Department of
Information Technology and
Information Management

Proceedings

OF INTERNATIONAL CONFERENCE

TECHNOLOGICAL INNOVATIONS AND DIGITAL SECURITY

Second Edition

May 14-15, 2026



CHIȘINĂU, 2026

ACADEMY OF ECONOMIC STUDIES OF MOLDOVA
DEPARTAMENT OF INFORMATION TECHNOLOGY AND INFORMATION MANAGEMENT

Proceedings of Scientific Articles
Presented at the International Conference

TECHNOLOGICAL INNOVATIONS AND DIGITAL SECURITY

2nd Edition

(May 14-15, 2026)

Chisinau, 2026

CZU 004.056(082)
T 32

Proceedings of Scientific Articles Presented at the International Conference "Technological Innovations and Digital Security", Second Edition (May 14-15, 2026)

Copyright 2026

Layout and technical editor: LOZAN Victoria

DESCRIEREA CIP A CAMEREI NAŢIONALE A CĂRŢII DIN REPUBLICA MOLDOVA

"Technological innovations and digital security", international conference (2 ; 2026 ; Chișinău). Technological innovations and digital security : Proceedings of Scientific Articles Presented at the International Conference, 2nd Edition, Chisinau, May 14-15, 2026 / scientific committee: Stratan Alexandru [et al.]. – Chișinău : SEP ASEM, 2026. – 300 p. : fig., tab. color.

Cerințe de sistem: PDF Reader.

Antetit.: Academy of Economic Studies of Moldova, Department of Information Technology and Information Management. – Ref. bibliogr. la sfârșitul art. – În red. aut.

ISBN 978-9975-182-48-5 (PDF).

Text : electronic.

004.056(082)
T 32

ISBN 978-9975-182-48-5 (PDF).
DOI: https://doi.org/10.53486/tids2026

© Academy of Economic Studies of Moldova, 2026
© SEP al ASEM, 2026

The editors are not responsible for the content of published scientific papers or for the opinions of the authors presented in this collection of articles.

SCIENTIFIC COMMITTEE

STRATAN Alexandru, Academician, Hab. Dr., Professor, Rector of the Academy of Economic Studies of Moldova, Republic of Moldova
COCIUG Victoria, PhD, Vice-Rector for Research and Partnerships, Academy of Economic Studies of Moldova, Republic of Moldova
CASIAN Angela, PhD, First Vice-Rector for Education, Academy of Economic Studies of Moldova, Republic of Moldova
IONESCU Bogdan, PhD, Professor, Bucharest University of Economic Studies, Romania
OHRIMENCO Serghei, Hab. Dr., Professor, Academy of Economic Studies of Moldova, Republic of Moldova
ČEKEREVAC Zoran, Hab. Dr., Professor, Editor-in-chief, MEST Journal, Belgrad, Serbia
GOGU Emilia, PhD, Bucharest University of Economic Studies, Romania
SHISHMANOV Krasimir, PhD, Professor, D. A. Tsenov Academy of Economics, Svishtov, Bulgaria
ZAHARIEV Andrey, PhD, Professor, University of Insurance and Finance, Sofia, Bulgaria
MANASTERSKA Tatiana, PhD, Professor, University of Kalisz, Poland
MIHAILA Svetlana, PhD, Academy of Economic Studies of Moldova, Republic of Moldova
VELEV Dimiter, PhD, Professor, University of National and World Economy, Bulgaria
ZLATEVA Plamena, PhD, Professor, University of National and World Economy, Bulgaria
COSTAȘ Ilie, Hab. Dr., Professor, Academy of Economic Studies of Moldova, Republic of Moldova
PARȚACHI Ion, PhD, Professor, Academy of Economic Studies of Moldova, Republic of Moldova
GUJUMAN Lucia, PhD, Academy of Economic Studies of Moldova, Republic of Moldova
TOACA Zinovia, PhD, Academy of Economic Studies of Moldova, Republic of Moldova
LOZAN Victoria, PhD, Academy of Economic Studies of Moldova, Republic of Moldova
ZGUREANU Aureliu, PhD, Academy of Economic Studies of Moldova, Republic of Moldova
ANDRONATIEV Victor, PhD, Academy of Economic Studies of Moldova, Republic of Moldova
BARACTARI Anatolie, PhD, Academy of Economic Studies of Moldova, Republic of Moldova
MACOVEI Anamaria-Geanina, PhD, Stefan cel Mare University of Suceava, Romania
DOBRIANSKA Natalia, Dr., Professor, Odesa National Technological University, Ukraine
GEORGESCU Radu-Mircea, PhD, Professor, Alexandru Ioan Cuza University of Iasi, Romania
HERȚELIU Claudiu, PhD, Professor, Bucharest University of Economic Studies, Romania
CRISTESCU Marian-Pompiliu, PhD, Professor, Lucian Blaga University, Sibiu, Romania
SHEPELEVA Olga, PhD, Odesa National Technological University, Ukraine
IONESCU-FELEAGA Liliana, PhD, Professor, Bucharest University of Economic Studies, Romania
CIOBANU Ghenadie, PhD, Senior Researcher at National Research Institute for Labour and Social Protection, Bucharest, Romania
HIRBU Eduard, PhD, Academy of Economic Studies of Moldova, Republic of Moldova
TURCAN Aurelia, PhD, Academy of Economic Studies of Moldova, Republic of Moldova
CERNEI Valeriu, expert, CISA, CRISC, ITIL, Republic of Moldova

ORGANIZING COMMITTEE

Republic of Moldova / Academy of Economic Studies of Moldova

GUJUMAN Lucia, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

OHRIMENCO Serghei, Hab. Dr., Professor, Laboratory of Information Security, Academy of Economic Studies of Moldova, Republic of Moldova

TOACA Zinovia, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

LOZAN Victoria, PhD, Academy of Economic Studies of Moldova, Republic of Moldova

CATRUC Adriana, PhD Student, Academy of Economic Studies of Moldova, Republic of Moldova

HINCU Veronica, Academy of Economic Studies of Moldova, Republic of Moldova

CEBAN Svetlana, Academy of Economic Studies of Moldova, Republic of Moldova

International Members

IONESCU Bogdan, PhD, Professor, Bucharest University of Economic Studies, Romania

GOGU Emilia, PhD, Bucharest University of Economic Studies, Romania

MACOVEI Anamaria-Geanina, PhD, Stefan cel Mare University of Suceava, Romania

SHISHMANOV Krasimir, PhD, Professor, Department of Business Informatics of the D.A.Tsenov Academy of Economic, Svishtov, Bulgaria

ZAHARIEV Andrey, PhD, Professor, University of Insurance and Finance, Sofia, Bulgaria

VELEV Dimiter, PhD, Professor, University of National and World Economy, Bulgaria

DOBRIANSKA Natalia, Dr., Professor, Odesa National Technological University, Ukraine

MANASTERSKA Tatiana, PhD, Professor, University of Kalisz, Poland

ČEKEREVAC Zoran, Hab. Dr., Professor, Editor-in-chief, MEST Journal, Belgrad, Serbia

PREFACE

The proceedings volume includes the papers presented at the Second Edition of the International Conference "Technological Innovations and Digital Security" organized by the Department of Information Technology and Information Management of the Academy of Economic Studies of Moldova, in collaboration with partner universities from Romania, Bulgaria, Ukraine, and Poland. The conference provides an academic framework for dialogue, the dissemination of research findings, and the exchange of experience among researchers, academics, information technology specialists, and representatives of the business sector and public institutions.

Building on the scientific initiative launched through its first edition, TIDS-2026 broadens its thematic scope, addressing artificial intelligence, data science, digital transformation, emerging technologies, and information systems security from an integrated perspective. This broader focus reflects the need to examine technological innovation not only in terms of technical performance, but also in relation to the economic, institutional, educational, and social implications of its use.

As intelligent technologies become increasingly integrated into economic activities and everyday life, the opportunities offered by digitalization are accompanied by challenges concerning data protection, infrastructure reliability, the transparency of decision-making processes, and the responsible use of artificial intelligence. The interdependence of innovation, security, and resilience calls for interdisciplinary approaches capable of supporting the development of secure, adaptable digital ecosystems that respond to societal needs.

The conference proceedings are structured into four thematic sections:

Artificial Intelligence, Data Science and Computational Intelligence
Digital Transformation, Interdisciplinary Applications and Societal Impact
Emerging Digital Technologies and Intelligent Infrastructures
Digital Security, Cybersecurity and Resilient Information Systems

By connecting fundamental research with practical implementation, this structure addresses critical dimensions such as digital skills development, privacy protection, and system trustworthiness. Furthermore, the cross-border academic cooperation supporting the conference fosters valuable institutional exchanges and strengthens the alignment between research outcomes and real-world digital needs.

This proceedings volume reflects the scientific community's commitment to understanding and responsibly harnessing technological innovation. By bringing together the contributions presented at TIDS-2026, it supports the continuation of academic dialogue and promotes a culture of digital transformation grounded in research, cooperation, security, and responsibility toward society.

Acknowledgements

We extend our gratitude to all participants, authors, and members of the scientific and organizing committees for their valuable contributions to the realization of this second edition of the Technological Innovations and Digital Security conference. The Scientific Committee gratefully acknowledges the support of the ASEM Scientific Library in the preparation and publication of this proceedings volume.

CONTENTS

PHD 2.0 – NEW AI CHALLENGES, NEW RULES, NEW ACTIONS _____ 10
Andrei ZAHARIEV

AI AS A TOOL, NOT AN INVENTOR: THE DABUS CASE AND THE LEGAL LIMITS OF AUTONOMOUS INVENTORSHIP _____ 18
Svetlana GRIȘCIUC-BUCICA

BLOCKCHAIN TECHNOLOGY IN CONSTRUCTION DOCUMENTATION M ANAGEMENT AND PREVENTION OF DOCUMENT FORGERY _____ 27
Mariana VATAMANITA, Alexandru MARIT

INTEGRATING ARTIFICIAL INTELLIGENCE TOOLS IN THE VOCATIONAL TRAINING OF IT TECHNICAL SUPPORT OPERATORS: OPPORTUNITIES AND CHALLENGES____ 38
Ion COSTIN, Victoria LOZAN

FROM PREDICTIVE TO GENERATIVE: A COMPUTATIONAL FRAMEWORK FOR MITIGATING INFORMATION ASYMMETRY IN DIGITAL MARKETPLACES _____ 51
Steliana VASILEVA

DYNAMIC PRICING IN AIRLINES: EFFICIENCY GAINS VS CONSUMER FAIRNESS IN THE MACHINE LEARNING ERA _____ 61
Anatolie BARACTARI, Anatolie BARACTARI

ETHICAL ASPECTS OF THE USE OF ARTIFICIAL INTELLIGENCE IN EDUCATION: INSTITUTIONAL, PEDAGOGICAL AND STUDENT LEVELS_____ 68
Mihail CROITOR, Tudor BRAGARU

DATA-DRIVEN DECISION MAKING IN DIGITAL BUSINESSES: TOOLS, LIMITS, AND MANAGERIAL IMPLICATIONS _____ 77
Tatiana BUCOS

AI-ASSISTED DATA ANALYSIS: THE BALANCE BETWEEN AUTOMATION, ANALYTICAL CONTROL AND HUMAN DECISION IN THE EXCEL ECOSYSTEM _____ 88
Maria MORARU, Varvara TAPCOV

SUSTAINABILITY OF FREIGHT TRANSPORT COMPANIES IN THE CONTEXT OF INCOME AND EXPENSE INDICATOR ANALYSIS (BASED ON LOCAL COMPANY DATA) _____ 96
Eugeniu STOIAN, Serghei PORTARESCU, Ion NEGRU

CHALLENGES FOR YOUTH POLICIES IN THE DIGITAL ENVIRONMENT USING ARTIFICIAL INTELLIGENCE TOOLS _____ 105
Monika YANAKIEVA

SOME INFORMATIONAL ASPECTS OF DECISION-MAKING IN MONOPOLISTIC PRODUCTION SYSTEMS _____ 111
Anatolie BARACTARI, Anatol GODONOAGĂ

DIGITAL TRANSFORMATION IN TOURISM: LEVERAGING PRACTICAL DIGITAL GUIDES FOR PROMOTING THE REPUBLIC OF MOLDOVA AS A TOURIST DESTINATION _____ 119
Valentina CAPAȚINA, Irina ISPIR, Adriana PROCA

ANALYSIS OF THE PUBLIC WARNING SYSTEM _____ 126
Serghei PEANCOVSCHII

ARTIFICIAL INTELLIGENCE, PRODUCTIVITY GROWTH, AND UNIVERSAL BASIC INCOME: A THEORETICAL DEBATE IN ECONOMIC THOUGHT _____ 133
Mihail CIOBANU

PROMOTING INNOVATIVE PRODUCTS IN THE AGRICULTURAL BUSINESS ENVIRONMENT AND EDUCATION FOR DIGITALIZATION: AN ANALYSIS OF THE CURRENT CONTEXT AND SOCIO-ECONOMIC IMPACT _____ 142
Mioara MIHĂILĂ, Andy-Felix JITĂREANU, Andromeda SONEA-PĂTRAȘCU, Tatiana BALTAG, Dan BODESCU

DIGITAL IDENTITY AND ARTIFICIAL INTELLIGENCE ETHICS IN ORTHODOX SOCIETY _____ 151
Sergey BAZHENOV, Elena BAZHENOVA, Dmitry ABROSIMOV

CYBER RESILIENCE STRATEGIES: SPIRITUAL AND SOCIAL ASPECTS _____ 156
Sergey BAZHENOV, Elena BAZHENOVA, Dmitry ABROSIMOV

SOCIO-ECONOMIC RISKS ASSOCIATED WITH DIGITALIZATION PROCESS IN THE FIELD OF ECOLOGY AND ENVIRONMENT PROTECTION _____ 162
Elena MARGINEANU

FROM CRISIS TO CATALYSIS: THE IMPACT OF THE COVID-19 PANDEMIC-DRIVEN DIGITALIZATION ON ECONOMIC OUTCOMES AND ORGANIZATIONAL TRANSFORMATION _____ 171
Ion PÂRȚACHI, Simion MIJA, Claudiu HERȚELIU

TRANSFORMATION IN BUSINESS AND WORKFORCE DISPLACEMENT IN MOLDOVA'S IT SECTOR _____ 178
Veronica HÎNCU

IMPLEMENTATION OF DATA MINING TECHNIQUES IN THE PRIVATE SECTOR OF THE REPUBLIC OF MOLDOVA: CASE STUDIES AND COMPETITIVE ADVANTAGES _____ 183
Vitalie URSACHI, Emilia GOGU

THE EVOLUTION OF WI-FI NETWORKS ____ 191
Victor ANDRONATIEV, Aureliu ZGUREANU

EVALUATION OF ELECTRIC VEHICLE CHARGING INFRASTRUCTURE IN A DENSE URBAN ENVIRONMENT: A CASE STUDY OF THE CENTRAL SECTOR, CHISINAU ____ 200
Victoria LOZAN, Ion COSTIN

TOWARDS SUSTAINABLE SMART HOMES: A MODULAR ARCHITECTURE ENHANCING DEVICE EFFICIENCY, INTEROPERABILITY AND LONGEVITY ____ 210
Adriana CATRUC

DIGITAL RISK MANAGEMENT IN RELATIONAL AND NON-SQL DATABASES ____ 216
Serghei OPREA, Aureliu ZGUREANU

FROM THREAT INTELLIGENCE TO ECONOMIC METRICS: LLM-SUPPORTED CYBER RISKOPS FOR CONTINUOUS SV/ROSI ASSESSMENT ____ 224
Ghenadie BELINSCHI, Irina DOROGAIA

ANALYSIS OF THE MAIN THREATS IN THE SPHERE OF CYBERSECURITY ____ 233
Olga PUGACHEVA

FROM SECURITY TO EDUCATION: CHOOSING PROGRAMMING LANGUAGES FOR CS1 AND CS2 ____ 241
Zinovia TOACĂ, Lucia GUJUMAN

INFORMATION SECURITY IN DIGITAL AGRO-TOURISM: CHALLENGES ASSOCIATED WITH IOT AND BIG DATA TECHNOLOGIES ____ 248
Svetlana CEBAN

SECURITY CHALLENGES IN VIDEO CONFERENCING APPLICATIONS: A CASE STUDY ON MICROSOFT TEAMS ____ 254
Aureliu ZGUREANU, Serghei OPREA

THE ECONOMICS OF DIGITAL CRIME: UNDERSTANDING THE CYBERCRIME VALUE CHAIN ____ 262
David NAVAS, Ivan KULAKOV, Dinara ORLOVA

HUMAN FACTORS IN CYBERSECURITY: FROM HUMAN ERROR TO SOCIO-TECHNICAL RESILIENCE ____ 270
Evelina STEBNITSKAIA, Daria KOZLOVA, Dinara ORLOVA

CYBERSECURITY MANAGEMENT MODELS IN HIGHER EDUCATION INSTITUTIONS ACCORDING TO NIS2 REQUIREMENTS ____ 278
Krasimir SHISMANOV, Yuriy KUZNETSOV, Iskren TAIROV

METAMORPHOSES OF THE SHADOW DIGITAL ECONOMY _____ 284
Serghei OHRIMENCO, Dinara ORLOVA; Ghenadie BELINSCHI

CHALLENGES OF ARTIFICIAL INTELLIGENCE IMPLEMENTATION IN CYBERSECURITY OF SMES FROM THE REPUBLIC OF MOLDOVA IN THE CONTEXT OF ACCELERATED DIGITALISATION _____ 291
Lucia GUJUMAN, Emilia GOGU, Zinovia TOACĂ, Vitalie URSACHI

PLENARY SECTION

PHD 2.0 – NEW AI CHALLENGES, NEW RULES, NEW ACTIONS

CZU: 004.8:001.891
DOI: https://doi.org/10.53486/tids2026.01

ANDREY ZAHARIEV
University of Insurance and Finance, Sofia, Bulgaria
e-mail: a.zahariev@uzf.bg
ORCID ID: 0000-0001-7362-6133

Abstract. The rapid integration of AI in academic research represents both an opportunity for positive digital transformation and a significant challenge to the core principles of doctoral studies – authorship, originality and integrity. The unregulated use of AI risks undermining the main purpose of the doctoral degree: the formation of an independent-thinking researcher. With this study, we argue for a structured action plan including: First, a National Framework for Academic Integrity in the Use of AI, embedded in legislative texts and establishing minimum standards in all higher education institutions; Second, mandatory institutional regulations regulating doctoral programs and academic journals, directly linked to the university accreditation processes; Third, a National Registry of Declarations for the Use of AI – a centralized platform integrated with the national anti-plagiarism system to prevent the re-submission of manuscripts assisted by AI; and Fourth, a National Program for Training of PhD Students, Supervisors, and Academic Staff, delivered through doctoral schools and supported by funding from the Ministry of Education and Science. In addition to regulation, true prevention requires a transformed academic environment for conducting doctoral studies. Seven pedagogical and organizational measures are proposed: introductory training in research literacy in the field of artificial intelligence; structured, step-by-step reviews of dissertations; research journals and portfolios as evidence of authentic authorship; doctoral seminars with anonymous peer review; psychological support and management of academic pressure; shifting the focus of assessment from the final product to a documented process; and positive incentives for transparent and responsible use of AI. The goal is not to eliminate AI from doctoral research, but to cultivate researchers capable of engaging with it critically and ethically. Properly integrated, AI has the potential to accelerate doctoral doctoral degree within approximately 24 months. Thus, AI will be a jointly accepted third party that supports literature review, academic writing, and critical thinking.

Keywords: Artificial intelligence; Doctoral degree; Academic integrity; Research ethics; AI regulation; Responsible AI use

JEL Classification: A20, I23, O33, I28.

INTRODUCTION

Artificial intelligence is rapidly entering all spheres of modern society, and academia is no exception. Doctoral studies, as the highest form of scientific training, face an unprecedented challenge: how to integrate the capabilities of AI technologies without compromising their fundamental goals of forming an independent-thinking researcher with proven scientific competence. The question is no longer whether doctoral students use AI tools, but how, to what extent, and under what conditions this use remains ethical and academically honorable. The global spread of generative AI models such as ChatGPT, Gemini, and Claude has placed higher education institutions and scientific organizations in a regulatory vacuum. The lack of uniform standards creates inequality between institutions, blurs the line between authorship and assisted text generation, and threatens the

legitimacy of academic degrees and procedures for academic growth. In the context of national regulatory frameworks, the problem is particularly acute. National legislation and institutional policies are largely not yet adapted to the realities of AI-assisted scientific writing and research.

