevant conclusions.

Several tools are currently available through AI, each of which can be used in specific ways that maximize benefits while avoiding the disadvantages associated with them. For example, **chatbot systems** are software programs capable of simulating conversations with human users, typically through text (in chat interfaces) or voice (via voice assistants). They are designed to automatically answer questions, provide information, or perform tasks without the intervention of a human operator. Such systems can be used to support and guide taxpayers at various stages of fiscal procedures, helping to ensure a more uniform application of tax legislation.[2]

[1] Emilia Lucia Catană, *Modernizing Administrative Law in the Era of Digital Transformation: The Electronic Administrative Act*, *"Revista de Drept Public",* No. 4/2019, Universul Juridic Publishing, pp. 21–26; Emilia Lucia Catană, *The Impact of Digitalization of Public Administration Activities on the Administrative Act: Normative, Jurisprudential, and Administrative Procedure Codification Perspectives*, in *"Revista de Drept Public"*, No. 3/2022, pp. 117–119; Laurențiu Șoneriu, *Digital Transformation of Public Administration in Romania and the European Union*, *"Studia Securitatis"*, No.2/2023, pp. 18–25; Flavia Ghencea, *Digitalization of Public Services: Constraints and Opportunities for the Public Education System*, "Proceedings of the conference *Digitalization of Law and Public Administration in the Pandemic Context"*, Ovidius University, Constanța, Universul Juridic Publishing, Bucharest, 2021, pp. 243–254

[2] Cristina Oneț, *From Digitalization to AI in Tax Debt Administration*, *"Revista de Drept Public"*, Supplement, 2025, pp. 61–76

These systems can be implemented immediately, as they are well suited for simple processes of taxpayer assistance and guidance. They can provide information on deadlines for submitting tax returns, payment deadlines, payment methods, types of taxes owed, available tax facilities, outstanding tax liabilities, and more. The use of such systems presents significant advantages, including uninterrupted availability, rapid, accurate, and consistent responses, and the elimination - or at least substantial reduction - of pressure on support services. In Romania, the public is still becoming familiar with these tools; however, the systems themselves can help address this issue by offering adequate guidance, including instruction on their use. These simpler systems also improve accessibility to information for users less familiar with complex digital platforms, in addition to providing access to tax-related information.

Machine learning systems, or automated learning models, are algorithms that learn from data to make predictions, recognize patterns, or take decisions without being explicitly programmed for each scenario. Instead of following fixed rules written by a programmer, a machine learning model analyses historical data it stores, either introduced during development or acquired over time during operation. It “learns” to identify relationships between variables and can subsequently apply this knowledge to make estimates or decisions in new situations. *Machine learning* models can therefore be used in more complex processes involving large data flows from taxpayers, offering a high degree of accuracy in their predictions. This is possible because they automate repetitive tasks and adapt to changes in data. This brief analysis highlights numerous advantages of AI use in tax debt administration.

First, AI increases operational efficiency**.** AI can automate repetitive processes such as collecting data from tax returns, automatically verifying tax bases, classifying tax liabilities, monitoring payment deadlines, and generating payment notifications where necessary. It enables the processing of large volumes of data in very short periods, thus reducing processing times.

Second, AI provides high levels of predictability and prevention**,** as machine learning models can identify taxpayers at high risk of non-payment or anticipate problematic fiscal behaviours. This allows the tax authority to optimize tax collection and recovery by producing risk scores and establishing action priorities.

Third, AI can reduce human error. Automating routine decisions and verifying data automatically can significantly decrease the number of mistakes.

Furthermore, AI can substantially improve the relationship between the tax authority and taxpayers**.** AI-powered *chatbot systems* can provide rapid and personalized responses regarding tax liabilities and procedures. Taxpayers can also receive tailored recommendations on matters of high interest, such as payment options or instalment arrangements. In summary, the potential advantages of using AI in tax administration include:

- Increased administrative efficiency**,** as AI can automate numerous routine activities (processing declarations, verifying data, analysing risks), significantly reducing time and costs and freeing the tax authority to focus on strategic tasks.
- Improved revenue collection, since machine learning algorithms can identify patterns of non-compliance and detect fraud at an early stage.
- Reduced bureaucracy and human error**,** because automating processes limits the risk of human error and accelerates data processing.
- Greater transparency and trust**,** as AI can facilitate access to clear and up-to-date information, improving taxpayer guidance and enhancing public confidence in fiscal authorities.

- Support for data-driven decision-making, since AI enables complex analysis of large volumes of fiscal data, contributing to strategic decision-making in public policy development.

It remains important to note that any of the potential advantages described above may disappear - or even turn into vulnerabilities - if the implementation of IT systems in the tax administration is poorly executed, poorly organized, too slow, or carried out without an integrated concept or without rigorous coordination among the various electronic systems of national and/or European public administration.

Major Risks and Challenges

Artificial intelligence does not present only advantages; there are also significant risks and challenges that require the highest level of attention.

A first set of issues concerns data confidentiality and protection against any form of interference**.** The administration of tax debts involves access to sensitive data, and both legislators and tax authorities must ensure that risks of inadequate protection are eliminated. Therefore, the implementation of AI must strictly comply with legislation regarding fiscal secrecy and the protection of personal data.

A second set of issues relates to decision-making transparency and the provision of appropriate explanations**.** Decisions made by AI systems must be explainable and communicated to those affected.

Third, by its nature, AI is algorithm-based and responsive to the information it acquires over time. Consequently, AI models can incorporate or amplify **existing biases** in historical data, potentially leading to incorrect or inequitable fiscal treatment. Thus, the digital systems of Romania's National Agency for Fiscal Administration (NAFA) face a variety of **cybersecurity risks**[1] which may affect data integrity, information confidentiality, and service availability, including:

a) IT infrastructure vulnerabilities. The accelerated digitalization of National Agency for Fiscal Administration through systems such as e-Factura, RO e-Transport, SAF-T, and e-TVA has brought benefits in combating tax evasion, but has also exposed the agency to new cyber risks. The lack of modern IT infrastructure and adequate protection measures can lead to specific vulnerabilities exploitable by attackers.

b) Cyberattacks and security incidents. In the past, National Agency for Fiscal Administration has been targeted by cyberattacks that compromised taxpayers' personal data. Although security measures have been strengthened, the risk remains constant, considering the complexity and frequency of modern cyberattacks.

c) Deficiencies in access control and data management. The absence of clear policies on access control and data management may lead to unauthorized access to sensitive information. ANAF personnel must know and comply with information security procedures and report any security breaches.

d) Dependence on external solutions. The use of external software products, including those developed in Romania, may introduce additional security risks. For example, a Romanian software product used by National Agency for Fiscal Administration enabled the detection of phantom companies involved in tax fraud, highlighting the importance of continuously evaluating the security of external solutions.

[1] Daniela Panc, *Cybersecurity at the National and International Level: Normative and Institutional Instruments*, Hamangiu, Bucharest, 2017, p. 235

Among the cybersecurity risks National Agency for Fiscal Administration faces in the digitalization process, **external cyberattacks** are particularly notable, especially in a complex and uncertain global context. An **AI-driven attack** can be defined as a cyberattack or digital aggression in which the attacker (or aggressor system) uses AI-based techniques and systems (e.g., machine learning algorithms, content generation, autonomous adaptation) to automate, scale, personalize, and/or dynamically adapt attack steps (such as reconnaissance, target selection, execution, and evasion). These attacks become more effective, harder to detect, and capable of exploiting emerging vulnerabilities faster than traditional attacks.[1] Relevant types of AI-driven attacks[2] in the fiscal domain include:

a) Automated cyberattacks on fiscal infrastructure. Examples include adaptive malware exploiting vulnerabilities in fiscal databases or intelligent DDoS attacks on National Agency for Fiscal Administration portals, preventing taxpayers from submitting returns or making payments, potentially causing severe consequences such as public budget losses and fiscal disorder.

b) Disinformation and cognitive attacks. These may take the form of deepfakes or false announcements appearing to originate from National Agency for Fiscal Administration, generating panic and confusion among businesses and citizens. They may also involve coordinated phishing campaigns using AI-generated emails, leading to large-scale theft of authentication data from the Virtual Private Space or other National Agency for Fiscal Administration or Romanian Customs Authority platforms.

c) Compromise of fiscal data integrity. AI algorithms could selectively modify or delete transactions in e-Factura/SAF-T, affecting VAT collection and the accuracy of fiscal risk analyses. Attacks on connected cash registers could generate false revenue reporting.

d) Exploitation of interdependencies. AI could be used to identify vulnerabilities in interoperability between National Agency for Fiscal Administration and other institutions (Treasury, Ministry of Finance, banks) or target APIs, allowing unauthorized access to financial data. Based on this theoretical analysis of potential AI-driven attacks, the main **cybersecurity risks** that could affect the digitalization of Romania's tax administration can be summarized as follows:

a) Cyberattacks (hacking, ransomware, DDoS), given that National Agency for Fiscal Administration and the Ministry of Finance manage highly sensitive data (personal identification numbers, incomes, invoices, transactions). Attackers may attempt to paralyze electronic systems, encrypt data, or steal information for fraudulent purposes.