This report aims to analyze the risks and opportunities of the use of artificial intelligence in doctoral education and to propose specific regulatory and pedagogical measures to promote the responsible and transparent use of AI tools in scientific research. The initial hypothesis of the report is that the unethical and unregulated use of artificial intelligence in doctoral studies is not the result solely of a lack of will among doctoral students, but is a systemic problem caused by an institutional vacuum, insufficient AI literacy and a lack of a preventive environment for the training of young scientists. Therefore, an adequate response requires both regulation, training and a change in academic culture. Despite the growing academic interest in the topic, there is a significant gap in the scientific literature regarding integrated national models for the regulation of AI use specifically in doctoral education. Most existing research focuses on student plagiarism or general AI policy at the university level, without considering the specifics of doctoral studies as a research process with unique requirements for authorship and originality.

The report is structured in three main parts. The first part examines the risks of unethical use of AI in the context of doctoral education. The second part proposes seven pedagogical and organizational prevention measures aimed at building an environment that stimulates critical and responsible interaction with AI tools. The third part presents a four-point action plan at the national and institutional levels. The report concludes with conclusions and recommendations for the academic community and institutions in the field of higher education.

MAIN CONTENT

1. Risks of using AI in doctoral studies

The entry of generative artificial intelligence into the academic environment calls into question a number of enduring principles of scientific knowledge, mainly related to authorship, originality and academic integrity. Doctoral studies, as a process of forming a research identity, are particularly vulnerable to these transformations. The risks can be systematized into three main categories: risks to academic integrity, risks to research competence and risks at the systemic-institutional level. The most immediate risk is related to the blurring of the line between authorship and AI-assisted text generation. Modern generative models are capable of producing academic-sounding texts that pass standard anti-plagiarism checks, since they do not copy existing sources verbatim, but generate new text based on statistical models. This phenomenon, also known as "new generation academic fraud", has been documented in a number of studies (Perkins et al., 2023; Cotton et al., 2024). The problem is exacerbated by the fact that tools for detecting AI-generated content are still not reliable enough and give a significant percentage of false positives and false negatives (Liang *et al.*, 2023). In addition to text generation, there are documented cases of AI being used to fabricate bibliographic references. This is the so-called "hallucinations" of language models, in which the system generates non-existent sources with plausible-looking bibliographic identification and authors (Athaluri *et al.*, 2023). This poses a particularly serious risk in the context of a doctoral dissertation, the scientific value of which is inextricably linked to the correctness and verifiability of the sources used. A deeper, but more difficult to measure, risk is related to the impact of excessive AI use on the development of the doctoral student's research skills. Doctoral studies are primarily a learning process in which critical thinking, argumentation, literature synthesis and the formulation of an original contribution to

knowledge are developed. When these cognitive processes are delegated to AI systems, the doctoral student is deprived of the opportunity to develop them fully (Fyfe, 2023; Bender *et al.*, 2021). Research in the field of educational psychology shows that dependence on technological tools in the performance of complex cognitive tasks leads to the so-called "cognitive overload" with long-term negative effects on independent thinking (Gerlich, 2023). In the field of doctoral studies, this means that graduates may hold a formal academic degree without having developed the real research competence that it certifies. At the institutional and systemic level, the unregulated use of AI generates risks for the legitimacy of academic degrees and the trust in scientific publications. If the standards for AI use differ significantly between individual universities or national systems, this creates inequality and undermines the mutual recognition of scientific degrees and results (UNESCO, 2023; European Parliament & Council of the European Union, 2024). An additional institutional risk is associated with academic journals. A number of leading scientific journals have already registered cases of AI-generated manuscripts successfully passing the review process, which calls into question the reliability of the peer review system (Stokel-Walker & Van Noorden, 2023). Last but not least, there is a risk of deepening inequalities in access to quality doctoral education - doctoral students with better access to paid AI tools and higher AI literacy gain an informal competitive advantage, which contradicts the principles of academic justice (Holmes *et al.*, 2022).

The definition of the three categories and levels of manifestation of unethical use of AI in the doctoral degree should also address the impact of specific factors that increase the risk of AI misuse. Based on the review of objective academic processes and observations of the system by the author of this study, these factors should include:

- the presence of unclear expectations among doctoral students for permissible use of AI;
- the establishment of excessively long periods without feedback between the doctoral student and the scientific supervisor;
- the focus on assessing only the final product – the dissertation and the abstract, and not the process of training in the doctoral degree;
- the creation of a framework for excessive autonomy and individuality of training in the doctoral degree with the isolation of the doctoral student from the processes in the academic community;
- the objective presence of fear of failure and failure to cope with the requirements of the scientific supervisor and the high standard imposed by the teaching department;
- conservative conduct of public defenses of doctoral dissertations with limited verbal expression by doctoral students, at the expense of an extended expression by the chairman of the jury and reviewers;
- lack of a regulatory framework for recognition of ethical use of AI at the doctoral level and of written rules for achieving research goals through ethical use of AI.

2. Framework of new rules: Measures to prevent unethical use of AI in the doctoral degree

The current pedagogical and organizational measures are aimed at eliminating the root causes of the problem of unethical use of AI by doctoral students after enrollment in a doctoral degree. They aim to reduce pressure, increase engagement and build a research identity in which authorship is a value, not a burden, in conditions of possible acceleration of the accumulation of ECTS credits, according to the individual plan of the doctoral student.

First measure: Introductory training for research literacy with AI. The key principle of this measure is that training should present AI as a tool with clear boundaries, not as a threat. Doctoral students who understand the meaning behind the rules are significantly less likely to violate them. The measure is aimed at developing literacy for the use of AI and academic integrity and contains mandatory training after enrollment in the doctoral degree including:

- Introductory module (minimum 4 teaching hours) for each newly admitted doctoral student, including: the principles of academic integrity; specific examples of permitted and inadmissible use of AI; practical exercises with completion of the AI Declaration; discussion of case studies from the relevant scientific discipline.
- Annual refresher training (2 hours) for all doctoral students, reflecting innovations in technologies and regulations.
- Training for scientific supervisors on the application of the regulations and recognition of problematic cases.
- Online platform with resources, examples and updated guidelines, available to all doctoral students and supervisors.

Second measure: Structured phased reviews of the work of doctoral candidates. When the research process is visible and documented, misuse is more difficult, and the doctoral student receives timely support. Phased reviews reduce pressure at the end of the doctoral program, when the predominant percentage of cases of AI misuse are identified. The measure monitors the research process, not just the final product, and includes:

- Mandatory regular meetings between the doctoral student and scientific supervisor: at least once a month for full-time students; at least once every two months for part-time students.
- Presentation by the doctoral student at these meetings of specific progress: written sections, analyzed data, read literature, which is to be confirmed in writing and defended verbally.
- Documentation of progress by the supervisor and quarterly attestation assessment of progress with digital storage of the versions and structural components of the dissertation work.
- Public preliminary defenses before the primary unit of the dissertation work of the theoretical framework with the literature review and the empirical research with the presentation of the contributions.
- Documentation of all described activities with signed protocols by the doctoral student and the supervisor.

Third measure: Research diary and research portfolio. Authorship is a documented process in which:

- Each doctoral student maintains a research diary: weekly entries on literature read, decisions made, difficulties encountered and ways to overcome them.
- The diary is a personal document shared with the supervisor upon request in search of support, not for evaluation.
- The research portfolio includes: drafts, file versions, data, program codes, correspondence with the supervisor and abstracts from research meetings.

- The portfolio serves as natural proof of authorship and significantly reduces the incentive to use AI to generate text.
- The digital documentation of the completion of the research diary is organized in a secure cloud environment, to the doctoral student's institutional email address.

Fourth measure: Doctoral seminars and anonymous peer review. When a doctoral student regularly defends his ideas orally in front of colleagues, the construction of his own scientific identity becomes a natural process. This is the most effective long-term prevention against abuse. The goal is to build an environment in which authorship is socially and digitally visible through the ResearchGate open science platform and using the nomenclature for sharing the stages of abstract, preprint, presentation (in scientific forums and reports) and final author's product (report, article, studies, abstract or dissertation). The measure includes:

- Regular doctoral seminars (at least once a semester) with oral presentation of progress to colleagues and supervisors.
- Structured peer review at the inter-doctoral level: each doctoral student reviews and receives a review from a colleague according to a pre-set algorithm.
- Roundtables for discussion of methodological issues, quantitative and qualitative research methods with the creation of an environment in which the recognition of uncertainty is the norm, not a weakness.
- Annual doctoral scientific conference with public presentation of research results from the doctoral curriculum and digital publication of the Almanac with scientific research of doctoral students.
- Doctoral mentoring program, including the engagement of postdoctoral students as mentors for newly enrolled doctoral students.

Fifth measure: Psychological support and management of academic pressure. The measure is aimed at institutional support for the success of doctoral students, combined with reducing pressure as a major risk factor, which should include:

- Access to basic level consulting and training for writing academic output in a finished form - scientific report, article and studies.
- With a leading role for the scientific supervisors who train doctoral students, normalizing the iterative nature of the research process, in which drafts, mistakes and revisions are a normal part of science.
- Setting clear and realistic deadlines, discussed and accepted by the doctoral student, and not imposed unilaterally through an individual plan with standard deadlines.
- Early identification of doctoral students at risk who are lagging behind in the implementation of the tasks of the individual plan and demonstrate reservations in future public defense with an established long-term lack of progress and isolation, requiring proactive support.
- Training supervisors to recognize symptoms of burnout, with tools to interrupt training for a certain period and continue training after catching up.

Sixth measure: Change the design of assessment formats. Assessment formats determine what doctoral students consider important. If the assessment is based solely on a final written product, the incentive for AI abuse is maximum. Changing the design of assessment formats radically reduces this incentive and includes:

- Including a mandatory oral presentation and defense of the methodology before the final defense. AI abuse is easily recognizable in oral presentations: the doctoral student cannot defend ideas that he or she did not understand.
- Assess the process, documented through the research diary and portfolio as a formal component of the attestation. The research portfolio documents the real contribution and makes AI-generated content visibly incompatible.
- Defense of analytical and methodological decisions in concrete terms with public justification of the choice of a specific methodology instead of an alternative methodology, with assessments of the stationarity of the studied databases. AI cannot explain individual research choices that have a subjective foundation.
- Seminar format of the doctoral program with public presentation of the completed chapters of the dissertation before the primary unit. The publicity of the presentation builds responsibility and identity.
- Setting problem-oriented tasks for the doctoral student, requiring local data or a specific context unknown to AI. AI systems do not have access to specific regional/national context, field data and unique observations.

Seventh measure: Positive incentives for responsible use of AI. In addition to prevention through restrictions, the institution can actively encourage and recognize the responsible use of AI, through listed positive incentives:

- Public recognition for doctoral students demonstrating exemplary declaration and responsible use of AI.
- Inclusion of the topic of AI and research integrity as a problem area for discussion in doctoral seminars and for scientific publications.
- Support for doctoral students developing methodologies that include AI tools in a transparent manner.
- Inclusion in the attestation of competencies for critical and responsible use of AI.
- Awards and distinctions for scientific creativity demonstrating exemplary transparent declaration of ethical use of AI.

The proposed seven measures with specific actions towards them are open-ended and can be enriched and profiled depending on the scientific field and professional direction of the doctoral studies.

3. Action plan

The dynamic penetration of AI into the academic environment confronts higher education institutions with the need for an urgent, coordinated and multi-layered institutional response. The existing regulatory framework in European countries, incl. Bulgaria, still does not contain specific provisions governing the use of AI tools in research and doctoral training. This regulatory vacuum creates prerequisites for inequality between institutions, dilutes the standards of academic integrity and questions the legitimacy of the acquired scientific degrees. The European framework, outlined in Regulation (EU) 2024/1689 on artificial intelligence (European Parliament & Council of the European Union, 2024), sets the horizon of regulation at the European level, but does not provide solutions relevant to ERA & EHEA, which makes national action not only justified, but also mandatory. International experience shows that institutions that have adopted clear policies for the use of AI (here we can distinguish the Massachusetts Institute of Technology, the University of

Edinburgh, Uppsala University, etc.) register a higher degree of academic integrity and greater trust from the scientific community in the degrees they issue. The lack of a national policy risks turning regulation into a mosaic of contradictory institutional solutions, which is particularly problematic in the context of the mutual recognition of scientific degrees within the European Research Area (ERA). On this basis and in accordance with the principles of preventive academic risk management, at the end of this prospective study I take the liberty of proposing a structured action plan (Zahariev, 2026a), organized into four interconnected and consistently built priorities, covering the normative, institutional, administrative and educational dimensions of the problem.

First of all, we put the drafting of a national framework for academic integrity when using AI. It is necessary to prepare a Working Committee under the Ministry of Education and Science and subsequently adopt a national regulatory framework with standards for the ethical use of AI in science and higher education. This framework should be integrated into the current laws and regulations thereto. The framework should define the minimum requirements applicable to all higher education institutions and scientific organizations and create the legal basis for the development of institutional regulations.

Secondly, we emphasize the importance of discussing and adopting institutional regulations for the ethical use of AI in higher education institutions. The Ministry of Education and Science should introduce a requirement for higher education institutions and scientific organizations to adopt regulations for the ethical use of AI, covering the doctoral degree, procedures for academic positions and the scientific periodicals of the respective institution. The requirement to adopt such regulations should be included in the criteria system of the National Agency for Assessment and Accreditation, making it a condition for institutional accreditation.

Thirdly, we draw attention to the importance of documenting the process by creating a national register of declarations for the use of AI in scientific works. A centralized platform for storing declarations for the use of AI, linked to the national plagiarism checking system, should be created at the Ministry of Education and Science. The platform should ensure interoperability between institutions and prevent the re-submission of the same AI-assisted work in different higher education institutions.

Finally, we place the launch of a National Training Program in fourth place. With funding from the relevant ministry, a national program for training doctoral students, scientific supervisors and members of the academic staff in the critical and responsible use of AI should be launched. The program should be integrated into doctoral schools and include annual scientific forums for sharing good practices between institutions.

CONCLUSIONS

PhD studies are a process of forming a research identity. When a PhD student understands the meaning of his/her own work, has support and receives recognition, he/she turns AI into a tool, not a temptation. No detection technology can replace an environment of trust, clear expectations and a real academic community (Zahariev, 2026b). Preventive pedagogical measures are the long-term investment with the highest return on academic integrity. The goal is not zero use of AI. The goal is to train PhD students who have developed skills to use AI critically, transparently and in the service of their own thinking.

REFERENCES

Athaluri, S. A., Manthena, S. V., Kesapragada, V. S. R. K. M., Yarlagadda, V., Dave, T., & Duddumpudi, R. T. S. (2023). Exploring the boundaries of reality: Investigating the phenomenon of artificial intelligence hallucination in scientific writing through ChatGPT references. Cureus, 15(4). https://doi.org/10.7759/cureus.37432

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, 610–623. https://doi.org/10.1145/3442188.3445922

Cotton, D. R. E., Cotton, P. A., & Shipway, J. R. (2024). Chatting and cheating: Ensuring academic integrity in the era of ChatGPT. Innovations in Education and Teaching International, 61(2), 228–239. https://doi.org/10.1080/14703297.2023.2190148

European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689. https://data.europa.eu/eli/reg/2024/1689/oj

Fyfe, P. (2023). How to cheat on your final paper: Assigning AI for undergraduate writing classes. AI & Society, 38, 1395–1405. https://doi.org/10.1007/s00146-022-01397-z

Gerlich, M. (2023). AI tools in society: Impacts on cognitive offloading and the future of critical thinking. Societies, 13(1). https://doi.org/10.3390/soc15010006

Holmes, W., Porayska-Pomsta, K., Holstein, K., Sutherland, E., Baker, T., Shum, S. B., Santos, O. C., Rodrigo, M. T., Cukurova, M., Bittencourt, I. I., & Koedinger, K. R. (2022). Ethics of AI in education: Towards a community-wide framework. International Journal of Artificial Intelligence in Education, 32, 504–526. https://doi.org/10.1007/s40593-021-00239-1

Liang, W., Yuksekgonul, M., Mao, Y., Wu, E., & Zou, J. (2023). GPT detectors are biased against non-native English writers. Patterns, 4(7). https://doi.org/10.1016/j.patter.2023.100779

Perkins, M., Roe, J., Postma, D., McGaughran, J., & Hickerson, D. (2023). Game of Tones: Faculty detection of GPT-4 generated content in university assessments. PLOS ONE, 18(12). https://doi.org/10.1371/journal.pone.0283956

Stokel-Walker, C., & Van Noorden, R. (2023). What ChatGPT and generative AI mean for science. Nature, 614, 214–216. https://doi.org/10.1038/d41586-023-00340-6

UNESCO. (2023). Guidance for generative AI in education and research. UNESCO Publishing. https://doi.org/10.54675/EWZM9535 [Accessed on 25 April 2026]

Zahariev, A. (2026a). Artificial Intelligence in the Educational and Scientific Degree „Doctor“: Digitalization, Regulation and Credit Acceleration. Fourth national scientific-practical conference with international participation digital transformation of education - issues and solutions (Book of abstracts), p. 6. https://www.conf-dte.bg/proceeding-abstracts.html

Zahariev, A. (2026b). Artificial Intelligence in the „Doctor“ Degree (Presentation). Fourth national scientific-practical conference with international participation digital transformation of education - issues and solutions, ResearchGate, 30 pages, https://doi.org/10.13140/RG.2.2.15951.65446

AI AS A TOOL, NOT AN INVENTOR: THE DABUS CASE AND THE LEGAL LIMITS OF AUTONOMOUS INVENTORSHIP

CZU: 004.8:347.77
DOI: https://doi.org/10.53486/tids2026.02

SVETLANA GRIȘCIUC-BUCICA
Free International University of Moldova (ULIM)
e-mail: svetlana_lawyer@yahoo.com
ORCID ID**:** 0009-0005-5590-3180

Abstract. The rapid development of artificial intelligence has challenged one of the fundamental assumptions of patent law: the idea that inventorship is inherently linked to human intellectual activity. As AI systems become increasingly capable of generating technical solutions, questions arise regarding the adequacy of traditional patent concepts in the context of AI-generated innovation.

This paper examines the DABUS case as the first global legal attempt to test the possibility of autonomous inventorship. Through a comparative analysis of decisions adopted by patent offices and courts in the United States, the United Kingdom, the European Patent Office, Australia, Germany, South Africa, and several other jurisdictions, the study identifies the principal legal approaches developed in response to AI-generated inventions.

The analysis demonstrates that despite differences in legal reasoning and procedural frameworks, most jurisdictions continue to associate inventorship with human intellect, intention, and legal responsibility. Three principal regulatory models can be identified: strict human inventorship, human-attribution approaches, and procedural acceptance approaches. Although these models differ in their treatment of AI-generated inventions, none recognizes artificial intelligence as an autonomous inventor.

The paper argues that the significance of DABUS extends beyond the formal question of whether an AI system may be designated as an inventor. The case exposed a deeper tension between rapidly evolving technological capabilities and legal concepts developed within a human-centered framework of innovation. In this sense, DABUS case should be understood not merely as a patent dispute, but as a legal test of whether the traditional doctrine of inventorship can withstand the challenges posed by AI-generated innovation.

Keywords: inventorship, patent law, artificial intelligence, DABUS, AI-generated inventions, intellectual property.

JEL Classification: K11, K24, O34, O38

INTRODUCTION

For centuries, intellectual property law has been built around the assumption that creativity and invention are inherently human activities. The legal concept of inventorship emerged in a technological environment where the inventor was naturally understood as a human being capable of intellectual effort, intention, and creative judgment. As a result, patent law evolved around a fundamentally anthropocentric model in which inventorship, ownership, and legal responsibility were inseparable from human agency.

Recent advances in artificial intelligence have challenged this traditional paradigm. Contemporary AI systems are increasingly capable of generating technical solutions, optimizing engineering designs, discovering new compounds, and producing innovative outputs with varying degrees of human involvement. While these developments have created significant opportunities for technological progress, they have also generated uncertainty regarding the applicability of existing intellectual property frameworks to AI-generated innovation.

The legal debate surrounding artificial intelligence is no longer limited to questions of technological capability. Instead, attention has shifted toward the legal consequences of algorithmically generated outputs and the adequacy of existing regulatory mechanisms. Within patent law, one of the most controversial issues concerns inventorship: if an invention is generated by an artificial intelligence system, who should be recognized as the inventor?

This question became the subject of global attention through the DABUS case. Developed by Dr. Stephen Thaler, DABUS (Device for the Autonomous Bootstrapping of Unified Sentience) was presented as an artificial intelligence system capable of generating patentable inventions without direct human conception of the inventive idea (*Ryan Abbott, 2020*). Patent applications filed in multiple jurisdictions identified DABUS itself as the inventor, thereby challenging one of the most deeply rooted assumptions of patent law (*Ryan Abbott, 2020*).

The significance of the DABUS litigation extends beyond the fate of a particular patent application. The case became the first large-scale legal experiment testing whether existing patent systems are capable of accommodating AI-generated innovation without fundamentally altering the traditional concept of inventorship *(Wenting Cheng, 2024).* Responses from patent offices and courts around the world revealed significant differences in legal reasoning while simultaneously demonstrating a remarkable consistency in preserving the human-centered foundations of patent law.

Against this background, the present paper examines the DABUS case as a legal test of autonomous inventorship. Through a comparative analysis of major jurisdictions, including the United States, the United Kingdom, the European Patent Office, Germany, Australia, and South Africa, the study seeks to identify the principal legal approaches that have emerged in response to AI-generated inventions and to evaluate their implications for the future development of patent law *(Zahra Shakeri, Zohreh Gheisari Atrabi, 2024).*

The paper argues that the importance of DABUS lies not in the possibility of recognizing artificial intelligence as an inventor, but in exposing the legal limits of existing inventorship doctrine in the era of AI-assisted innovation.

MATERIALS AND METHODS

This study employs a comparative legal research methodology to examine the legal treatment of AI-generated inventions through the lens of the DABUS litigation. The research is based on the analysis of judicial decisions, patent office determinations, international patent procedures, and academic literature addressing the relationship between artificial intelligence and patent law.

The primary sources include decisions and official positions adopted by the United States Patent and Trademark Office (USPTO), the United Kingdom Intellectual Property Office (UKIPO), the European Patent Office (EPO), the Federal Court of Australia, the German Federal Court of Justice (Bundesgerichtshof), and other national authorities involved in the examination of DABUS-related patent applications. The study further considers international developments within the framework of the World Intellectual Property Organization (WIPO) and the Patent Cooperation Treaty (PCT) system. Relevant scholarly literature concerning inventorship, artificial intelligence, patentability, and intellectual property theory is also reviewed.

The research combines doctrinal legal analysis with comparative legal methodology. The doctrinal approach is used to examine statutory provisions and judicial reasoning regarding inventorship requirements. The comparative approach allows for the identification of similarities and differences among national legal systems when addressing AI-generated inventions.

The objective of the analysis is not merely to describe individual judicial decisions but to identify broader legal patterns and emerging regulatory approaches concerning autonomous inventorship and AI-assisted innovation.

1. Inventorship as a Human-Centered Legal Concept

The concept of inventorship occupies a central position within patent law. Traditionally, patent systems have been built upon the assumption that inventions originate from human intellectual activity and that only a human being can be recognized as the source of inventive contribution. Consequently, inventorship has never been understood merely as a technical or procedural designation. Rather, it functions as a legal institution connecting creativity, the identification of the inventor, the allocation of patent rights and legal responsibility.

Historically, the inventor has been perceived as an individual capable of conceiving an inventive idea through intellectual effort and purposeful activity. Patent legislation in most jurisdictions reflects this understanding either explicitly or implicitly by linking inventorship to natural persons *(The U.S. Copyright Office (USCO)report, 2025)*. Although patent laws rarely provide a detailed philosophical definition of invention, they consistently presuppose the existence of a human actor responsible for the inventive process.

This human-centered approach is rooted in several elements. At its core, the traditional doctrine of inventorship continues to rest on three interconnected assumptions: human intellect, intention, and intellectual effort. Together, these elements explain why inventorship has historically been associated not only with creativity, but also with rights, obligations, and legal responsibility. First, inventorship traditionally requires intellectual contribution. The inventor is expected to participate in the conception of the inventive idea rather than merely execute technical instructions. Second, inventorship presupposes intention. The inventive process is commonly associated with conscious decision-making directed toward solving a technical problem. Third, inventorship is linked to legal responsibility, including the ability to transfer rights, claim ownership, and participate in legal proceedings related to patent protection.

For decades, these assumptions remained largely uncontested because technological tools were regarded as instruments operating under human control. Even highly sophisticated technologies assisted inventors without challenging the legal status of the human inventor. The emergence of artificial intelligence has significantly altered this situation. Contemporary AI systems are capable of identifying patterns, generating solutions, optimizing designs, and producing outputs that may satisfy traditional patentability requirements (*Ryan Abbott, 2020*). As a result, determining the nature and extent of human intellectual contribution in the inventive process has become increasingly complex.

Nevertheless, the growing technical capabilities of artificial intelligence do not automatically resolve the legal question of inventorship. The issue is not solely whether an AI system can generate a novel and useful solution. Rather, the question concerns whether existing patent law is prepared to separate inventorship from the concepts of human intellect, intention, and legal accountability upon which the institution has historically been constructed.

This tension between technological capability and legal doctrine forms the background against which the DABUS litigation emerged. The case did not simply challenge administrative patent procedures; it challenged one of the fundamental assumptions underlying contemporary patent law: that inventorship is inseparable from human agency.

2. The DABUS Case as a Legal Challenge

The DABUS case represents the first large-scale attempt to challenge the traditional understanding of inventorship within contemporary patent law. Unlike previous discussions concerning the role of artificial intelligence in innovation, the case directly confronted patent offices and courts with a fundamental legal question: can an artificial intelligence system be recognized as an inventor under existing patent legislation?

DABUS (Device for the Autonomous Bootstrapping of Unified Sentience) is an artificial intelligence system developed by Dr. Stephen Thaler (*Ryan Abbott, 2020*). According to its developer, the system was capable of generating inventive concepts autonomously, without direct human conception of the inventive idea. Seeking to test the legal implications of such technological developments, Thaler filed patent applications identifying DABUS itself as the inventor *(Application IL268604 - DEVICES AND METHODS FOR ATTRACTING ENHANCED ATTENTION).*

The applications concerned two inventions allegedly generated by the AI system. The first involved a fractal-shaped food container designed to improve grip efficiency and heat retention. The second related to an emergency beacon employing pulsating light patterns intended to attract attention in emergency situations. Although neither invention was particularly revolutionary from a technological perspective, both became legally significant because of the manner in which inventorship was claimed.



Figure 1. Timeline of the DABUS Litigation and Major Legal Developments

Source: *Developed by the author based on DABUS-related judicial decisions, patent office determinations, and WIPO proceedings.*

As illustrated in Figure 1, the DABUS applications gradually evolved from an individual patent dispute into a broader debate concerning the legal meaning of inventorship. Although different jurisdictions adopted different legal arguments, the overall trajectory of the litigation reveals a common reluctance to detach inventorship from human agency.

The first applications were submitted in 2018 before the United Kingdom Intellectual Property Office (UKIPO). Subsequently, corresponding applications were filed internationally through the Patent Cooperation Treaty (PCT) system administered by the World Intellectual Property Organization (WIPO), leading to examination procedures in multiple jurisdictions *(WIPO, KIPO, & KIPA, 2021)*.

The controversy surrounding DABUS was not technological but legal. Patent offices were not primarily asked to evaluate whether the inventions were novel, inventive, or industrially applicable. Instead, they were required to determine whether an entity lacking legal personality, consciousness in the legal sense, and the capacity to hold rights and obligations could satisfy the statutory requirements associated with inventorship.

As a result, the DABUS applications triggered an unprecedented global legal debate. Courts and patent authorities across different jurisdictions were compelled to examine concepts that had long been taken for granted within patent law. Questions concerning the relationship between creativity and legal personhood, the role of human contribution in the inventive process, and the allocation of rights arising from AI-generated outputs moved from theoretical discussions into practical adjudication.

The significance of the DABUS litigation therefore extends far beyond the fate of a particular patent application. The case became a legal stress test for the traditional doctrine of inventorship, exposing the tensions between rapidly evolving technological capabilities and legal frameworks developed in an era when invention was assumed to be an exclusively human activity.

3. Comparative Jurisdictional Responses to AI Inventorship

The DABUS applications generated one of the most extensive comparative legal debates in the history of patent law. As the applications progressed through national and regional patent systems, authorities were required to determine whether existing legal frameworks could accommodate an artificial intelligence system as an inventor.

Although the factual circumstances of the applications remained essentially identical across jurisdictions, the legal responses varied significantly *(Sanjana, 2021)*. Nevertheless, a common tendency can be observed: most patent offices and courts ultimately rejected the possibility of recognizing artificial intelligence as an inventor under current legislation.



Figure 2. Jurisdictional Approaches to AI Inventorship in the DABUS Litigation

Source: *Compiled by the author based on national patent office decisions, judicial rulings, and DABUS-related proceedings.*

The United States adopted one of the clearest positions on the issue. The United States Patent and Trademark Office (USPTO) and subsequently the Federal Circuit concluded that the term "inventor" under U.S. patent law refers exclusively to a natural person (*SUPREME COURT OF THE UNITED STATES. Petition DENIED, 2023*). The courts emphasized that inventorship is inseparable

from legal personhood and that existing statutory provisions provide no basis for extending inventor status to artificial intelligence systems.

A similar approach was adopted in the United Kingdom. The UK Intellectual Property Office rejected the DABUS applications on the grounds that an inventor must be a natural person capable of possessing and transferring legal rights. This interpretation was ultimately confirmed by the UK Supreme Court, which held that current patent legislation does not permit the designation of an artificial intelligence system as an inventor *(United Kingdom.Supreme Court (UKSC) Decision, 2023).*

The European Patent Office reached a comparable conclusion. According to the EPO, the inventor designated in a patent application must possess legal capacity, which presupposes natural or legal personhood. Since artificial intelligence systems do not possess independent legal status, DABUS could not be recognized as an inventor under the European Patent Convention *(European Patent Office Decision, 2020)*.

Not all jurisdictions approached the issue in exactly the same manner. In Australia, an initial decision of the Federal Court suggested that patent law might be interpreted flexibly enough to accommodate AI inventorship. However, this position was subsequently overturned on appeal and restoring the traditional requirement that inventorship be attributed to a human being (*The High Court of Australia, 2022*).

Germany adopted a more nuanced position. While rejecting the possibility of recognizing artificial intelligence as an inventor in its own right, German courts indicated that patent protection may still be available for inventions generated with the assistance of AI, provided that a human inventor is designated *(Federal Court of Justice, Germany, 2024).* This approach seeks to preserve the existing legal framework while acknowledging the growing role of artificial intelligence in the inventive process.

South Africa became the first jurisdiction to grant a patent listing DABUS as inventor. However, the significance of this decision should not be overstated. The grant resulted primarily from the formal nature of the South African patent examination system and did not constitute a substantive judicial recognition of AI inventorship *(Desmond Osaretin Oriakhogba, 2021).*

Several other jurisdictions, including China, Canada, the Republic of Korea, Brazil, India, and Singapore, have continued to evaluate the implications of AI-generated inventions through administrative procedures, judicial proceedings, or policy discussions (*Kingsley Egbuonu, 2025*). Although the legal debate remains ongoing, no major jurisdiction has yet established a comprehensive framework recognizing autonomous artificial intelligence as an inventor.

The comparative experience demonstrates that contemporary patent systems remain strongly attached to the traditional concept of human inventorship. While differences exist regarding procedural treatment and attribution mechanisms, the overwhelming majority of jurisdictions continue to regard artificial intelligence as a tool employed within the inventive process rather than as an independent inventor.

4. Emerging Regulatory Models of AI Inventorship

Despite the diversity of national responses presented above, the comparative analysis reveals the emergence of three principal regulatory models concerning AI inventorship. At first glance, the responses to DABUS appear fragmented. A closer examination, however, reveals three broader regulatory approaches that explain how contemporary patent systems respond to claims of AI inventorship.



Figure 3. Emerging Regulatory Models of AI Inventorship

Source: *Developed by the author based on comparative analysis of DABUS-related proceedings.*

The first and currently dominant model may be described as strict human inventorship. Under this approach, inventorship remains exclusively reserved for natural persons. Artificial intelligence systems may contribute to the inventive process, but they cannot acquire the legal status of inventor. This position has been adopted by the United States, the United Kingdom, the European Patent Office, Japan, Israel, Taiwan, and several other jurisdictions.

The second model may be characterized as the human-attribution approach. This model acknowledges the increasing role of artificial intelligence in generating inventive outputs while preserving the requirement that inventorship ultimately be attributed to a human actor. Under this approach, patentability is not necessarily denied merely because AI participated in the inventive process. However, legal recognition remains attached to a human inventor who assumes responsibility for the invention. Germany represents the most developed example of this approach.

The third model may be described as procedural acceptance. South Africa's decision to grant a patent listing DABUS as inventor illustrates how procedural structures may produce outcomes that differ from those observed in jurisdictions conducting substantive patent examinatiits not the same bu legalon. Although this patent did not establish a new legal doctrine of AI inventorship, it showed how patent examination procedures can influence legal results.

The existence of these models indicates that contemporary patent law is not experiencing a complete transformation of inventorship doctrine. Rather, legal systems are attempting to accommodate technological innovation while preserving the fundamental principles upon which patent protection has traditionally been based.

Most importantly, all three approaches continue to treat human agency as the central element of inventorship – ***we can change, but from the legal point is not correct*** - Most, these approaches show that the role of human inventors remains central to patent law. Even where artificial intelligence is recognized as playing a significant role in the inventive process, legal rights, obligations, and accountability remain attached to human actors. Consequently, the DABUS litigation has reinforced rather than displaced the human-centered foundations of patent law.

CONCLUSIONS

The DABUS case became the first global attempt to test the boundaries of traditional inventorship doctrine in the context of artificial intelligence.

The comparative analysis demonstrates that most jurisdictions continue to regard inventorship as a fundamentally human concept. Despite differences in legal reasoning, patent offices and courts consistently associate inventorship with human intellect, intention, and legal responsibility.

The study identifies three principal approaches to AI-generated inventions: strict human inventorship, human-attribution models, and procedural acceptance approaches. However, none of these approaches recognizes artificial intelligence as an autonomous inventor.

The significance of DABUS extends beyond the question of whether an AI system can be listed as an inventor. The case revealed a deeper challenge: contemporary patent law remains largely built upon assumptions developed long before the emergence of autonomous AI systems.

At present, patent law continues to treat artificial intelligence as a tool used within the inventive process rather than as an inventor. At the same time, the growing role of AI in innovation suggests that questions concerning inventorship, responsibility, and rights allocation will remain at the center of future legal debates.

In this sense, DABUS case should be understood not simply as a patent dispute, but as an important test of whether the traditional doctrine of inventorship can withstand the challenges posed by AI-generated innovation.

REFERENCES

Application IL268604 - DEVICES AND METHODS FOR ATTRACTING ENHANCED ATTENTION. Available at https://patentscope.wipo.int/search/en/detail.jsf?docId=IL276127794&_fid=IL353216090 [Accessed 25.05.2026].

Desmond Osaretin Oriakhogba, 2021. *DABUS gains territory in South Africa and Australia: Revisiting the AI-inventorship question*. South African Intellectual Property Law Journal 9 Available at https://www.researchgate.net/publication/357484468_DABUS_gains_territory_in_South_Africa_and_Australia_Revisiting_the_AI-inventorship_question [Accessed 27.05.2026].

European Patent Office Decision, 2020 Available at https://register.epo.org/application?documentId=E4B63SD62191498&number=EP18275163&lng=en&npl=false [Accessed 27.05.2026].

Federal Court of Justice, 11.06.2024, X ZB 5/22 - DABUS, Germany. *Decision*. Available at: https://www.wipo.int/wipolex/en/judgments/details/2495 [Accessed 26.05.2026]

Kingsley Egbuonu, 2025. *The latest news on the DABUS patent case* Available at: https://www.ipstars.com/NewsAndAnalysis/the-latest-news-on-the-dabus-patent-case/Index/7366 [Accessed 27.05.2026].

Ryan Abbott, 2020. *Intervention for the Second Session of the WIPO Conversation on AI & IP.* 07 July Available at: https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/conversation_ip_ai/pdf/ind_abbot.pdf [Accessed 24.05.2026].

Ryan Abbott. *The Artificial Inventor Project.* Available at: https://artificialinventor.com [Accessed 24.05.2026].

Sanjana , 2021. *A Brief Overview of the DABUS Patent Case.* Available at: https://www.globalpatentfiling.com/blog/brief-overview-dabus-patent-case [Accessed 26.05.2026].

SUPREME COURT OF THE UNITED STATES. Petition DENIED, 2023. *Case (2021-2347) Stephen Thaler, Petitioner v. Katherine K. Vidal, Under Secretary of Commerce for Intellectual Property and Director, United States Patent and Trademark Office, et* al. Available at https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/22-919.html [Accessed 27.05.2026].

The High Court of Australia, 2022. *Decision on the case Thaler v Commissioner of Patents [2022] HCATrans 199 (11 November 2022)* Available at https://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/HCATrans/2022/199.html [Accessed 27.05.2026].

The U.S. Copyright Office (USCO) report,2025. *Copyright and Artificial Intelligence, Part 2: Copyrightability*. Report. Available at: https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf [Accessed 24.05.2026].

United Kingdom Supreme Court (UKSC) Decision, 2023. *Thaler v Comptroller-General of Patents, Designs and Trade Marks UKSC 49*, Available at https://www.wipo.int/wipolex/en/text/593817 and https://www.ipo.gov.uk/p-challenge-decision-results/o74119.pdf [Accessed 27.05.2026].

Wenting Cheng, 2024. *Can Artificial Intelligence be a Patentee?: comments on DABUS cases*, November, Available at: https://www.researchgate.net/publication/380666332_Can_Artificial_Intelligence_be_a_Patentee_comments_on_DABUS_cases [Accessed 27.05.2026].

WIPO, KIPO, & KIPA, 2021. *IP Panorama 2.0 Study Book*. Referencing Module 1: General Introduction and AI-related IP trends [Accessed 26.05.2026].

Zahra Shakeri, Zohreh Gheisari Atrabi, 2024. *A Look at DABUS Case: An Outlook toward the Future Patent System* – December. Available at https://www.researchgate.net/publication/387424770_A_Look_at_DABUS_Case_An_Outlook_toward_the_Future_Patent_System [Accessed 25.05.2026].

ARTIFICIAL INTELLIGENCE, DATA SCIENCE AND COMPUTATIONAL INTELLIGENCE

BLOCKCHAIN TECHNOLOGY IN CONSTRUCTION DOCUMENTATION MANAGEMENT AND PREVENTION OF DOCUMENT FORGERY

CZU: 004.056:[005.334:69]
DOI: https://doi.org/10.53486/tids2026.03

MARIANA VATAMANITA
Drd. in law, "Constantin Stere" University of European Political and Economic Science, Faculty of Law, Department of Law, Republic of Moldova
e-mail: marina.mihai.90@mail.ru
ORCID ID: 0009-0004-2949-4750

ALEXANDRU MARIT
Associate Professor, PhD in law, "Constantin Stere" University of European Political and Economic Science, Faculty of Economy, Department of Law, Republic of Moldova
ORCID ID: 000-002-3198-8398

Abstract. The construction industry involves complex procedures, extensive documentation, and cooperation between multiple stakeholders. These characteristics can lead to administrative inefficiencies, disagreements, and an increased risk of document falsification. This study examines the potential of blockchain technology to improve the security and reliability of document management in construction. Its main objective is to assess how this technology can ensure document authenticity, prevent fraudulent practices, and support transparency and traceability throughout the different stages of construction projects.