b) Data breaches or unauthorized access, which may occur if the infrastructure is not properly secured. Taxpayer data could be accessed by unauthorized individuals for illegal purposes.

c) Phishing and attacks targeting users (taxpayers and officials). Fake emails mimicking ANAF notifications, already documented in Romania, may cause taxpayers to download infected files or enter data on fraudulent websites.

[1] Hooman Alavizadeh, Julian Jang-Jaccard, Tansu Alpcan, Seyit Ahmet Camtepe, *A Markov game model for AI-based cyber security attack mitigation*, "arXiv:2107.09258, Computer Science and Game Theory", 2021 https://arxiv.org/abs/2107.09258

[2] Kadapa Chenchi Reddy, Mohamad Saleem, *Anticipatory Cyber Crimes during the AI Era – An Indian Context*, "*International Journal of Intelligent Systems and Applications in Engineering (IJISAE)",* 12(4), 2024, pp. 5447–5459; Nimra Bashir, Muhammad Zeeshan Zafar, *AI-powered Cyberattacks: Impacts and Defense Strategies*, "*World Journal of Advanced Research and Reviews"*, 25(3), 2025, pp. 510–512

d) Software vulnerabilities and lack of patches. National Agency for Fiscal Administration systems are complex, developed by different vendors, and difficult to integrate. Any component may remain vulnerable if patches are not applied promptly.

e) Interoperability and data transfer issues between institutions. Some projects involve data exchanges between National Agency for Fiscal Administration, Ministry of Finance, Customs, Ministry of Transport, etc. Inadequately secured interfaces may lead to breaches.

f) Internal risks (insider threats). Employees with privileged access may misuse the system (data theft, manipulation). Insufficient monitoring of internal activities increases risk.

g) Dependence on external providers and geopolitical risks. Many solutions are developed with EU funding or by private companies. Limited control over infrastructure may create vulnerabilities.

These types of cyberattacks can severely undermine the digitalization of tax administration. The consequences extend beyond immediate or short-term disruptions and may target National Agency for Fiscal Administration's digital systems while also affecting the overall functioning of the public financial system. These consequences can be grouped as follows:

- Financial impact: revenue losses for the state (due to undetected evasion, collection disruption, payment interruptions, etc.).
- Operational impact: blockages in submitting declarations, massive delays in VAT refunds, unavailability of IT systems, and disruption of economic activity.
- Reputational impact: reduced taxpayer trust in National Agency for Fiscal Administration, resulting in lower voluntary compliance.
- Legal and political impact: serious breaches of GDPR and EU directives (e.g., NIS2), potentially generating sanctions and external pressure.
- Strategic impact: attacks could be used by hostile state actors to destabilize the economy, disrupt public finance stability, and cause severe consequences for the functioning of the entire public system.

Solutions and Best Practices Applicable in Romania

To adequately address all the risks associated with the large-scale implementation of National Agency for Fiscal Administration's digital systems, it is necessary to identify viable solutions that consider priorities such as:

a) Secure authentication and access, both for officials and taxpayers, including the use of digital identity (the new ROeID project) for unified and secure access.

b) Data encryption, which must be ensured at all times, both when platforms are accessed and when they are at rest. Storage of sensitive documents must be conducted in cyber-secure environments.

c) Monitoring and early detection, which can be achieved through the use of systems to detect attempted attacks and by continuously monitoring internal activities to prevent abuses.

d) Protection against external attacks through the implementation of advanced firewalls, anti-DDoS solutions, network segmentation, and any other modern tools designed to provide these results.

e) User education (officials and taxpayers), through organizing cybersecurity training for officials and anti-phishing awareness campaigns for the general public.

f) Updates and vulnerability management by implementing software standardization measures to reduce "chaos" between applications.

g) Backup and operational continuity through daily execution of specific data protection operations, creation of redundant data centres, and development and implementation of disaster recovery plans.

h) Governance and transparency through ISO 27001 certifications regarding information security, as well as periodic external audits of National Agency for Fiscal Administration's IT infrastructure.[1]