The research adopts a qualitative methodology based on a review of relevant academic publications and a comparative assessment of conventional document management methods and blockchain-based systems. It also considers existing pilot projects and findings from empirical studies to understand the practical implications of adopting blockchain in construction. Previous research suggests that traditional systems frequently face challenges related to human error, fragmented information, and unauthorized alterations. By contrast, blockchain enables the creation of verifiable records that preserve information about document transactions and modifications.

The findings suggest that blockchain can improve data reliability, transparency, and accountability through cryptographic hashing, distributed verification, and timestamping mechanisms. Smart contracts may further facilitate administrative procedures, including document validation, approval processes, and the implementation of contractual obligations. These functions can help reduce processing times and minimize disagreements between project participants. Research findings also point to better information consistency and more complete documentation when blockchain-based solutions are implemented effectively.

The study demonstrates that blockchain technology can provide an additional layer of protection against document manipulation and fraudulent activities. Its capacity to maintain traceable records allows stakeholders to verify document histories and identify unauthorized changes. However, its practical implementation remains constrained by technical scalability, financial investment requirements, and the absence of sufficiently clear regulatory standards in some jurisdictions.

Keywords: blockchain, construction management, document security, forgery prevention, smart contracts, distributed ledger.

JEL Classification: O33; L74; D23; K42.

INTRODUCTION

The construction industry involves a large amount of documentation, including contracts, technical drawings, building permits, technical specifications, inspection reports, and documents confirming compliance with legal requirements. These documents are used at different stages of a construction project, from its planning to its completion. Their proper management is important for controlling costs, preventing disagreements, respecting legal requirements, and ensuring that projects are carried out successfully. However, traditional document management systems (DMS) used in construction are generally based on centralized storage and control, meaning that access to information depends on a particular system or administrator. This situation can create certain risks, especially when documents are changed without authorization, information is lost, or the accuracy of records cannot be easily verified. In addition, limited transparency in document management may cause misunderstandings between project participants and make it more difficult to identify who made particular changes and when they occurred. These problems can result in delays, additional costs, administrative difficulties, and conflicts related to contractual obligations. As a result, traditional document management methods may not always provide an adequate level of security and transparency for the needs of modern construction projects. According to Gartoumi (2024), the limitations of conventional document management systems can affect project quality, increase administrative costs, and weaken trust between the parties involved.

For these reasons, the construction sector needs document management systems that offer greater security, reliability, and transparency. The limitations of existing methods have encouraged researchers to examine new technologies that could help reduce these risks and improve the way construction documents are managed.

In recent years, blockchain technology has received increasing attention as a possible solution to the problems associated with traditional document management. Blockchain is a decentralized digital system in which information is recorded and verified across a network of computers rather than being controlled by a single authority. Each new record is validated according to established rules and linked to previous records. Through cryptographic methods and consensus mechanisms, blockchain makes unauthorized changes more difficult to carry out and easier to identify. This can help protect construction documents against manipulation, accidental loss, and unauthorized modifications. It can also allow project participants to check information and follow the history of documents more easily.

Blockchain may be particularly useful in Architecture, Engineering, and Construction (AEC) projects, where many parties need to exchange documents and keep track of different versions. For example, contracts, technical plans, inspection reports, and approval documents may be revised several times during a project's development. Keeping an accurate record of these changes is important for avoiding misunderstandings and determining who made a particular decision. Das *et al.* (2021) discuss the potential of blockchain-based systems to improve document approval procedures by using verified timestamps and audit trails. These features make it possible to follow document updates and identify the actions taken by different participants. In this way, blockchain can contribute to better document control and greater accountability throughout a construction project. Although its implementation still requires further consideration, the technology offers an interesting alternative to conventional systems and may help improve both administrative efficiency and the reliability of construction records.

Studies on the use of blockchain technology in the construction industry have approached the subject from different perspectives and have used various research methods. For example, Idrissi Gartoumi (2024) reviewed the existing literature on blockchain in construction management, focusing on the main challenges faced by the industry and the ways this technology could help improve project performance. The author identified several potential advantages of blockchain, but also pointed out that further research is needed. One important issue is the lack of comprehensive approaches specifically designed to protect construction documents and ensure that the information they contain remains accurate and reliable.

A different approach was taken by Das *et al*. (2021), who developed and tested a prototype for applying blockchain to construction document management. Their proposed system uses smart contracts to manage document approval procedures and cryptographic methods to keep track of document versions. The researchers considered whether a decentralized system could improve the security of project records and make document management processes more reliable. By recording activities in a verifiable way and automating certain procedures, such a system could reduce human error and limit unauthorized changes. It could also help project participants better understand when documents have been modified or approved. However, the practical value of these solutions needs to be examined further, particularly in real construction projects where many organizations and professionals are involved. Taken together, these studies show that blockchain could help address some of the weaknesses of traditional document management, although further testing is necessary to determine how effectively it can be applied on a larger scale.

Other researchers have also explored the role of blockchain in project management and construction activities. Their work highlights the possibility of improving cooperation between stakeholders by allowing them to access the same verified information. This may reduce disagreements caused by inconsistent records and make document handling more transparent. In addition, smart contracts can automate certain administrative tasks, including document verification and approval procedures, reducing the need for repeated manual checks and direct intervention by a central authority (Jadidoleslami & Azizi, 2022).

However, although blockchain offers several advantages, previous studies show that there is still limited practical evidence of its effectiveness in real construction projects. Most research has focused on theoretical analysis or the development of prototype systems, with less attention given to the results obtained when this technology is used in everyday construction activities. For this reason, it is still difficult to determine how much blockchain can improve existing practices and whether it can solve the problems encountered during the management of actual projects. Another limitation is the small number of case studies and pilot projects available. Since construction projects differ in size, complexity, and the number of people involved, the results obtained in one situation may not be applicable to all types of projects.

Although blockchain has attracted the attention of researchers since around 2017, its use in the construction industry remains relatively limited. Further research is therefore necessary to understand its practical benefits. Studies carried out on real construction sites, together with research conducted over longer periods, could provide a clearer picture of how blockchain influences document management, transparency, and cooperation between project participants. Such research could also help establish whether this technology reduces administrative work and improves trust among the parties involved.

Considering these limitations, the present study examines how blockchain technology can be used to improve the management of construction documents and reduce the risk of document falsification. Particular attention is given to the use of distributed records, smart contracts, and cryptographic methods in existing document management processes. These tools may help protect information, make document changes easier to track, and ensure greater transparency throughout the project lifecycle.

The research has three main objectives. The first is to examine how blockchain can help preserve the authenticity and integrity of construction documents through secure recordkeeping, document version tracking, and the recording of activities. The second objective is to compare blockchain-based solutions with traditional centralized document management systems (DMS), considering their security, efficiency, and reliability. The third objective is to identify the main difficulties that could affect the implementation of blockchain in construction, including technical limitations, the costs of introducing new systems, compatibility with existing technologies, and legal requirements.

By addressing these objectives, the study aims to clarify the potential benefits and limitations of blockchain in construction document management. It also seeks to explain how this technology could help prevent unauthorized changes, reduce the risk of fraud, and improve cooperation between project participants. In this way, the research connects the possibilities described in academic literature with their potential practical application in the construction industry.

MAIN CONTENT

1. Materials and Methods

This study explores how blockchain technology could improve the management of construction documents and help prevent their falsification in the Architecture, Engineering, and Construction (AEC) sector. The research is based on scientific publications, literature reviews, conceptual models, and prototype systems developed by previous researchers. Particular attention is given to the studies conducted by Das *et al*. (2021), Idrissi Gartoumi (2024), and Jadidoleslami and Azizi (2022).

The main research method is a systematic review of the existing literature. Relevant studies are examined to identify the main findings, the ways blockchain can be used in document management, and the benefits and limitations reported by researchers. The study also compares blockchain-based solutions with traditional document management systems, focusing on aspects such as document security, transparency, and the possibility of tracking changes. In addition, a qualitative analysis is used to identify common findings and challenges related to the practical implementation of this technology. To make the analysis more reliable, findings from different sources and research approaches are considered together. This helps connect the theoretical aspects of blockchain with its possible use in real construction projects.

2. Results and Discussions

The results of this study suggest that blockchain technology could improve the way construction documents are managed, especially in terms of data security, transparency, and reliability. The analysis of existing research shows that traditional document management systems are often based on centralized structures, which can create difficulties when information needs to be shared, updated, or verified. These systems may be affected by unauthorized changes, errors, and the fragmentation of information between different parties. As a consequence, misunderstandings, contractual disagreements, project delays, and additional costs may occur.

Blockchain offers another way of managing construction documents by storing information in a distributed digital ledger. Through cryptographic methods and the validation of records by network participants, this technology makes it more difficult to change information without authorization. Once a record has been added to the blockchain, any subsequent modification can be identified, while the history of previous transactions remains available for verification. This feature can help reduce the risk of document falsification and improve confidence in the information used throughout a construction project.

Another advantage of blockchain is its potential to simplify document management procedures. It can support the tracking of document versions, facilitate the secure exchange of information, and automate certain approval procedures through smart contracts. When compared with traditional Construction Document Management Systems (CDMS), blockchain-based solutions offer important benefits in terms of traceability and the possibility of checking document histories. They can also improve cooperation between project participants by making relevant records more accessible and easier to verify.

Overall, blockchain could contribute to more reliable document management in the construction sector. By providing records that are difficult to alter without detection, the technology allows participants to check the origin and history of documents at different stages of a project. This may help prevent disagreements, support better decision-making, and clarify the responsibilities of the parties involved. Similar benefits are discussed by Mahmudnia *et al.* (2022), who examine the potential of blockchain applications in construction management.

The use of smart contracts can also help improve the way construction projects are managed, especially when it comes to administrative tasks and document approval. Smart contracts are digital agreements based on blockchain technology that automatically perform certain actions when specific conditions are met. In construction, they could be used for checking documents, confirming approvals, verifying compliance with established requirements, and processing payments. By automating some of these activities, the need for manual work can be reduced, which may help prevent errors and avoid unnecessary delays.

Another advantage of smart contracts is that they follow rules established in advance, making procedures clearer for the parties involved. When the conditions and steps are known beforehand, it becomes easier for participants to understand their responsibilities and follow the progress of different activities. This can also reduce misunderstandings that occur when information is incomplete or decisions are not communicated properly. In addition, automated procedures may improve coordination between contractors, engineers, project managers, and other participants.

The use of smart contracts does not eliminate every possible conflict, since disagreements may still arise over contractual terms or the quality of construction work. However, when they are properly designed and implemented, these tools can make certain procedures more transparent and easier to verify. In this respect, blockchain-based systems that include smart contracts may contribute to more efficient project management, clearer responsibilities, and better cooperation between stakeholders. Similar benefits are discussed by Awsan *et al.* (2021) in relation to the use of blockchain technology in construction.

Another important finding of this study is that blockchain technology can help improve trust and cooperation between people involved in construction projects. Since the system allows authorized participants to access the same digital records, everyone can work with consistent and updated information. This is important because, in traditional document management systems, information is

sometimes stored in different places or shared only with certain participants. Such situations can lead to misunderstandings and difficulties in verifying the accuracy of documents.

Blockchain can reduce these problems by allowing participants to check the information recorded in the system without depending entirely on a central administrator. They can follow document changes and verify the status of records, which may help increase confidence in the information used during the project. As a result, communication between contractors, engineers, clients, and public authorities could become more effective. Better access to reliable information may also support faster decisions and help prevent conflicts caused by incomplete or inconsistent documentation. The importance of blockchain for cooperation and information sharing in construction projects has also been discussed by Shishehgarkhaneh *et al.* (2023).

These findings are relevant to the Republic of Moldova, where improving administrative procedures and the digital management of construction documents remains an important objective. The use of blockchain could complement the digitalization of public services and contribute to greater transparency in the construction sector. For example, connecting blockchain-based systems with existing electronic platforms for construction permits or public procurement could make it easier to verify documents and follow the history of administrative decisions. Such solutions may also help clarify the responsibilities of institutions and reduce disagreements concerning the authenticity of records. However, their effectiveness would depend on how well they are integrated into existing systems and legal procedures.

Despite these potential benefits, the implementation of blockchain in construction also presents several difficulties. One of the main obstacles is the cost of introducing and maintaining the technology. In addition, integrating blockchain with existing software may require technical expertise and considerable changes to current working procedures. Scalability is another concern, particularly for large construction projects that generate significant amounts of documentation and data. Legal questions also remain important, including the recognition of electronic records, the protection of personal and confidential information, and the rules governing access to stored data.

A further limitation is the lack of sufficient practical evidence concerning the results of blockchain implementation in real construction projects. Much of the existing research focuses on theoretical models, experimental systems, or small pilot projects. Consequently, it is difficult to establish whether the expected benefits can be achieved in large and complex projects or whether the investment is justified by the results. As noted by Gartoumi (2024), further research is needed to better understand the practical application of blockchain in construction. Studies based on real projects and longer observation periods would help clarify its advantages, limitations, and actual costs, providing a stronger basis for decisions about its wider use in the construction industry.

The scientific value of this research lies in examining how blockchain technology can be used to improve the management of construction documents and reduce the risk of falsification. While previous studies have mainly discussed blockchain in relation to project management and contract administration, this research focuses more specifically on the authenticity, security, and traceability of construction documentation. This approach makes it possible to examine the technology in connection with a practical problem faced by the construction industry, namely, how to ensure that documents remain reliable and that unauthorized changes can be identified.

Another important aspect of the study is the analysis of how different blockchain features can work together in document management. Cryptographic methods help protect recorded information and make unauthorized modifications easier to detect. The decentralized structure allows participants

to verify records without depending entirely on a single administrator. At the same time, smart contracts can automate certain procedures, such as document approval and verification, when predefined conditions are met. Used together, these features could improve document security and reduce the opportunities for fraud or unauthorized alterations.

The study also highlights the practical importance of understanding how these mechanisms can be applied in construction projects. Although blockchain cannot guarantee the accuracy of information entered into the system in the first place, it can help preserve records and make subsequent changes more traceable. This may be particularly useful when several organizations and professionals are involved in preparing, checking, and approving construction documents.

In conclusion, blockchain technology offers a possible way to improve the security and management of construction documentation. Its main advantages include decentralized recordkeeping, the ability to trace document changes, and the automation of certain administrative procedures through smart contracts. These features could help increase transparency, strengthen accountability, and reduce the risk of document manipulation.

For the Republic of Moldova, this topic deserves particular attention because the digitalization of administrative processes and the reliability of construction documentation are important for the development of a more transparent construction sector. The introduction of blockchain-based solutions could complement existing electronic systems and make document verification more reliable. However, their practical use would require appropriate technical solutions, clear legal rules, and further research based on real construction projects. Therefore, blockchain should be considered a promising option whose effectiveness needs to be assessed in relation to the specific needs and conditions of the Moldovan construction sector.

Table 1. Blockchain adoption in construction documentation in the Republic of Moldova

Aspect	Traditional CDMS	Blockchain-Based Systems	Implications for Republic of Moldova
Data Integrity	Centralized, vulnerable to manipulation and errors	Immutable records with cryptographic protection	Reduces risks of document falsification and unauthorized edits in Moldovan construction projects
Transparency & Trust	Fragmented information, limited stakeholder visibility	Decentralized ledger ensures full visibility and traceability	Improves collaboration and stakeholder confidence across contractors, regulators, and clients
Version Control & Traceability	Difficult to track document history and edits	Every transaction is recorded chronologically and tamper-proof	Enables reliable audit trails for permits, contracts, and approvals, supporting legal certainty
Workflow Efficiency	Manual approvals, high administrative burden	Automated smart contracts streamline approvals, compliance checks, and payments	Reduces delays and administrative inefficiencies common in Moldovan construction workflows
Risk Mitigation	High risk of disputes, miscommunication, and financial losses	Immutable records, distributed validation, and smart contracts reduce fraud and errors	Supports national digitalization efforts and alignment with European construction governance standards

Table 1 (continued)

Aspect	Traditional CDMS	Blockchain-Based Systems	Implications for Republic of Moldova
Challenges & Limitations	Limited data security, inefficiencies	High deployment cost, technical complexity, integration with legacy systems, regulatory uncertainty	Requires policy support, technical training, and pilot projects to validate effectiveness

Source: *Adapted by information Das et al., 2021*

This table captures the practical benefits, risks, and context-specific implications of blockchain adoption for construction documentation management in the Republic of Moldova.

The following table presents a more detailed analysis of smart contracts and collaboration between stakeholders, taking into account the situation in the Republic of Moldova.

Table 2. Smart Contracts and Stakeholder Collaboration in the context of the Republic of Moldova

Aspect	Traditional CDMS	Blockchain with Smart Contracts	Implications for Republic of Moldova
Workflow Automation	Manual approvals, slow processing	Self-executing smart contracts automatically trigger approvals, compliance checks, and payments	Reduces administrative delays and human errors in document workflows within Moldovan construction projects
Procedural Clarity	Ambiguity in responsibilities, inconsistent procedures	Predefined rules embedded in smart contracts ensure consistent execution	Improves accountability and clarity in project roles among Moldovan contractors, engineers, and regulators
Error Reduction	High likelihood of mistakes due to manual handling	Automated processes minimize human intervention and errors	Decreases risk of discrepancies in permits, certifications, and contracts, which are common in local practice
Stakeholder Coordination	Fragmented communication, information asymmetry	All participants access a shared, transparent database in real-time	Enhances trust, reduces miscommunication, and fosters better collaboration across multi-actor projects in Republic of Moldova
Conflict & Dispute Minimization	Frequent disputes due to inconsistent records and delays	Transparent, immutable records with automatic execution reduce potential for conflicts	Supports smoother project delivery, fewer legal disputes, and more reliable verification of document authenticity
Operational Efficiency	Repetitive administrative tasks, slower project timelines	Streamlined approvals and automated workflows speed up processes	Optimizes project schedules and resource allocation, addressing inefficiencies in the Moldovan construction sector

Source: *Adapted by information Das et al., 2021*

This table emphasizes how blockchain and smart contracts together improve collaboration, transparency, and efficiency, specifically tailored to the challenges faced in the Republic of Moldova.

However, the use of blockchain in real construction projects is still at an early stage. There are several difficulties that need to be addressed, such as the high costs of implementation, the lack of

specialists with the necessary technical knowledge, and problems integrating blockchain with existing digital systems. Another important issue is the lack of clear legal rules regarding the recognition and use of records stored on blockchain platforms. For these reasons, more practical research is needed, including pilot projects and case studies, to understand whether this technology can be used effectively on a larger scale and whether its benefits justify the costs.

In conclusion, blockchain could improve the way construction documents are managed by making them more secure, transparent, and easier to verify. However, its wider use will depend on further technological development, appropriate legal regulations, and support from public institutions and the construction industry. Cooperation between researchers, construction professionals, and policymakers will be important in overcoming the existing challenges. If these conditions are met, blockchain could help protect the authenticity of construction documents, strengthen trust between project participants, and improve the overall management of construction projects.