A phased and concise action strategy would initially focus on securing access to ANAF platforms and safeguarding critical data within these platforms. In the medium term, efforts should aim at strengthening the infrastructures supporting these digital systems, while in the long term, alignment with EU standards and the expansion of AI and Big Data use for intelligent tax administration should be pursued.[2] In this context, the APIC (Efficient Administration through Consolidated Information) project was designed - a Big Data initiative by National Agency for Fiscal Administration aimed at managing large volumes of structured and unstructured data, capable of performing risk analyses, predictive modelling, and automating taxpayer risk analysis. Its purpose is to enable National Agency for Fiscal Administration to precisely identify where and when tax evasion occurs, so that inspection resources can be directed exactly where needed. The main features and functionalities of APIC include:

a) Integration of information from multiple sources such as e-Invoice, electronic cash registers, SAF-T, and other internal and external databases.

b) Development of predictive analyses to assess and estimate risky tax behaviours using algorithms, statistical models, and machine learning systems.

c) An integrated IT tool to automate risk analysis, reducing subjectivity and increasing efficiency in National Agency for Fiscal Administration's decision-making regarding inspections.

The estimated completion date for this project is December 2025; however, there are discussions suggesting that the module allowing data analysis from e-Invoice may only be available in 2026. Meanwhile, intermediate modules are being developed to enable data collection and analysis for preliminary use of useful information. A project of this magnitude must demonstrate significant advantages to justify its implementation. Properly implementing APIC is expected to allow more efficient allocation of inspection resources, thereby reducing costs and increasing revenue collection by combating tax evasion before it becomes highly costly.

Additionally, automating risk analysis can reduce subjectivity, errors, and delays in decision-making (rather than relying on traditional notifications or manual inspections). At the same time, connecting tax data with external sources (banks, chambers of commerce, registries, etc.) can provide a more comprehensive view of taxpayers' actual fiscal situation. Furthermore, predictive modelling and Big Data use can detect subtle patterns of tax evasion or fraud that would otherwise be difficult to identify. However, no human-created system is infallible. Several risks, limitations, and challenges associated with APIC have been identified. Initially, these include project implementation delays. Even if the implementation deadline is December 2025, some opinions suggest that the complete finalization of all

[1] Mir Mehedi Rahman, Bishwo Prakash Pokharel, Sayed Abu Sayeed, Sujan Kumar Bhowmik, Naresh Kshetri, Nafiz Eashrak, *riskAIchain: AI-Driven IT Infrastructure – Blockchain-Backed Approach for Enhanced Risk Management, "Risks"*, Vol. 12, No. 12, 2024, https://doi.org/10.3390/risks12120206

[2] Nicoleta Anemarie Munteanu, *NATO's Mechanisms for the Governance of Cybersecurity*, "*Studia Securitatis"*, Vol. XIX, No. 1/2025, pp. 208–217

modules - particularly those related to e-Invoice, electronic cash registers, and SAF-T, may extend into 2026 or beyond.

Moreover, a Big Data system always depends on the quality of the data it processes. If the data are from diverse sources, uncertain, incomplete, inconsistent, or inaccurate, predictive models and risk analyses will lack precision and thus may be contestable. Technical capacity and infrastructure must also be optimal to handle large data volumes, timely processing, security, and efficient storage. This requires National Agency for Fiscal Administration to have robust infrastructure, data centres, and adequate hardware and software resources. Another sensitive issue is the availability of specialized personnel to operate such a platform, as well as a significant number of experts in Big Data, data science, machine learning, and cybersecurity. Unfortunately, Romania currently lacks a sufficient pool of public-sector experts in these fields.

Additionally, the protection of personal data and the confidentiality of economic and financial information are critically important. GDPR regulations, the right to privacy, professional secrecy, and similar provisions require the adoption of special measures regarding access to and processing of data. Therefore, the system must be equipped with clear operational rules, audits, authorizations, and access levels. Another significant challenge for the implementation and operation of the system is legislative changes. Excessive legislative mobility creates difficulties not only for taxpayers but also for National Agency for Fiscal Administration when expanding Big Data operations, as unpredictability can significantly hinder system operability. In theory, these systems should be flexible and easily adaptable, but this can complicate their initial development.

Finally, to provide positive and constructive responses to all these challenges, significant investments are required for licenses, infrastructure, maintenance, and updates. Project governance must be properly managed from the outset to avoid numerous interventions and corrections that would further increase implementation and operational costs. In conclusion, APIC represents a major transformation in National Agency for Fiscal Administration's operations. It will ensure a shift from resource-intensive and subjective manual inspections to intelligent, objective, and rigorous digital analysis targeting actual tax evasion. The faster it is implemented, the sooner the pressure on compliant taxpayers is reduced and the collection of public funds is improved.