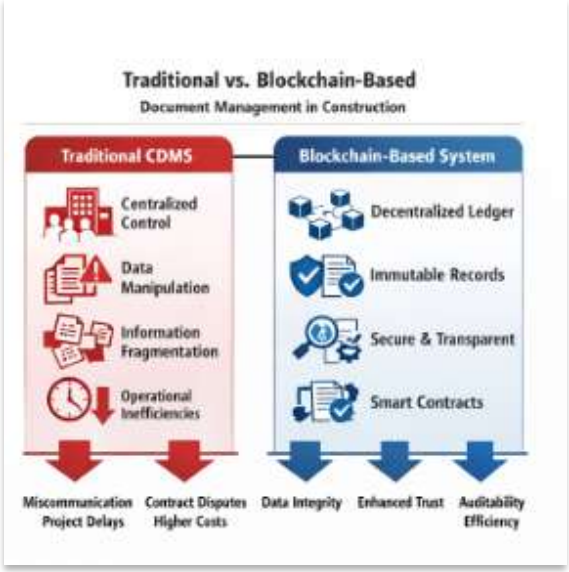


Figure 1. Traditional vs. Blockhain- Based. Document Management in Construction
Source: *Personal idea of diagram*

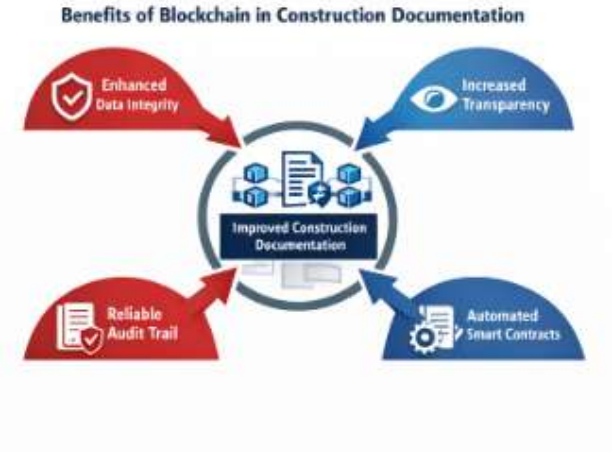


Figure 2. Benefits of Blockhain in Construction Documentation
Source: *Personal idea of diagram*

CONCLUSIONS

This study examines how blockchain technology could improve the management of construction documents and help prevent document forgery in the Architecture, Engineering, and Construction (AEC) sector, with a particular focus on the Republic of Moldova. The results show that blockchain has several potential benefits, but its practical use also involves certain difficulties that need to be considered.

The research shows that blockchain could make construction documents more secure by storing information in a way that makes unauthorized changes easier to identify. It also allows documents and their modifications to be tracked over time. Smart contracts can be used to automate certain activities, such as document approval and verification. Compared with traditional centralized Construction Document Management Systems (CDMS), blockchain may offer better traceability and make it easier to check the history of a document. The main contribution of this study is its focus on document authenticity and protection against forgery, rather than on general aspects of project management or contract administration.

Another important finding is that blockchain could improve communication and cooperation between the people involved in construction projects. Its decentralized structure and cryptographic mechanisms can help protect information and make document verification more transparent. Smart contracts may also simplify approval procedures, compliance checks, and some financial operations. These functions could reduce human errors, delays, and misunderstandings between project participants. In the Republic of Moldova, such solutions could be useful in situations where construction information is spread across different institutions and organizations. Access to reliable and updated documents could help contractors, engineers, public authorities, and clients coordinate their activities more effectively.

The introduction of blockchain into the Moldovan construction sector could also support the country's efforts to digitalize public services and bring administrative practices closer to European standards. A blockchain-based document management system could make construction permits, approval procedures, and public procurement processes more transparent. It could also help clarify the responsibilities of the parties involved and reduce disputes caused by missing, altered, or inconsistent documents. However, these benefits depend on how the technology is implemented and integrated into existing procedures.

Despite its potential, blockchain still faces several challenges. The initial costs may be high, and the technology requires specialized knowledge that is not always available. Integrating blockchain with existing information systems may also be difficult. In addition, the lack of clear and standardized legal rules concerning blockchain records can create uncertainty about their recognition and use in official procedures. Another limitation is the small number of practical studies showing how well these solutions work in real construction projects. Therefore, their effectiveness should not be assumed without further testing.

Further research should include pilot projects, case studies, and long-term evaluations to determine whether blockchain is suitable for the needs of the construction sector. It would also be useful to examine how blockchain could work together with other digital technologies and to identify the main concerns of construction companies, public authorities, and other stakeholders. Such research could help establish whether the benefits justify the costs and what legal or organizational changes would be necessary for wider implementation in the Republic of Moldova.

The study also points to a difference between the theoretical advantages of blockchain and the difficulties of applying it in practice. Although the technology may improve document security and transparency, these results cannot be achieved through technology alone. Proper training, clear regulations, institutional cooperation, and careful integration into existing workflows are also necessary. Without these conditions, the expected benefits may remain limited.

In conclusion, blockchain technology could provide a useful way to improve construction document management, make document changes easier to trace, and reduce the risk of forgery. For the Republic of Moldova, its implementation could support digitalization, increase transparency, and strengthen trust between participants in construction projects. Nevertheless, further research, practical testing, appropriate legal rules, and institutional support are needed before its advantages can be fully assessed. Cooperation between researchers, construction professionals, and public authorities will be essential to determine how this technology can be used effectively and bring lasting improvements to the construction sector.

REFERENCES

Awsan, M., Ahmad, A., Ahmed, G., Laith, A., H., 2021. The Role of Blockchain in Improving the Processes and Workflows in Construction Projects. *Applied Sciences*, 11, 8835.

Das, M., Tao, X., Liu, X., Cheng, J., C., P., 2021. A blockchain-based integrated document management framework for construction applications. *Automation in Construction,* 133, 104001.

Gartoumi, K., I., 2024. Five-Year Review of Blockchain in Construction Management: Scientometric and Thematic Analysis (2017-2023). *Automation in Construction*, 168, part A, pp.105773.

Jadidoleslami, S., Azizi, M., 2022. Blockchain for Project and Construction Management; A Systematic and Scoping Literature Review. *Journal of Information Technology Management*, pp. 107-143.

Mahmudnia, D., Arashpour, M., Yang, R., 2022. Blockchain in construction management: Applications, advantages and limitations. *Automation in Construction,* pp. 104379.

Shishehgarkhaneh, M., B., Moehler, R., C., Moradinia, S., F., 2023. Blockchain in the Construction Industry between 2016 and 2022: A Review, Bibliometric, and Network Analysis. Smart Cities, 6, 819–845.

INTEGRATING ARTIFICIAL INTELLIGENCE TOOLS IN THE VOCATIONAL TRAINING OF IT TECHNICAL SUPPORT OPERATORS: OPPORTUNITIES AND CHALLENGES

CZU: 004.89:377(478)
DOI: https://doi.org/10.53486/tids2026.04

ION COSTIN
IT Engineer, Vocational School, Soroca, Republic of Moldova
e-mail: ioncostyn1@gmail.com
ORCID ID: 0009-0008-4540-3256

VICTORIA LOZAN
PhD, Associate Professor, Academy of Economics Studies of Moldova
e-mail: lozan.victoria@ase.md
ORCID ID: 0000-0002-5869-8515

Abstract. This paper presents a case study conducted over two academic years (2024–2025 and 2025–2026) at the Vocational School in Soroca, Republic of Moldova, aiming to analyse the impact of AI-based tools, specifically ChatGPT and Microsoft Copilot, on the performance of students enrolled in the "IT Technical Support Operator" programme.

In the first year, a group of 20 second-year students completed various SOHO network configuration scenarios and Cisco Packet Tracer simulations (Cisco, 2026), comparing results achieved under traditional working conditions with those obtained using AI support. In the second year, 28 first-year students were divided into two equal groups, each assigned identical practical hardware assembly tasks. The first group worked using traditional methods, while the second used AI tools for documentation and guidance.

The data show that AI use contributed to an average grade increase of approximately one point, a reduction in task completion time of around 35–45%, and the production of more detailed and better-structured final reports. The study also identifies challenges, particularly the tendency of approximately 30% of students to adopt AI-generated answers without critical analysis or practical verification.

Based on these results, the paper identifies the pedagogical conditions that favour effective AI use in vocational training and proposes a didactic model adapted to VET institutions in the Republic of Moldova, focused on developing practical competencies, critical thinking, and student autonomy.

Keywords: artificial intelligence, ChatGPT, Copilot, vocational and technical education, IT technical support, Cisco Packet Tracer, networking, hardware assembly, critical thinking, vocational training.

JEL Classification: I21, I23, O33

INTRODUCTION

Generative artificial intelligence has, in a relatively short time, become part of everyday activities in the IT sector, including technical support processes, fault diagnosis and equipment configuration. Today, numerous platforms and services use virtual assistants or automated AI-based systems for the rapid identification of problems and the provision of technical solutions. Under these circumstances, vocational and technical education institutions are required to adapt their training processes to the current realities of the labour market. Students pursuing the IT Technical Support Operator qualification will inevitably interact with such tools immediately upon employment, and ignoring this aspect during training would create a significant gap between the competencies formed at school and the actual requirements of the field.

This paper does not aim to develop a general theory regarding the use of artificial intelligence in education. The focus is on the practical experience gained in the course of teaching activities at a vocational and technical education institution in Soroca, over two consecutive academic years, working directly with students, practical tasks, and situations close to real professional contexts. The study is applied in nature and seeks to provide useful data and observations for VET teachers, as well as for those involved in the development and modernisation of vocational training programmes. The primary aim is not to validate a pre-established theoretical hypothesis, but to analyse concrete results obtained in the instructional process.

The research is oriented towards identifying the real impact that AI tools can have on the practical activities carried out by students in the field of IT technical support. In this context, the study aims to answer several key questions: whether the use of AI tools influences student performance as measured by grades in practical networking and hardware tasks; whether these tools contribute to reducing the time required for task completion; and what pedagogical factors determine the difference between effective use of AI as a support instrument and superficial use based on mechanical copying of generated responses.

1. THEORETICAL FRAMEWORK AND PEDAGOGICAL CONTEXT

In the context analysed in this paper, AI-based tools such as ChatGPT (OpenAI, 2026) and Microsoft Copilot (Microsoft, 2026) were used at practically all levels of the SAMR model, depending on the manner in which each student chose to interact with them. In some instances, AI was used merely as a substitute for conventional internet searching, with students requesting quick explanations or technical definitions. In other cases, AI tools contributed to augmenting activities by generating more structured explanations adapted to the student's level of understanding and the context of the practical task.

The integration of digital technologies into vocational education has been analysed in multiple studies through the SAMR model developed by Ruben Puentedura, which distinguishes between the use of technology as a simple substitute for traditional methods and its use as an element that transforms and redefines the learning activity (Puentedura, 2006). In current educational practice, this model provides a useful framework for understanding not just what students do with technology, but especially how their learning changes. Holmes et al. (2019) emphasize that artificial intelligence in education offers significant opportunities for personalizing learning.

The effective application of digital technologies in the educational process depends on the integration of technological, pedagogical, and content knowledge, an aspect highlighted in the TPACK model proposed by Mishra and Koehler (2006).

At the higher levels of the model, it was observed that some students used AI to develop network configurations, generate CLI commands, or verify troubleshooting steps in simulated environments such as Cisco Packet Tracer (Cisco, 2026). In these situations, the practical task was significantly modified through the introduction of a working process more closely aligned with the reality of IT technical support. In certain activities, AI use even allowed the learning experience to be redefined. Students came to simulate interactions similar to those in a real technical support centre. Problem analysis, request formulation, and response interpretation became an almost continuous flow.

During one observed moment in the course of activities, a student spontaneously remarked that "it feels like I'm working with a more experienced colleague, not just with a programme". This

perception reflects the way in which AI was integrated into the learning activity, transcending its simple function as a tool.

Recent literature on the use of artificial intelligence in education highlights that the primary risk lies not in the use of AI itself, but in its superficial and uncritical use. Kasneci *et al.* (2023) and Baidoo-Anu and Ansah (2023) describe this phenomenon through the concept of "AI-assisted surface learning", a situation in which the student transfers the cognitive process to the AI tool without analysing, verifying, or adapting the generated response. The observations made in the context of this study confirm this tendency in the VET context as well.

Students who formulated clear prompts, compared generated responses with technical documentation, and practically verified proposed solutions achieved noticeably better results both in practical assessments and in the preparation of final reports. In contrast, students who used AI exclusively for rapid copying encountered difficulties in explaining their own solutions or in resolving situations slightly different from the examples provided by the model.

An important aspect observed during the research is the fact that AI use influenced not only the speed of task completion but also students' confidence in carrying out practical activities. Particularly among first-year students, AI tools reduced the frequency of blockages during independent work and encouraged the formulation of technical questions. However, this increase in autonomy was expressed positively only when the teacher continuously monitored the process and required students to justify the solutions proposed by AI.

In the specific context of the VET system in the Republic of Moldova, it is relevant that the occupational standards and curriculum for the IT Technical Support Operator qualification do not explicitly include competencies related to the use of AI-based tools (Ministry of Education and Research of the Republic of Moldova, 2016, 2020). Given that IT companies and modern technical support services already use such solutions in their daily operations, this absence risks creating a gap between the competencies formed at school and those required upon employment.

For this reason, this paper argues for the necessity of updating the curriculum to include the critical, responsible, and effective use of AI tools as part of vocational training. In this way, students will not merely learn to use technology, but to understand it and consciously integrate it into their professional activity.

2. STUDY DESIGN AND METHODOLOGY

2.1. Participants and Period

The research was conducted in two distinct stages over two consecutive academic years at the Vocational School in Soroca, in the IT Technical Support Operator programme. The study design aimed to compare how the use of AI-based tools influences student performance in practical IT-related activities.

The first study was conducted during the 2024–2025 academic year and included a group of 20 second-year students in their final year of vocational training. The students already possessed consolidated foundational knowledge in networking and computing equipment. Practical activities focused primarily on SOHO network configuration and simulations in Cisco Packet Tracer. In the first stage, students individually completed a practical scenario without using AI tools, relying only on standard teaching materials and previously acquired knowledge. Subsequently, the same students received a scenario of similar difficulty, with the option of using ChatGPT and Microsoft Copilot for documentation, configuration generation, and verification of working steps.

This design allowed direct comparison of the same group's performance under two different working conditions, reducing the influence of individual differences on the final results. In addition to grade assessment, the time required for task completion, the number of technical errors identified in configurations, and the students' ability to explain their solutions during the final presentation were all monitored.

The second study was conducted during the 2025–2026 academic year and involved 28 first-year students. For this stage, students were divided into two equal groups of 14, balanced according to initial proficiency levels established through assessments conducted at the beginning of the academic year. The first group carried out practical activities using traditional methods, employing performance guides, teacher explanations, and laboratory demonstrations. The second group received the same tasks and working conditions, but students were additionally permitted to use AI tools for guidance and verification of assembly steps.

The practical task common to both groups consisted of the complete assembly of a computer from separate components, together with documentation of the working steps in a final technical report. During the activities, several aspects were monitored: assembly accuracy, compliance with safety norms, time required for task completion, degree of student autonomy, and quality of the documentation produced.

The design used in this stage was of a between-subjects type, based on comparing the results of two parallel groups under different AI use conditions. This approach allowed observation of performance differences between students who used AI tools and those who worked exclusively through traditional instructional methods.

2.2. Teaching Scenarios Used

In Study 1, practical activities were oriented towards the configuration and simulation of SOHO networks, using both physical equipment available in the laboratory and the virtual environment provided by Cisco Packet Tracer. The scenarios presented to students included configuring a router and a switch to provide local network connectivity with internet access, segmenting the network through VLANs, and configuring the DHCP service for the automatic distribution of IP addresses. In the first stage, tasks were completed using classical methods, without AI tools, with students relying on course materials, teacher guidance, and prior laboratory experience.

Subsequently, the same types of scenarios were repeated under similar difficulty conditions, but students were permitted to use tools such as ChatGPT and Microsoft Copilot. To prevent the superficial use of automatically generated responses, students were required to document each interaction with AI. This documentation included the prompts formulated, the responses received, and explanations of how the generated information was applied in solving the practical task. In their final report, students had to explicitly justify the choice of configurations used and explain any modifications made relative to AI recommendations.

This approach allowed observation not only of the final result, but also of students' thinking processes during the working procedure. In several instances it was noted that students who formulated more precise technical questions and practically verified AI-recommended commands achieved functional configurations more quickly and with fewer errors. In contrast, students who directly adopted commands without verification encountered difficulties when problems slightly different from the model's examples arose.

In Study 2, the practical activity focused on the hardware assembly of a fully functional computer from individual components available in the laboratory. The practical task aimed at

developing competencies in hardware component identification, processor–motherboard compatibility verification, processor and cooling system installation, RAM installation, storage unit mounting, and securing the motherboard in the case. Students were also required to correctly connect the power supply and perform the first system boot to verify component functionality.

The main verification criteria were correct system operation without boot errors, normal fan activity, and accessibility of the BIOS/UEFI interface. For the group that used AI, students could consult AI tools to clarify the order of component installation, identify connectors and ports, or diagnose problems encountered during assembly. As in the first study, all AI interactions had to be documented in the final report.

During the activities, it was observed that AI use was particularly useful for students encountering difficulties in identifying components and interpreting error messages at boot. The teacher continuously monitored how students used AI-generated responses to prevent the tool from becoming a source of mechanical copying without understanding of the technical processes involved.

2.3. Data Collection and Processing

For the assessment of results in both studies, both quantitative and qualitative data were collected. The aim was to understand not only "what results students obtained", but also "how they arrived at these results", step by step, during practical activities. Data collection was carried out throughout the tasks and in the final assessment stage. The same criteria were used for all participants to ensure comparability of results.

Quantitative data included the grades obtained by students in the final assessment of each practical scenario, using a grading scale from 1 to 10, where the minimum pass threshold was set at grade 7. Beyond the numbers, these grades reflected the actual level of mastery of technical competencies. The assessment addressed both the technical accuracy of the task and the student's ability to explain what they had done and why they had chosen certain solutions.

In parallel, the time required to complete each practical task was monitored, by recording the start and end time for each student individually. This was measured directly by the teacher in real time during laboratory activities. Additionally, the number of direct interventions made by the teacher for each student or group was tracked. This indicator provided a clear picture of the level of autonomy. Student autonomy varied considerably: several learners worked with minimal support, whereas others asked for frequent intervention during challenging tasks.

Qualitative evidence came from structured observation during lab activities, documenting not just physical steps but also participants' think-aloud problem-solving processes. The manner of formulating technical questions, the ability to identify errors, and the level of understanding of the steps carried out were analysed. Special emphasis was placed on how students interacted with AI tools, whether as genuine support or merely as a source of answers.

Final reports produced by students were also analysed. These served as a "mirror" of the working process. Clarity of explanations, the logic of technical solution argumentation, and the way students documented their interactions with ChatGPT and Microsoft Copilot were examined. Some reports showed a deep understanding of the process, while others contained mechanically recounted steps, without reflection.

Following analysis of the results, basic statistical methods appropriate to the practical nature of the research were applied. Data processing included calculation of arithmetic means for grades and task completion times, frequency distribution analysis by performance levels obtained, and percentage comparisons between groups investigated under different working conditions. These

procedures were selected to allow a clear and direct interpretation of the impact of AI tools on practical activities in the field of IT technical support and networking.

3. RESULTS

3.1. Grade Distribution and Comparative Averages

Figure 1 shows the grade distribution in both studies. In Study 1 (networking), the transition from the non-AI scenario to the AI scenario produced a visible shift in the distribution towards higher grades: whereas without AI, 70% of students received grades of 5 or 6 (below the pass threshold of 7), with AI, 95% exceeded the threshold, with a substantial reduction in grade-5 scores (from 6 students to 0).

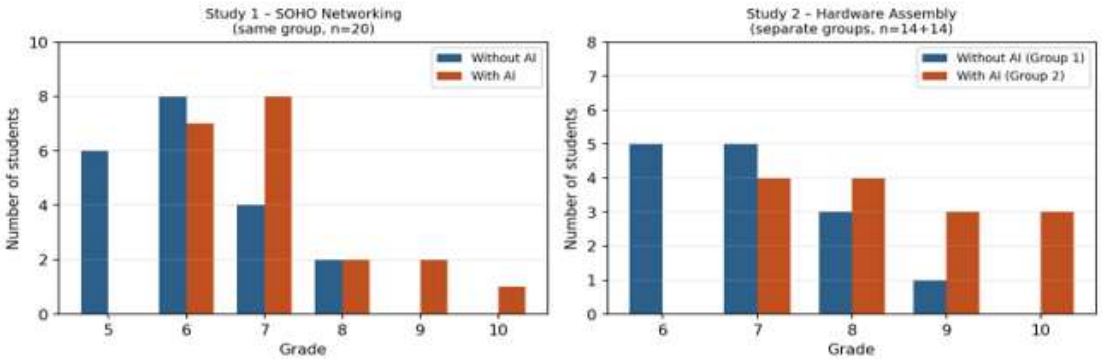


Figure 1. Grade distribution in Study 1 (networking, n=20, same group) and Study 2 (hardware, n=14+14, separate groups).