Conclusions

As highlighted in key international documents[1] shaping Romania's future development, good governance encompasses the principles, processes, and mechanisms through which public institutions and organizations are managed to promote transparency, accountability, efficiency, participation, adherence to the rule of law, and integrity, thereby contributing to sustainable development and strengthening public trust.

The integration of artificial intelligence into tax administration represents a transformative opportunity for Romania, offering the potential to modernize institutional processes, enhance fiscal efficiency, and reinforce the relationship between taxpayers and the state. By enabling rapid data processing, predictive risk analysis, automation of repetitive tasks, and data-driven decision-making, AI can significantly improve revenue collection while simultaneously reducing operational inefficiencies and human error. However, the

[1] European Commission, *European Governance: A White Paper.* Publications Office of the European Union, 2019; OECD, *Principles of Good Governance,* OECD Publishing, 2015; United Nations, *Principles of Effective Governance for Sustainable Development,* United Nations Department of Economic and Social Affairs, 2021

realization of this potential depends on careful, responsible, and transparent implementation. This study emphasizes that AI adoption is not merely a technological choice but also a legal, ethical, and institutional one. Compliance with the European regulatory framework - particularly Regulation (EU) 1689/2024 - requires the rigorous application of principles such as transparency, explainability, data protection, and human oversight.

Romania's tax administration exemplifies both the opportunities and vulnerabilities associated with digital transformation. On one hand, tools such as e-Factura, RO e-Transport, SAF-T, and the APIC system demonstrate tangible progress toward an intelligent and integrated fiscal management model. On the other hand, persistent challenges - such as insufficient cybersecurity infrastructure, legislative volatility, a shortage of specialized personnel, and weak interoperability - pose risks to the reliability and effectiveness of AI-based processes.

The analysis underscores that cybersecurity is a fundamental prerequisite for credible digital administration. AI-driven attacks, exploitation of IT vulnerabilities, and breaches of fiscal data compromise not only operational capacities but also public trust - an essential pillar of any effective fiscal system. Accordingly, the successful integration of AI in Romania's tax administration necessitates a balanced approach founded on several key principles:

- Prioritizing the security and integrity of fiscal infrastructure;
- Ensuring traceability, contestability, and oversight of AI-generated decisions;
- Maintaining normative stability and legislative predictability;
- Developing human capital through targeted recruitment and specialized training.

Importantly, AI should not replace the human dimension of public administration but rather enhance its capacity, providing tools that enable authorities to act more efficiently, fairly, and intelligently. When implemented with strategic vision and operational rigor, AI can contribute to a more intelligent, transparent, and resilient fiscal administration, reinforcing the integrity of Romania's public system and strengthening citizens' trust in state institutions.

The adoption of AI in tax administration thus represents a clear developmental opportunity for Romania, capable of significantly improving governance outcomes. While the path forward entails numerous risks and challenges, fear of these threats should not serve as a deterrent. Rather, it should inspire meticulous attention to detail, enabling the maximization of benefits and the proactive identification and mitigation of potential risks.

Bibliography

Books

1. Crevier, Daniel, *AI: The Tumultuous History of the Search for Artificial Intelligence,* Basic Books, New York, 1993
2. Luger, George., F., *Artificial Intelligence: Structures and Strategies for Complex Problem Solving (5th Ed.)*, Pearson, 2005
3. McCarthy, John; Minsky, Marvin; Rochester, Nathaniel; Shannon, Claude, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, Dartmouth College Archives, 1956
4. Nilsson, Nils, John, *Artificial Intelligence: A New Synthesis*, Morgan Kaufmann, 1998
5. Panc, Daniela, *Cybersecurity at the National and International Level: Normative and Institutional Instruments*, Hamangiu, Bucharest, 2017

6. Poole, David; Mackworth, Alan; Goebel, Randy, *Computational Intelligence: A Logical Approach*, Oxford University Press, 1998
7. Russell, Stuart; Norvig, Peter, *Artificial Intelligence: A Modern Approach (4th Ed.)*, Pearson, 2021