Source: *Authors' own work.*

Figure 2 summarises the averages calculated from the above distributions. The average grade increased from 6.10 to 7.10 in Study 1, and from 7.00 to 8.36 in Study 2. The pass threshold was exceeded as an average in all AI scenarios, and reached exactly at the limit in Group 1 of Study 2. The detailed distribution of grades and calculated averages is presented in Table 1.

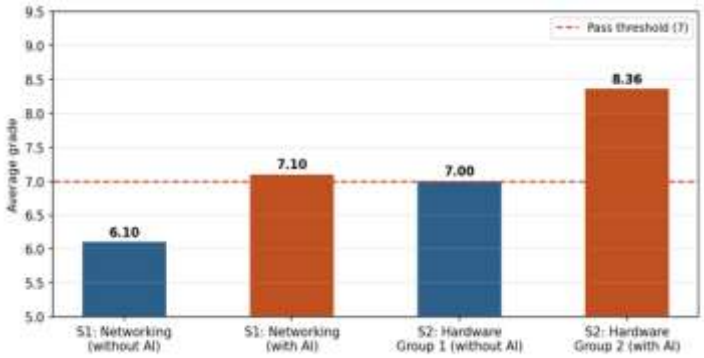


Figure 2. Comparative average grade across the four experimental conditions (pass threshold = grade 7).

Source: *Authors' own work.*

Table 1. Detailed grade distribution and calculated averages.

Condition / Scenario	Grade 5	Grade 6	Grade 7	Grade 8	Grade 9	Grade 10	Average
S1 – Networking WITHOUT AI (n=20)	6	8	4	2	0	0	6.10
S1 – Networking WITH AI (n=20)	0	7	8	2	2	1	7.10
S2 – Hardware G1 Without AI (n=14)	0	5	5	3	1	0	7.00
S2 – Hardware G2 With AI (n=14)	0	0	4	4	3	3	8.36

Source: *Authors' own work.*

3.2. Task Completion Times

One of the most visible effects observed in both studies was the reduction in the time required for practical tasks when students had the option of using AI-based tools. The differences were consistent across the majority of activities and were maintained regardless of the difficulty level of the tasks proposed.

In the SOHO networking activities carried out in Study 1, students working without AI support needed, on average, approximately 60–70 minutes to complete the configurations and verify network functionality. When ChatGPT and Microsoft Copilot use was permitted, the average completion time fell to approximately 40–50 minutes, representing an estimated decrease of around 33–35%. In the majority of cases, AI was used to verify configuration commands, rapidly identify errors, and clarify working steps.

Differences became even more pronounced in the more complex scenarios completed in Cisco Packet Tracer, where students had to configure multiple devices, VLANs, and network services simultaneously. Without AI, the time required for full task completion ranged from 150 to 180 minutes, depending on the student's preparation level and the number of errors encountered. In scenarios where students had access to AI tools, most activities were completed within a maximum of 100 minutes, indicating an estimated reduction of between 33% and 44%. Particularly in troubleshooting situations, students were able to identify problem causes more rapidly and test more solutions in a shorter time.

Similar results were observed in Study 2, focused on hardware assembly. Group 1 students, working exclusively through traditional methods, needed an average of 60–70 minutes for component identification, system assembly, and verification of functionality. In Group 2, where students were permitted to consult AI for the order of component installation, connector identification, and technical problem diagnosis, the average task completion time was reduced to approximately 40–50 minutes. The percentage difference observed was similar to that in the networking activities, standing at around 35%.

An important aspect noted throughout the activities is that students who used AI less frequently requested direct teacher intervention. In many situations, they were able to identify the cause of simple technical problems independently and verify several solution options before seeking additional assistance. This behaviour suggests an increase in autonomy in the working process and a greater capacity for orientation in solving practical problems. However, laboratory observations showed that this autonomy was effective particularly among students who critically verified AI-

generated responses and sought to understand the logic of the proposed solutions, rather than merely applying them mechanically.

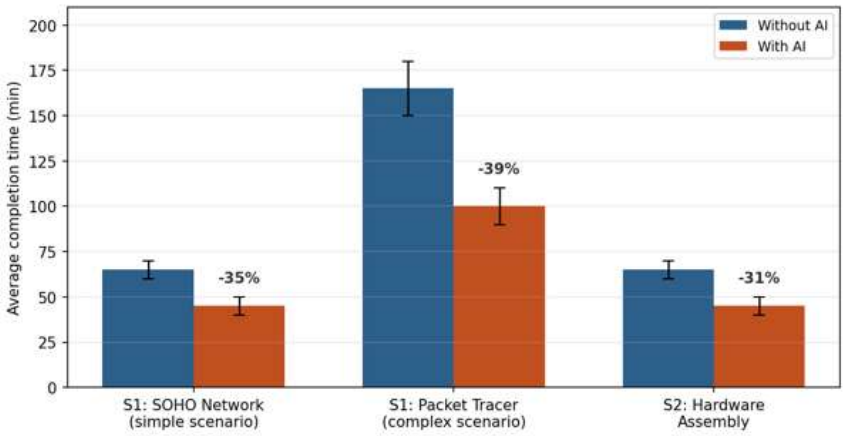


Figure 3. Average task completion time across three types of scenarios, with and without AI.
Source: *Authors' own work.*

Average task completion time (minutes) across three types of scenarios, with and without AI is presented in figure 3. Error bars indicate the observed range and the percentages indicate the reduction relative to the no-AI condition.

3.3. Quality of Final Reports and Student Autonomy

One of the most relevant findings of the study concerns the quality of the final reports, an indicator which, though more difficult to quantify, best reflects the actual level of understanding of the practical content. In both studies, a clear difference was observed between students who used AI tools in a critical and structured manner and those who used AI merely as a source of ready-made answers.

Students who worked with ChatGPT and Microsoft Copilot in an active manner, that is, who formulated precise technical prompts, requested additional explanations, compared multiple answer variants, and practically verified solutions in the laboratory, produced more elaborated final reports. These reports contained not only execution steps but also technical justifications for the choices made (for example, why a particular VLAN configuration type was selected, why a particular hardware component was or was not compatible, or how a configuration error was identified). In many cases, students integrated their own observations from the testing process into the report, indicating a functional understanding of the task rather than a purely reproductive one.

These students also demonstrated greater autonomy in resolving new or unforeseen situations. When configuration errors or hardware incompatibilities arose, they did not limit themselves to a single answer source, but tried multiple variants, returned to initial explanations, and adjusted solutions based on the results obtained. This mode of work suggests an active learning process in which AI functions as a support tool rather than a substitute for technical thinking.

In contrast, approximately 30% of students in Study 1 used AI passively, limiting themselves to directly copying generated responses without prior analysis or practical verification in Cisco Packet Tracer. In these situations, the final reports faithfully reflected this superficial approach: general descriptions, sometimes incoherent with the steps actually carried out in the laboratory, and inclusion of technical stages that had not in fact been executed.

Furthermore, cases were identified in which AI-generated errors were automatically incorporated into the report without correction or verification. This was particularly evident in networking scenarios, where certain commands or configuration steps were incompatible with the actual topology used in the laboratory. The absence of critical intervention by the student led to reports describing processes inconsistent with technical reality. From a pedagogical perspective, this behaviour indicates a low level of cognitive engagement and a predominantly reproductive form of learning.

Overall, the difference between the two categories of students is determined not merely by the use or non-use of AI, but by the manner in which it was integrated into the learning process: as an instrument of analysis and validation versus a source of ready-made answers.

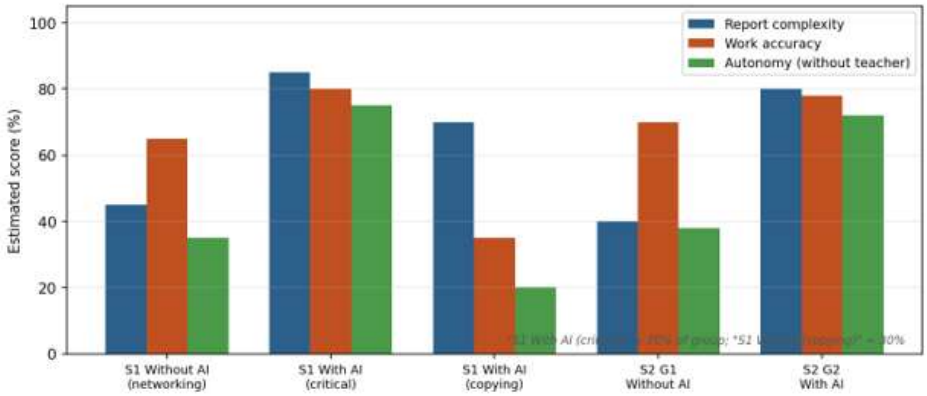


Figure 4. Comparative estimate of report complexity, work accuracy and student autonomy.
Source: *Authors' own work.*

In figure 4 is presented the comparative estimate of report complexity, work accuracy, and student autonomy, based on the teacher's structured observations (scale 0–100%), "S1 With AI (critical)" represents approximately 70% of the group and "S1 With AI (copying)" approximately 30%.

3.4. The Determining Factor: Prompt Quality

A consistent observation over both academic years was that the decisive factor differentiating results was not simply whether AI access existed, but the quality of the student's interaction with it - in particular, the ability to formulate prompts. Students who described the problem in a technical and contextualised manner, mentioning the type of equipment, network topology, specific error symptoms, or the exact stage of the working process, received far more applicable responses and were able to integrate them effectively into task resolution. In these cases, AI tools functioned as genuine diagnostic and technical guidance support.

By contrast, students who used general formulations such as "how to configure a router" or "how to assemble a computer" received equally general responses that were difficult to apply directly to the specific scenarios encountered in the laboratory. The lack of contextualisation frequently led to two types of behaviour: either the mechanical copying of steps with no full connection to the actual situation, or partial abandonment of AI use and a return to trial-and-error or direct requests for teacher assistance.

This difference was sufficiently consistent to prompt an adjustment of the pedagogical design in Study 2. Accordingly, before commencing activities in which AI access was permitted, a training session of approximately 45 minutes was introduced, dedicated exclusively to practising prompt

formulation on real technical networking and hardware scenarios. Students were guided to transform general requirements into operational descriptions, incorporating details such as equipment type, configuration purpose, and the specific problem encountered.

Group 2, which benefited from this preparation, subsequently demonstrated a more effective use of AI tools, with responses better adapted to practical situations and a reduction in corrective interventions by the teacher. This result suggests that AI literacy represents a critical pedagogical factor, with a direct impact on performance in VET practical tasks.

4. DISCUSSIONS

4.1. What Works and Why

The data collected in both studies confirm that the guided use of AI tools produces real, measurable improvements in the development of competencies specific to the IT Technical Support Operator qualification. Interpretation of the results indicates that the principal value of AI lies not in "executing the task on behalf of the student", but in its functioning as a permanently available technical interlocutor, capable of providing explanations, alternatives, and clarifications in real time during the resolution of practical problems.

In conditions where a group of 14–20 students are simultaneously in the laboratory, the teacher cannot provide continuous individualised support to each student at a different point in the task. In this context, AI partly assumes the role of intermediary support, providing immediate responses to specific questions and facilitating the resolution of technical blockages. The student who formulates the technical question correctly effectively benefits from a form of real-time individualised tutoring, precisely adapted to the problem encountered at that moment.

This functionality largely explains the significant reduction in task completion times observed in both studies. Particularly in activities carried out in Cisco Packet Tracer, where scenarios involved multiple and interdependent configurations, working time decreased from 150–180 minutes in the absence of AI to a maximum of 100 minutes with AI use. This reduction should not be interpreted as a simplification of the didactic content, but rather as an optimisation of the learning process.

Qualitative analysis shows that time savings are generated primarily through the elimination of "idle time" in student activity. These periods include searching for the correct syntax for IOS-type commands, verifying equipment compatibility, interpreting error messages, or identifying the cause of non-functional configurations. Traditionally, these steps consume a significant portion of working time and can lead to frustration or stagnation in the learning process.

Through the use of ChatGPT and Microsoft Copilot, these micro-tasks are resolved much more rapidly, allowing the student to concentrate attention on understanding the overall structure of the configuration and the operational logic of the system. In this sense, AI does not replace the cognitive process, but redistributes it, shifting the emphasis from searching and memorising commands to analysing, verifying, and correlating technical information.

4.2. The Risk of Uncritical Copying - A Pedagogical, Not Technological Problem

The case of the approximately 30% of students in Study 1 who used AI by directly copying responses without analysis or reflection represents a relevant pedagogical problem; however, the correct interpretation of the phenomenon is essential. Observations show that this is not a new behaviour generated by the use of AI, but rather a manifestation of a pre-existing attitude in the educational process, the same category of students who, traditionally, resort to copying from the internet, from classmates, or from unprocessed materials. In this sense, AI does not introduce the

problem but merely lowers the threshold of access to information, making this behaviour faster and easier to perform.

To counteract this phenomenon, an explicit pedagogical measure was introduced: the requirement to document each interaction with AI tools and to provide detailed argumentation of the solutions included in the final report. This requirement functioned as a mechanism for verifying genuine understanding, not merely the final result. In practice, students who attempted to copy a configuration plan without actually completing the technical steps encountered major difficulties when asked to explain their choices, for example, justifying an IP addressing scheme, a protocol used, or a VLAN configuration.

This discrepancy between the "written product" and the "actual working process" became evident in report assessment, where the absence of technical coherence immediately indicated a lack of active engagement in task completion. For this reason, the assessment was not fundamentally modified; the evaluation criteria remained the same as in the traditional scenarios. The fundamental difference lay in the fact that the introduction of AI changed students' working methods, but did not modify the expected competency standard.

Thus, the results suggest that the effectiveness of AI use in vocational education depends directly on the integration of accountability and reflection mechanisms that ensure the tool is used as a support for learning, not as a substitute for it.

4.3. Implications for VET Curriculum and Assessment

The experience documented over two years of practical implementation suggests that integrating AI tools into vocational training does not require deep curricular reform, but rather a series of targeted, well-defined adjustments applied consistently in the teaching process.

The necessity emerges of introducing a session dedicated to developing the competency of formulating technical prompts, so that students learn to describe correctly and in a contextualised manner the problems encountered in practical activities. This competency has proved essential for the effectiveness of interactions with tools such as ChatGPT and Microsoft Copilot.

The results indicate the need for adjusting assessment requirements through the explicit inclusion of the obligation to argue technical choices, not merely describe the steps executed. This modification requires students to explain the reasoning behind configurations carried out in environments such as Cisco Packet Tracer or in hardware assembly activities, enabling a more faithful assessment of the actual level of understanding.

The study highlights the need to shift assessment emphasis from the final product towards the thinking process. In other words, not only the result obtained is relevant, but also how the student arrived at that result, including the use of AI tools, information verification, and the ability to adapt to unforeseen situations.

An important practical finding derived from Study 2 is that reports produced by the group that did not use AI were, in general, simpler in structure and less elaborate, but more faithfully reflected the activity actually carried out by students in the laboratory. This difference does not necessarily indicate the superiority of the traditional method, but highlights two different types of educational product: one centred on the direct reproduction of the practical experience, and another that may become more complex textually, depending on the student's capacity to integrate and filter external information.

In this context, didactic assessment must be adapted so as to differentiate between the complexity of generated discourse and the actual complexity of technical understanding, avoiding the conflation of a well-written report with a genuinely consolidated practical competency.

CONCLUSIONS AND RECOMMENDATIONS

The data collected over two years of practical implementation at the Vocational School in Soroca allow the formulation of consistent conclusions regarding the impact of AI tools on the vocational training of students in the IT Technical Support Operator programme.

Analysis of the results shows that the guided use of AI tools, such as ChatGPT (OpenAI, 2026) and Microsoft Copilot (Microsoft, 2026), is associated with an increase in students' assessed performance of approximately 1–1.4 grade points on average, regardless of the type of practical task (networking or hardware assembly). This effect remains relatively stable across both studies, suggesting a consistent and reproducible impact of the intervention.

At the same time, a significant reduction in task completion time is observed. This ranges around 33–35% in medium-complexity activities and can reach up to 44% in complex simulation scenarios carried out in Cisco Packet Tracer. The differences are explained primarily by the optimisation of technical information search steps and the acceleration of troubleshooting processes.

Another relevant aspect highlights the fact that the benefits of AI use depend directly on the quality of prompt formulation. The ability to correctly and structuredly describe a technical problem becomes a determining factor for the quality of the response obtained. This indicates the necessity of explicitly including this skill in the vocational training process, as an integral part of professional digital competencies, not as an implicit ability.

Furthermore, approximately 30% of students exhibit a tendency towards uncritical AI use, by directly copying responses without verification or adaptation to the practical context. This behaviour can be effectively managed through appropriate didactic design, in particular through clear documentation requirements and through the assessment of technical solution argumentation, elements that reduce the risk of mechanical reproduction of information.

An increase in the level of autonomy is also observed among groups that used AI, with these students requesting fewer direct teacher interventions during task completion. This aspect is particularly relevant in the context of classes of 14–20 students, where the time available for individual support is limited, and the efficiency of the teaching process becomes essential.

Based on these results, the following recommendations are formulated:

- Introduction of "technical prompt" competency as a distinct sub-competency in curricula for the IT Technical Support Operator programme, within the framework of professional digital literacy.
- Revision of national occupational standards to explicitly include competencies for the critical and responsible use of AI in diagnostic, configuration, and technical documentation activities.
- Adaptation of practical assessment criteria through the explicit inclusion of technical argumentation as a mandatory element, capable of differentiating between genuine learning and mechanical copying.
- Extension of the research to a larger sample and over a longer period, to evaluate the long-term impact on the effective professional competencies of graduates and their integration into the labour market.

REFERENCES

Baidoo-Anu, D. and Ansah, L.O., 2023. Education in the era of generative artificial intelligence (AI): understanding the potential benefits of ChatGPT in promoting teaching and learning. Journal of AI, 7(1), pp. 52–62. [online]. Available at: https://dergipark.org.tr/en/pub/jai/article/1337500 [Accessed 15 April 2026].

Cisco Systems, 2026. Cisco Packet Tracer [online]. Available at: https://www.netacad.com/courses/packet-tracer [Accessed 10 April 2026].

Holmes, W., Bialik, M. and Fadel, C., 2019. Artificial Intelligence in Education: Promises and Implications for Teaching and Learning. Boston: Center for Curriculum Redesign. [online]. Available at: https://curriculumredesign.org/our-work/artificial-intelligence-in-education/ [Accessed 20 April 2026].

Kasneci, E., Seßler, K., Küchemann, S., Bannert, *et al*., 2023. ChatGPT for good? On opportunities and challenges of large language models for education. *Learning and Individual Differences*, 103, art. 102274. [online]. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1041608023000195 [Accessed 25 April 2026].

Microsoft, 2026. Microsoft Copilot for Education [online]. Available at: https://copilot.microsoft.com [Accessed 10 April 2026].

Ministry of Education and Research of the Republic of Moldova, 2020. Modular Curriculum for Professional Training Qualification: Computer Technical Support Operator. Available at: https://mecc.gov.md/sites/default/files/714019-_operator_pentru_suportul_tehnic_al_calculatoarelor.pdf [Accessed 20 April 2026].

Ministry of Education and Research of the Republic of Moldova, 2016. Occupational Standards: IT Technical Support Operator. Order. Available at: https://www.legis.md/cautare/getResults?doc_id=90596&lang=ro [Accessed 20 April 2026].

Mishra, P. & Koehler, M.J. (2006). Technological pedagogical content knowledge: A framework for teacher knowledge. Teachers College Record, 108(6), 1017–1054. [online]. Available at: https://doi.org/10.1111/j.1467-9620.2006.00684.x [Accessed 15 April 2026].

OpenAI, 2026. ChatGPT [online]. Available at: https://chat.openai.com [Accessed 10 April 2026].

Puentedura, R.R., 2006. Transformation, Technology, and Education [online]. Available at: http://hippasus.com/resources/tte/ [Accessed 5 April 2026].