Studies and Articles

1. Alavizadeh, Hooman; Jang-Jaccard, Julian; Alpcan, Tansu; Camtepe Seyit Ahmet, *A Markov game model for AI-based cyber security attack mitigation*, ”arXiv:2107.09258, Computer Science and Game Theory”, 2021, https://doi.org/10.48550/arXiv.2107.09258
2. Bashir, Nimra; Zafar, Muhammad Zeeshan, *AI-powered Cyberattacks: Impacts and Defense Strategies*, ”*World Journal of Advanced Research and Reviews*”, 25(3), 2025, https://doi.org/10.30574/wjarr.2025.25.3.0751
3. Campbell, Murray; Hoane, A. Joseph; Hsu, Feng-hsiung, *Deep Blue*, ”Artificial Intelligence”, 134(1–2), 2002, https://doi.org/10.1016/S0004-3702(01)00129-1
4. Catană, Emilia Lucia, *The Impact of Digitalization of Public Administration Activities on the Administrative Act: Normative, Jurisprudential, and Administrative Procedure Codification Perspectives*, “*Revista de Drept Public*”, No. 3, 2022
5. Catană, Emilia Lucia, *Modernizing Administrative Law in the Era of Digital Transformation: The Electronic Administrative Act*, ”*Revista de Drept Public*”, No. 4, 2019
6. Dragomir, Andreea Nicoleta, *The Role of Technology in Migration Management: Balancing Security, Ethics, and Human Rights*, in „*Studia Securitatis*”, 18(2), 2024
7. Ghencea, Flavia, *Digitalization of Public Services: Constraints and Opportunities for the Public Education System*, in the proceedings of the conference *Digitalization of Law and Public Administration in the Pandemic Context*, Ovidius University, Constanța, Universul Juridic Publishing, Bucharest, 2021
8. Kadapa Chenchi Reddy, Mohamad Saleem, *Anticipatory Cyber Crimes during the AI Era – An Indian Context*, ”*International Journal of Intelligent Systems and Applications in Engineering*”, 12(4), 2024
9. Munteanu, Nicoleta, Anemarie, *NATO's Mechanisms for the Governance of Cybersecurity*, ”*Studia Securitatis*”, Vol. XIX, No. 1/2025
10. Oneț, Cristina, *From Digitalization to AI in Tax Debt Administration*, ”*Revista de Drept Public*”, Supplement, 2025
11. Petlenko, Yulia; Tarnu, Lucian; Shchehliuk, Bohdan; Nate, Silviu, *Enhancing the Effectiveness of Defence Planning through the Implementation of Capability-Based Budgeting and Civilian Control*, *AJEE Journal*, 2023 https://doi.org/10.33327/AJEE-18-6.4-n000477
12. Rahman, Mir Mehedi; Pokharel, Bishwo Prakash; Sayeed, Sayed Abu; Bhowmik, Sujan Kumar; Kshetri, Naresh; Eashrak, Nafiz, *riskAIchain: AI-Driven IT Infrastructure – Blockchain-Backed Approach for Enhanced Risk Management*, „*Risks*”, Vol. 12, No. 12, 2024, article 206 https://doi.org/10.3390/risks12120206
13. Roditiș, Maria; Tabacariu, Andreea; Trăușan-Matu, Ștefan, *Image recommendation system based on social, semantic, and visual aspects*, ”*Romanian Journal of Human-Computer Interaction*”, 4(1), 2011
14. Silver, David; Huang, Aja; Maddison, Cristopher J., et al., *Mastering the game of Go with deep neural networks and tree search*, ”Nature”, 529, 2016, https://doi.org/10.1038/nature16961

15. Șoneriu, Laurențiu, *Digital Transformation of Public Administration in Romania and the European Union*, ”*Studia Securitatis*”, 2, 2023
16. Turing, Alan *Computing Machinery and Intelligence*, ”Mind”, 59(236), 1950
17. Vatamanu, Anca Florentina; Tofan, Mihaela, *Integrating Artificial Intelligence into Public Administration: Challenges and Vulnerabilities*, in *„Administrative Sciences”,* Vol. 15, No. 4, 2025, https://doi.org/10.3390/admsci15040149

Documents

1. European Commission, *European Governance: A White Paper. Publications Office of the European Union, 2019*
2. OECD, *Principles of Good Governance,* OECD Publishing, 2015
3. United Nations, United Nations Department of Economic and Social Affairs, *Principles of Effective Governance for Sustainable Development,* 2021

European Normative Acts

1. European Parliament and of the Council, *Regulation (EU) 2024/1689 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144*
2. European Parliament and of the Council, *Directives (EU) 2014/90 on marine equipment*
3. European Parliament and of the Council, *Directives (EU) 2016/797 on the interoperability of the rail system within the European Union*