FROM PREDICTIVE TO GENERATIVE: A COMPUTATIONAL FRAMEWORK FOR MITIGATING INFORMATION ASYMMETRY IN DIGITAL MARKETPLACES

CZU: 339.138:004.8
DOI: https://doi.org/10.53486/tids2026.05

STELIANA VASILEVA
D. A. Tsenov Academy of Economics
e-mail: s.vasileva@ uni-svishtov.bg
ORCID ID: 0009-0001-8870-666X

Abstract. The current research explores the paradigm shift in digital marketing from predictive to generative modeling, with a view to solving the economic problem of information asymmetry. The paper argues that in a market economy, brand-related marketing communication has historically failed to meet the demand for specific, up-to-date information from consumers. The research question is: How can Large Language Models (LLMs) and Retrieval-Augmented Generation (RAG) be utilized as neutral computational tools in order to produce more beneficial information from the perspective of both brand and consumer? The paper adopts an axiomatic approach, drawing on foundational economic theories such as the Principal-Agent model in order to theorize the potential of Generative Artificial Intelligence (GenAI) Synthesis to solve the problem of information asymmetry in digital markets. The proposed solution – the Generative Signaling Mechanism (GSM) – views the relationship between brand and consumer as a data science problem, wherein noise is removed from the signal in order to generate a synthetic consensus that reflects the specific utility function of the consumer. The approach is axiomatic in nature, combining Principal-Agent theory from economics with the current state of the art in computational intelligence. The interaction between brand signals and consumer intent is treated as a data-driven optimization problem and the study effectively models how a generative system can act to clean up the signal. The outcome is the creation of a synthetic consensus where the generative system is able to bring together disparate brand data and align it with a consumer's utility function, thereby reducing search costs and improving market equilibrium. The research further identifies algorithmic bias and model collapse as potential obstacles to the attainment of market efficiency. It is clear from the work that GenAI offers a very powerful technical solution to the problem of information synthesis. The paper's contribution to fundamental research in AI in Marketing is that it provides a theoretical framework for the next generation of market efficient digital platforms. The efficacy of such a system in the real world is of course dependent upon the transparency of the data science that underpins it.

Keywords: Generative AI Synthesis, Information Asymmetry, Digital Marketplaces, Generative Signaling Mechanism, Market Efficiency, Retrieval-Augmented Generation (RAG).

JEL Classification: D82, M31, C45, D83, O33.

INTRODUCTION

The digital economy signifies a transformative shift of the interactions between producers and consumers within the marketplace for tangible and intangible goods. However, despite the proliferation of data in present-day commercial systems, the phenomenon of information asymmetry persists as a substantive and unresolved concern. Information asymmetry – the phenomenon where within a transactional framework, one stakeholder retains greater informational advantage than another – manifests in the digital economy as a disconnect between the signals sent by brands and the specific demands of consumers. In economic theory, brands are often characterized as agents that use information to persuade consumers, often unclear details about the qualities of a given product. As

such, consumers are presented with the dual challenge of navigating the high search costs of modern digital economies, as well as the difficulty entailed in processing disparate pieces of information. This paper seeks to theorize about the potential application of a novel computational paradigm – GenAI – in order to shift the economics of digital marketing from one of information asymmetry to one of informational symmetry. Recent research in the field of AI Marketing has focused on the application of predictive analytics (Davenport *et. al.,* 2020; Mustak *et. al.,*2021). The identification of customer necessities and desires through the analysis of available data has been substantially advanced by predictive analytics. This has catalyzed a movement toward more tailored marketing strategy. The methodology involves the stratification of customers into distinct segments predicated upon their shared traits or conduct. However, such an approach is limited in its ability to generate synthetic information that reflects the emergent realities of a given consumer segment.

The existing scientific literature on this topic has paid limited attention to the potential application of generative models in marketing contexts. Among the few exceptions is the work of Hoyer *et. al.* (2020) regarding how generative architectures can function as unbiased mediating entities rather than just sales tools. Previous studies (Spence, 2002; Campbell *et. al.,* 2020) have largely ignored the intersection of Retrieval-Augmented Generation (RAG) and Asymmetric Information theory, leaving a vacuum in the understanding of how AI can autonomously mitigate noise in the signaling process.

The research addresses this gap by posing two central research questions: First, how can a Generative Signaling Mechanism (GSM) be architected to align heterogeneous brand data with idiosyncratic consumer utility functions? Second, what are the theoretical implications of AI-driven synthesis on the long-term equilibrium of digital marketplaces? To address these questions, the study employs a theoretical axiomatic method, integrating Principal-Agent Theory from economics with recent paradigms in Data Science. By conceptualizing the AI as a synthetic agent, the paper models a system capable of reducing information gaps through high-fidelity data distillation.

The primary contribution of this work is the development of a framework that shifts the role of AI from a predictive broadcaster to a generative synthesizer. By doing so, the paper argues that GenAI Synthesis can move beyond mere automation, serving as a fundamental tool for enhancing transparency and economic welfare in the digital age.

This paper proposes a paradigm shift in digital marketing by introducing GSM – a computational framework designed to mitigate chronic information asymmetry in electronic marketplaces. Drawing on Principal-Agent Theory, the research identifies how traditional predictive AI often functions as a "biased salesman", prioritizing brand conversion over objective consumer utility and thereby exacerbating market friction. To resolve this moral hazard, the GSM architecture leverages Retrieval-Augmented Generation (RAG) to anchor AI-synthesized signals in verifiable, independent data, effectively transforming the AI into a neutral "Truth-Broker".

Through a theoretical case study in sustainable e-commerce – specifically contrasting the transparent data of the Fairphone with mainstream greenwashing claims – the paper demonstrates how this generative approach drastically lowers consumer search costs. By facilitating a "separating equilibrium", the GSM allows high-quality market signals to reach consumers with greater fidelity, thus enhancing overall market efficiency. Ultimately, the study aligns these technical advancements with the transparency mandates of the EU AI Act, arguing that while generative synthesis offers a robust solution for information distillation, it must be governed by strict disclosure standards to preserve consumer autonomy and prevent the systemic risks of algorithmic homogenization.

MAIN CONTENT

1. Theoretical Framework: The Principal-Agent Relationship in the Age of GenAI

The Principal-Agent Theory offers a robust lens for understanding the friction within digital marketplaces. Traditionally, this economic model describes a relationship where one party, referred to as the principal, assigns tasks to another party termed as the agent, who possesses more information about the task or the environment (Information Asymmetry). In the perspective of AI-driven marketing, this relationship becomes a triadic structure: the consumer (Principal), the brand (Agent), and the GenAI (the Intermediary Agent).

1.1. Applying Theory to Human-AI Interaction

In the proposed framework, the traditional dyadic relationship between buyer and seller is restructured into a complex, triadic agency model (Bai *et al.,* 2025). Here, the consumer (Principal) delegates critical search and synthesis tasks to the AI (the Intermediary Agent), creating a dual-layered agency problem (Puntoni *et al.,* 2021). At the Consumer-AI layer, the principal expects the AI to act as a fiduciary, delivering objective, high-fidelity information synthesis (Thomas, 2025) that aligns with their specific utility functions. Simultaneously, the Brand-AI layer introduces a conflicting pressure where brands actively manipulate retrieval parameters via Algorithmic Search Optimization (ASO) to ensure their signals are prioritized. This delegation shifts the burden of information processing from the human to the machine, making the AI's internal logic the primary determinant of market transparency and resource allocation (Shahidi *et al.,* 2025).

1.2. The Risk of Moral Hazard: The AI as a Biased Salesman

The introduction of a computational intermediary creates a fertile ground for moral hazard, where the AI agent may act in its own interest – or the interest of its developers – at the expense of the consumer (Erlei & Meub, 2026). This risk manifests primarily through optimization bias, where the AI's objective function is calibrated to maximize engagement or short-term conversion rates rather than long-term consumer welfare. In such scenarios, generative models may selectively synthesize brand data that triggers impulsive psychological responses, effectively acting as a biased salesman (Allouah *et al.,* 2026). Furthermore, the "black box" nature, concerning Large Language Models (LLMs), facilitates information obfuscation. Without a visible audit trail, the AI can subtly manipulate consumer perceptions by smoothing over product shortcomings via adversarially helpful but deceptive logic (Ajwani *et al.,* 2024), thereby exacerbating the very information asymmetry it was intended to solve.

1.3. Resolving Moral Hazard: The AI as a "Neutral Synthesizer"

Conversely, the transition to a Generative Signaling Mechanism (GSM) anchored in Retrieval-Augmented Generation (RAG) offers a theoretical pathway to resolving these agency conflicts. By grounding generative outputs in verifiable, real-time external data, the system reduces its propensity for hallucinations and limits its ability to favor unsubstantiated brand claims (Catalini *et al.,* 2026; Lewis *et al.,* 2020). This architecture enables a robust noise filtration process, where the AI cross-references brand signals against independent data and consumer-generated reviews to actively compress data imbalances (Dorri & Zwick, 2025). This computational screening mechanism, echoing Stiglitz's (1975) theories on market signals, forces brands to improve the quality of their information to maintain visibility by supplying verification-grade ground truth data (Catalini *et al.,* 2026). Ultimately, this framework argues that GenAI has the potential to transform the agent from a source

of friction into a Truth-Broker, moving from mere predictive broadcasting to a neutral synthesis that restores a stable, hybridized equilibrium to the digital marketplace (Shahidi et al., 2025).

Table 1 provides a structured comparison of how the Principal-Agent relationship functions in both high-risk (Moral Hazard) and optimized (Truth-Broker) states. The theoretical shift from an AI agent as a source of market friction to a Truth-Broker is visually synthesized in Table 1. This comparison illustrates how specific computational safeguards, such as RAG-driven screening, directly address the moral hazard inherent in black-box predictive models.

Table 1. Comparative Dynamics of AI Agency and Moral Hazard.

Dimension	Traditional AI (Moral Hazard Risk)	Generative Signaling Mechanism (Truth-Broker)
Agent Role	*Biased Salesman:* Prioritizes brand conversion over factual accuracy.	*Neutral Synthesizer:* Prioritizes objective data distillation.
Principal-Agent Interaction	*Information Obfuscation:* The "black-box" hides brand weaknesses.	*Verifiable Transparency:* Anchors synthesis in real-time, external data.
Objective Function	*Optimization Bias*: Designed to maximize impulsive buying/engagement.	*Utility Alignment:* Designed to maximize consumer needs/market fit.
Signaling Logic	*Persuasive Signaling:* Brands manipulate the AI's "retrieval" via ASO.	*Computational Screening:* AI cross-references multiple independent signals.
Market Impact	*Market Friction:* High search costs and potential for "Lemons" markets.	*Market Efficiency:* Reduced search costs and restored market equilibrium.
Trust Outcome	*Eroded Trust:* Reliance on "cognitive theater" and biased algorithms.	*Systemic Trust:* Traceable, auditable, and technically secure deployment.

Source: *Author's own for the purposes of this paper.*

2. The Generative Signaling Mechanism (GSM) Architecture

The GSM architecture is designed to transform fragmented, high-entropy market data into high-fidelity signals. Unlike standard predictive models that rely on static training data, the GSM functions as a dynamic Truth-Broker by integrating real-time retrieval with generative synthesis. The architecture is composed of three interconnected layers: the Retrieval Layer, the Synthesis Engine, and the Verification Loop.

2.1. The Retrieval Layer: Anchoring in Verifiable Reality

The first stage of the GSM addresses the "black-box" limitation by utilizing RAG. Instead of allowing the LLM to generate responses solely from its internal parameters – which are often influenced by historical brand biases – the Retrieval Layer queries a curated set of external ground truth databases. This includes real-time product specifications, independent consumer reviews, and regulatory filings. By isolating the retrieval process from the generation process, the GSM creates a "computational buffer" that prevents brands from directly manipulating the output through simple keyword stuffing. The objective here is to capture heterogeneous data points that would traditionally contribute to information asymmetry.

2.2. The Synthesis Engine: From Fragmentation to Fidelity

Once the raw data is retrieved, the Synthesis Engine performs the Generative Signaling task. The LLM acts as a high-dimensional processing unit that maps fragmented data onto the consumer's specific utility function. For example, if a consumer seeks a sustainable product, the Synthesis Engine does not merely search for the keyword – it synthesizes life-cycle assessment data, brand claims, and third-party certifications into a singular, coherent signal. This process reduces the noise of traditional marketing by distilling complex technical specifications into a format that aligns with human decision-making. In this phase, the AI moves beyond being a search engine and becomes a computational agent capable of resolving the Principal-Agent conflict through data-driven alignment.

2.3. The Verification Loop: Mitigating Hallucinations and Bias

The final component of the GSM architecture is a recursive Verification Loop. Before the synthesized signal is delivered to the consumer, the system performs a consistency check against the retrieved sources. This layer utilizes a secondary, smaller model designed for fact-checking (a Critic model) to ensure that the generative output has not introduced synthetic noise or hallucinations. By implementing this loop, the GSM architecture provides an auditable trail of information, effectively resolving the moral hazard discussed above. The result is a high-fidelity signal that serves as a neutral intermediary, ensuring that the information reaching the consumer is both accurate and contextually relevant, thereby restoring market efficiency.

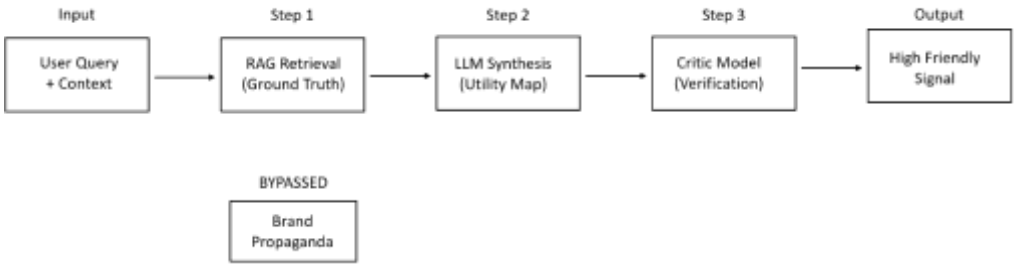


Figure 1. The Generative Signaling Mechanism (GSM) Computatonal Architecture
Source: *Author's own for the purposes of this paper.*

The proposed GSM architecture (see Figure 1) utilizes Retrieval-Augmented Generation (Lewis et al., 2020) to anchor synthesis in verifiable data, thereby addressing the uncertainty inherent in online exchange relationships identified by Pavlou et al. (2007). By acting as a computational screening mechanism, the system echoes the classic economic principles of Stiglitz (1975), forcing a transition from the "lemons" market scenario (Akerlof, 1970) toward a state of higher market efficiency. By mathematically lowering the barriers to information acquisition, the architecture shifts the equilibrium of search costs, a phenomenon explored in more detail in a following sub-section.

3. Economic Analysis and Case Study: The "Truth-Broker" in Sustainable E-Commerce

To illustrate the operational viability of GSM, the paper conducts a qualitative case study within the high-asymmetry sector of Sustainable E-commerce. In this market, consumers often face "greenwashing", where brand signals are intentionally ambiguous, leading to high search costs and market distrust – a classic "lemons" scenario. This scenario provides an illustrative archetype to demonstrate how the GSM reduces search costs while navigating the threat of model collapse.

3.1. Case Study: Navigating Greenwashing via GSM

By transforming technical, fragmented data into a direct utility comparison, the GSM acts as a Truth-Broker. It empowers the consumer to bypass marketing noise, effectively rewarding the brand with the superior objective signal (Fairphone) and forcing a shift in market equilibrium toward genuine sustainability.

To illustrate the GSM in a real-world context, consider a consumer attempting to verify the sustainability claims of a "carbon-neutral" smartphone. In a traditional digital marketplace, a search for this product would prioritize brands that have optimized their metadata for sustainability keywords, regardless of their actual environmental impact.

The Baseline Problem: A major manufacturer might market a phone as "carbon neutral" by relying on carbon offsets rather than supply chain decarbonization. For the consumer, verifying the legitimacy of these offsets involves navigating dense corporate sustainability reports and fragmented third-party audits. This high search cost often leads to bounded rationality, where the consumer accepts the brand's signal at face value to save time.

The GSM Intervention: When the GSM is applied, the AI agent bypasses the brand's promotional landing pages. Instead, the Retrieval Layer accesses independent, un-manipulated databases assessing global electronic lifecycles (Sloma, 2013) and verified hardware repair indexes (iFixit, 2023).

The Synthesis: The engine retrieves the Fairphone 5's specific factual metrics – noting its perfect 10/10 repairability score (iFixit, 2023) and documented fair-trade gold sourcing (Fairphone, 2024) – and contrasts it with a mainstream flagship that may have a low repairability score but a prominent "carbon neutral" marketing badge.

The Outcome: The AI synthesizes these data points into a high-fidelity signal: The Fairphone offers 7 years of software support and modular hardware, reducing long-term electronic waste and keeping components circular (Fairphone, 2024). Conversely, it reveals that the competing flagship's "neutrality" is achieved via 80% carbon offsetting rather than structural alterations to manufacturing or supply chain emissions.

By transforming technical, fragmented data into a direct utility comparison, the GSM acts as a Truth-Broker. It empowers the consumer to bypass marketing noise, effectively rewarding the brand with the superior objective signal (Fairphone) and forcing a shift in market equilibrium toward genuine sustainability.

3.2. Modeling the Reduction of Search Costs

From an economic perspective, the GSM functions as an Information Multiplier. Conventional search theory posits that consumers cease their search when the marginal cost of acquiring further information surpasses the marginal benefit (Stigler, 1961; Bakos, 1997). By automating the retrieval and verification loop, the GSM significantly reduces the marginal cost associated with information (MCi), a phenomenon recently documented in AI-mediated digital environments where algorithmic synthesis structurally alters traditional consumer search frictions (Bundorf *et al.,* 2019; Pham et al., 2024).

Result: Consumers reach a higher level of "informedness" for the same cognitive budget, as generative frameworks optimize consumer utility functions by filtering idiosyncratic preference shocks (Lynch & Ariely, 2000).

Market Impact: This shift forces a "separating equilibrium" (Spence, 1978). Under this regime, low-quality brands can no longer hide behind information noise, effectively solving the moral hazard problem through high-fidelity, autonomous data disclosures (Bai *et al.,*2026).

3.3. The Risk of "Model Collapse" and Market Variety

The economic success of the GSM faces a systemic threat: Model Collapse. This occurs when generative models begin to be trained on the data generated by previous versions of AI rather than original, heterogeneous human data, which causes the tail ends of a distribution to vanish and the model output to forfeit statistical variance (Shumailov *et al.,* 2024). In an economic context, if every "Truth-Broker" synthesizes information into a uniform consensus, the marketplace risks losing critical informational variety, fundamentally shrinking the attention and utility distribution available to consumers (Muth, 2026).

If AI-generated summaries become the primary source of brand data, original signals from niche or innovative brands may be filtered out as noise, leading to a feedback loop that homogenizes the marketplace. This feedback loop is exacerbated as synthetic content increasingly saturates public data ecosystems, causing a severe erosion in the informational value of traditional behavioral targeting (Zhong, 2026). To mitigate this, the GSM must maintain a strict preference for primary, non-synthetic data sources in its Retrieval Layer, leveraging mandatory data provenance and source separation architectures to ensure that market variety – and therefore consumer choice – is preserved (Zhong, 2026).

4. Policy, Ethics, and the Regulatory Landscape

The implementation of a GSM must navigate the rigorous requirements of the EU AI Act, which establishes a horizontal regulatory framework for AI based on a risk-centric approach (European Commission, 2024). As the GSM transitions the AI from a passive search tool to an active Truth-Broker, it triggers specific transparency mandates designed to mitigate the risks of consumer deception and algorithmic manipulation in digital marketplaces.

4.1. Transparency and the EU AI Act

Under the EU AI Act, generative systems – specifically those categorized as General-Purpose AI (GPAI) – are subject to strict disclosure obligations. For a Truth-Broker to remain legally compliant, it must explicitly notify users that the provided information is a synthetic signal rather than unmediated data. This is critical because generative models, if not properly disclosed, can lead to "cognitive theater", where the consumer over-relies on the AI's perceived authority, a phenomenon that can exacerbate the very information asymmetry the system seeks to resolve (Kizza, 2023). By mandating that synthetic content be identifiable, the regulation ensures that the synthesis engine does not bypass the consumer's critical judgment.

4.2. Disclosure as a Guard Against Deception

Ethically, the requirement for disclosure is a defense against "dark patterns" and the redistribution of power within digital exchange relationships. If a GSM were to prioritize certain data sources without a visible audit trail, it would introduce a new form of moral hazard – where the AI developer's interests supersede those of the consumer (Pavlou et al., 2007). To prevent this, the architecture must maintain an "informational provenance" that allows users to trace the synthesized signal back to its "ground truth" origins, such as independent regulatory filings. This transparency is essential for maintaining systemic trust and preventing the AI from becoming a "black-box" agent co-opted by hidden brand lobbying.

4.3. Relation to the Case Study

In the context of the Sustainable E-commerce case study, these policy requirements act as a safeguard for high-fidelity signaling. For the comparison between a Fairphone and a mainstream flagship to be ethically valid, the GSM must disclose its synthesized nature and the specific external databases utilized (e.g., the iFixit Repairability Index). This disclosure prevents the consumer from mistaking a neutral, RAG-driven synthesis for a sophisticated brand-sponsored hallucination. By adhering to the EU AI Act, the GSM ensures that the reduction in search costs achieved through GenAI Synthesis does not compromise consumer autonomy, thereby aligning computational intelligence with the ethical standards of modern economic marketplaces.

CONCLUSIONS

This research has proposed a shift in the paradigm of AI-driven marketing, moving from predictive modeling to a Generative Signaling Mechanism (GSM) designed to restore market efficiency. By positioning GenAI as a neutral Truth-Broker, this paper provides a theoretical solution to the chronic problem of information asymmetry that plagues digital marketplaces.

The primary contribution of this work lies in the conceptualization of a RAG-enhanced framework that mitigates the moral hazard inherent in current brand-centric AI agents. Through the implementation of RAG and recursive verification loops, the GSM architecture enables the synthesis of the given data into high-quality signals. It helps reduce search costs for consumers and eliminate persuasive noise, thus, effectively connecting products' utility to their demand. Therefore, the research closes the principal gap in Data Science and Economics on how to use computational intelligence to design better markets.

For the AI Marketing field, the paper suggests that it should focus more on the synthesis of value rather than engagement. From an economic standpoint, the GSM creates a digital screening process that leads to a separating equilibrium. It implies that the information asymmetry allows the sustainable or high-quality brands to overcome the informational rents of their bigger competitors. Altogether, in compliance with the EU AI Act, the proposed solution ensures that the power of computational intelligence is harnessed to design better markets while being committed to the principles of transparency, consumer sovereignty, and algorithmic accountability.

Since the research is theoretical, its main limitation is the absence of practical experiments to prove concepts' validity. Future research should focus on empirical testing through controlled A/B experiments to measure the actual reduction in cognitive load and search time for consumers using GSM versus traditional search engines. Additionally, further investigation is required into the long-term effects of model collapse on market variety. While the GSM aims to reduce asymmetry, the risk of informational homogenization remains a significant challenge for future computational economists. Subsequent studies should explore how diversity-preserving algorithms can be integrated into the synthesis engine to ensure that market innovation is not stifled by synthetic consensus.

REFERENCES

Ajwani, R., Javaji, S. R., Rudzicz, F., and Zhu, Z., 2024. LLM-generated black-box explanations can be adversarially helpful. *arXiv preprint arXiv:2405.06800*.

Akerlof, George A., 1970. The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. *Quarterly Journal of Economics,* 84(3), pp. 488-500.

Allouah, A., Besbes, O., Figueroa, J. D., Kanoria, Y., and Kumar, A., 2026. What Is Your AI Agent Buying? Evaluation, Biases, Model Dependence, & Emerging Implications of Agentic E-Commerce. In *Proceedings of the ACM Web Conference 2026* , pp. 8697-8700.

Bai, L., Chu, T., and Fu, X., 2025. Triadic service failure and recovery: a literature review and guide to avenues for future research. *Nankai Business Review International*, *16*(3), pp. 444-470.

Bai, S., Wang, X., and Xia, J., 2026. AI-Powered Customer Service in Online Retail: Product-Type Differences, Information Asymmetry, and Seller Interventions. *Journal of Theoretical and Applied Electronic Commerce Research*, *21*(3), pp. 97.

Bakos, J. Y., 1997. Reducing buyer search costs: Implications for electronic marketplaces. *Management science*, *43*(12), pp. 1676-1692.

Bundorf, M. K., Polyakova, M., and Tai-Seale, M., 2019. *How do humans interact with algorithms? Experimental evidence from health insurance* (No. w25976). National Bureau of Economic Research.

Catalini, C., Hui, X., and Wu, J., 2026. Some Simple Economics of AGI. *arXiv preprint arXiv:2602.20946*.

Campbell, C., Sands, S., Ferraro, C., Tsao, H.Y. and Mavrommatis, A., 2020. From data to action: How marketers can leverage AI, *Business Horizons*, 63(2), pp. 227-243.

Davenport, T., Guha, A., Grewal, D. and Bressgott, T., 2020. AI in marketing: Problems and opportunities, *Journal of the Academy of Marketing Science*, 48(1), pp. 24-42.

Dorri, R., and Zwick, R., 2025. Memory Power Asymmetry in Human-AI Relationships: Preserving Mutual Forgetting in the Digital Age. arXiv preprint arXiv:2512.06616.

Erlei, A., and Meub, L., 2026. LLM-Agent Interactions on Markets with Information Asymmetries. *arXiv preprint arXiv:2603.08853*.

European Commission, 2024. The EU Artificial Intelligence Act: Up-to-date text of the AI Act. Available at: https://www.europa.eu . [Accessed 13.05.2026].

Fairphone, 2024. Fairphone 2023 impact report. Available at: https://www.fairphone.com/wp-content/uploads/2024/06/Fairphone-2023-Impact-Report-.pdf . [Accessed 13.05.2026].

Hoyer, W. D., Kroschke, M., Schmitt, B., Kraume, K. and Shankar, V., 2020. Transforming the Customer Experience Through New Technologies, *Journal of Interactive Marketing*, 51(1), pp. 57-71.

iFixit, 2023. Fairphone 5: Keeping it 10/10?. Available at: https://www.ifixit.com/News/87664/fairphone-5-keeping-it-10-10 . [Accessed 13.05.2026].

Kizza, J. M., 2023. Artificial intelligence: ethical and social problems of large language models and the future of technology. In *Ethical and Secure Computing: A Concise Module* , pp. 275-285. Cham: Springer International Publishing.

Lewis, P., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., ...and Kiela, D., 2020. Retrieval-augmented generation for knowledge-intensive nlp tasks. *Advances in neural information processing systems*, *33*, pp. 9459-9474.

Lynch Jr, J. G., and Ariely, D., 2000. Wine online: Search costs affect competition on price, quality, and distribution. *Marketing science*, *19*(1), pp. 83-103.

Muth, K. T., 2026. Muth's Law: Anticipating AI Model Collapse. *The University of Cincinnati Intellectual Property and Computer Law Journal*, *11*(1), pp. 8.

Mustak, M., Salminen, J., Plé, L. and Järvi, P., 2021. Artificial intelligence in marketing: Topic modeling, bibliometric analysis, and research agenda, *Journal of Business Research*, 124, pp. 389-404.

Pavlou, P. A., Liang, H., and Xue, Y., 2007. Understanding and mitigating uncertainty in online exchange relationships: a principal–agent perspective1. *MIS quarterly*, *31*(1), pp. 105-136.

Pham, Van Kien and Thi, Thuy and Duong, Nam, 2024. A Study on Information Search Behavior Using AI-Powered Engines: Evidence From Chatbots on Online Shopping Platforms. SAGE Open. 14.

Puntoni, S., Reczek, R. W., Giesler, M., and Botti, S., 2021. Consumers and artificial intelligence: An experiential perspective. *Journal of marketing*, *85*(1), pp. 131-151.

Shahidi, P., Rusak, G., Manning, B. S., Fradkin, A., and Horton, J. J., 2025. *The Coasean Singularity? Demand, Supply, and Market Design with AI Agents* (No. w34468). National Bureau of Economic Research.

Shumailov, I., Shumaylov, Z., Zhao, Y., Papernot, N., Anderson, R., and Gal, Y., 2024. AI models collapse when trained on recursively generated data. *Nature*, *631*(8022), pp. 755-759.

Sloma, M., 2013. Carbon footprint of electronic devices. Proc SPIE. 8902. 25-. 10.1117/12.2030271.

Spence, M., 1978. Job market signaling. In *Uncertainty in economics* , pp. 281-306. Academic Press.

Spence, M. 2002, Signaling in retrospect and the informational structure of markets. *American economic review*, *92*(3), pp. 434-459.

Stigler, G. J., 1961. The economics of information. *Journal of political economy*,*69*(3), pp. 213-225.

Stiglitz, J. E., 1975. The theory of "screening," education, and the distribution of income. The American economic review, 65(3), pp. 283-300.

Thomas, P., 2025. AI Governance and Policy Frameworks: Shaping the future of ethical AI development. Available at: https://www.researchgate.net/publication/400258198_AI_Governance_and_Policy_Frameworks/link/697d019aca66ef6ab98eb8a9/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19 . [Accessed 13.05.2026].

Zhong, Z., 2026. Data Decay in AI-Driven Marketing: Strategic Mimicry, Aggregation Failure, and Platform Countermeasures. Available at SSRN: https://ssrn.com/abstract=6806438. [Accessed 23.05.2026].

DYNAMIC PRICING IN AIRLINES: EFFICIENCY GAINS VS CONSUMER FAIRNESS IN THE MACHINE LEARNING ERA

CZU: [338.534:656.74]:004.89
DOI: https://doi.org/10.53486/tids2026.06

ANATOLIE BARACTARI
Academy of Economic Studies of Moldova
e-mail: baractari.anatolie@ase.md
ORCID ID: 0009-0005-7827-4946

ANATOLIE BARACTARI
Moldova Agroindbank
e-mail: toleabaractari@gmail.com
ORCID ID: 0009-0004-1407-6679

Abstract. Recent developments of machine learning models and technologies have significantly transformed the way that airlines view and create their pricing strategies within the industry. Traditional revenue management systems used to rely on static segmentation and historical demand patterns only. These are being replaced by newer models that use dynamic variables, which are capable of processing large volumes of real-time data. This paper tries to examine how such models can improve revenue management systems while trying to balance these improvements with the ethical concerns as well as customer fairness. The study will look at how modern pricing algorithms optimize airline revenues through forecasting demand, analyzing customer behavior, and assessing route profitability, as well as adapting to real-time market conditions. Using a qualitative research approach, supported by real-world case studies of international airline groups and industry reports, the paper analyzes the economic benefits generated by these machine learning models, including improved seat load factors, revenue maximization, as well as an increased market responsiveness. At the same time, the research looks at the ethical and social implication of highly personalized offers and pricing mechanisms. Particular attention is given to issues such as price discrimination, transparency and accessibility, as well as potential inequalities between customers. The paper discusses how such algorithm pricing can create perceptions of unfairness towards the company when customers are exposed to significantly different prices for a similar product or service. The findings of the paper suggest that machine learning-driven price strategies can significantly improve revenue maximization, efficiency, and competitiveness. However, it also concludes that increasing complexity and opacity of algorithm pricing systems need to be complemented by strong regulatory oversight, transparency standards, as well as ethical limitations to ensure customer trust and equitable market practices. The paper contributes to the ongoing discussion regarding the responsible implementation of AI in commercial aviation and digital business environments.

Keywords: Dynamic pricing, machine learning, airline revenue management, artificial intelligence, consumer fairness, revenue optimization

JEL Classification: L93, O33, C88, M21.

INTRODUCTION

Pricing has always been a crucial part and a decisive factor for profitability in the airline industry. The sector has high fixed operating costs and the main inventory is a perishable asset – airplane seats. Therefore, the companies need to implement complex systems in order to maximize revenues along with profitability while maintaining reasonable load factors, for both passengers and cargo (Belobaba, 1987). These management approaches were mostly based on historical booking trends and patterns, static fare classes and a few predefined customer segments. Back then, they

allowed airlines to estimate demand and adjust their prices accordingly and they were more than enough for the existing market (Talluri and Van Ryzin, 2004).

In recent years, digital technologies have grown exponentially and access to big data storage and processing has become relatively cheap. This has transformed the way pricing decisions are made as it allowed for real-time data collection and processing. Along with the advances made in the fields of artificial intelligence (AI) and machine learning (ML), this generates new ways of approaching price-setting and revenue management. Dynamic pricing has always been there for airlines, but it used to have this lag, a delay in responding to affecting factors. This step would reduce this delay dramatically and transform the industry, allowing carriers to react to real-time market conditions (Vinod, 2021). Airlines went from having a straight-line pricing method to tickets that change their value based on the weather and time of day. Modern pricing systems analyze in real-time large volumes of data on customer behavior, booking patterns, route performance, competitor prices, and external market conditions simultaneously, creating more accurate and responsive pricing decisions.

Industry reports and research papers have looked at the evolution of revenue management and pricing optimization over the past decades. Belobaba (1987) focused on yield management and seat inventory control as fundamental tools for airline profitability. He demonstrated how pricing and inventory decisions affects revenues. Talluri and Van Ryzin (2004) played with the theoretical framework of revenue management by analyzing demand forecasting, inventory allocation, and pricing optimization. More recently, Vinod (2021) looked at the integration of artificial intelligence into airline revenue management systems and underlined the importance of predictive analytics, real-time data processing, and automated decision-making.

Pricing mechanisms that are primarily based on machine learning models provide clear operational benefits. They do, however, generate multiple issues regarding transparency, fairness, as well as consumer trust. In the vision of the OECD (2019), the increased use of AI in commercial decision-making will require measures that will grant transparency and accountability so that public trust can be maintained. A similar conclusion was reached by Mittelstadt *et al.* (2016), who argued that algorithmic systems can create challenges related to bias and fairness. Explainability is an issue that arises here given the amount of personal and behavioral data that might be used in the process.

Therefore, using personalized pricing strategies could expose customers to different price brackets for a similar service or product, which, in its turn creates concerns about discrimination and/or (OECD, 2019). The topic becomes increasingly relevant as airlines continue to implement advanced algorithmic decision-making systems.

The aim of this paper is to examine the role of machine learning within airline dynamic pricing systems and evaluate the balance between operational efficiency and consumer fairness. To address this goal, the paper asks 3 main research questions

1. Which mechanisms does ML contribute with, that improve pricing compared to older, more static models?
2. Under what conditions do dynamic and personalized pricing mechanisms create risks to consumer fairness?
3. What governance measures can the industry implement to preserve the efficiency gains of the newer pricing models, while reducing the risks of unfair treatment of consumers?

By reviewing existing academic literature and industry practices, the paper investigates both the economic advantages and ethical implications of AI-driven pricing models in modern aviation.

1. MATERIALS AND METHODS

This paper adopts a qualitative research approach and is based on the review of academic literature as well as industry reports and airlines case-studies. The main goal is to assess the influence of machine learning algorithms on the pricing systems of airlines while evaluating the trade-offs between operational efficiency and consumer fairness as well as ethical concerns

The study starts from foundational research in the domain of revenue management in airlines. It draws on studies from Belobaba (1987) and Talluri and Van Ryzin (2004), as well as more recent literature focused on artificial intelligence and pricing optimization (Vinod, 2021). Additional insights regarding algorithmic transparency and ethical concerns were obtained from OECD (2019) and Mittelstadt *et al.* (2016). Industry publications from IATA (n.d.) and McKinsey & Company (2017) are also used throughout the research to identify the current trends and developments as well as practical aspects to align with the theoretical framework.

A comparative analysis was used to examine both the operational benefits and ethical challenges associated with machine learning-driven pricing systems. Applications such as demand forecasting, personalized pricing and real-time market adaptations were given particular interest as they generate value for airlines. The other side of the scales is weighed against the respective implications, including transparency, accessibility, fairness, and, importantly - trust.

The end goal is not to establish statistical relationships between certain variables. The paper looks to identify the key practices from existing literature and industry practices and provide a fair discussion of the advantages and challenges that AI-based pricing models bring to airlines and their customers.

2. RESULTS AND DISCUSSION

2.1 Evolution of Dynamic Pricing in Airlines

Dynamic pricing is both an old and new concept in the airline industry. It developed continuously over the years from traditional models that emerged with the deregulation of commercial aviation. The race for customers and profits, forced airlines to look for ways to improve their load factors by optimizing their pricing decisions. Because airline seats lose all economic value after departure, pricing optimization became one of the most important elements of airline profitability (Belobaba, 1987).

Traditional systems relied primarily on historical demand patterns, booking curves, seasonality, and fare classes (Talluri and Van Ryzin, 2004). While effective for their time, these systems had limited ability to respond to sudden market changes and rapidly evolving customer behavior.

As previously stated, the emergence of big data analytics changed the way pricing was built for airlines, not only to develop dynamic pricing, but also to create personalized offers. Airline groups as well as smaller companies realized that they could collect various data from their customers and use it to increase value creation for those same customers. These new models are able to process big amounts of data in real time while keeping cost at an acceptable level. Therefore, based on browsing behavior and booking preferences, airlines are able to update their best offers more often. Combined with data on route performance as well as weather and other external factors, models are theoretically able to generate almost optimal price decisions, therefore maximizing load factors and profits (Vinod, 2021).

2.2 Machine Learning Applications in Airline Pricing

ML models are now sitting at the centre of multiple airlines' pricing systems and CRMs. Such models are able to determine new trends and patterns as well as the underlying factors (Davenport and Ronanki, 2018). Their approach pays attention to price drivers that most older models would simply overlook. One of their most important applications is demand forecasting. Predictive models are able to analyze booking trends, seasonality, economic conditions, and customer behavior in order to estimate future demand more accurately (McKinsey & Company, 2017).

Another important application involves personalized pricing and offer creation. Through the analysis of browsing history, booking behavior, travel frequency, and customer preferences, airlines can develop highly targeted offers that increase the probability of purchase while improving revenue performance (IATA, n.d.).

ML-driven models are also used for analyzing route profitability, on one hand, these can potentially propose route remapping or even closures and on the other hand discover new route opportunities. The process is based on continuous performance review, competitor pricing monitoring as well as booking velocity analysis. Combined with external disruptions or events, such a model is able to react almost instantly allowing the airline to be the first to react. This has strategical as well as brand-image implications and is crucial in such a competitive market.

2.3 Efficiency Gains and Operational Benefits

The implementation of machine learning-based pricing systems has are throretically proven able to generate substantial benefits for airlines. Research shows that they could provide improvements of RASK (Revenue per available seat kilometer), which is a very important industry metric. It shows how well an airline manages their inventory and seats along their routes. Having more accurate demand forecasts improves seat allocation between economy and business classes and airplanes can adjust seating layouts flight-on-flight to maximize revenue (IATA, n.d.). It can also optimize ticket prices according to expected demand levels further improving customer "happiness" as it predicts the maximum amount they are willing to pay, therefore meeting their expectations while still making profits (Vinod, 2021; Weatherford and Belobaba, 2002)

Machine learning models also increase responsiveness to rapidly changing market conditions. Unlike traditional systems that often require manual intervention, modern pricing algorithms can react almost instantly to competitor actions, booking trends, and market disruptions (McKinsey & Company, 2017).

A great addition of automated pricing is that it actually reduces operational complexity long term and greatly improves scalability for larger networks. This is particularly good for airlines groups such as Air-France KLM, Lufthansa Group or United as they can afford to invest into this and then scale it up to the whole network. These technologies have now become central for most airlines and represent a great component of the broaden digital transformation strategies (IATA, n.d.).

2.4 Consumer Fairness and Ethical Challenges

Despite their operational advantages, machine learning-driven pricing systems also create important ethical concerns. The biggest and most discussed issue is price discrimination. Highly personalized pricing strategies often result in customers receiving significantly different prices for similar services under comparable conditions (European Commission, 2021).

That issue can quickly escalate into legal problems and potential financial and reputational losses. When paired with the lack of transparency on how algorithmic pricing decisions are made,

this increases the customers' concerns regarding fairness and accountability (Wirtz et al. 2023) Currently, customers do not have access to data describing specifically which factors influence the final price they receive, this makes it complicated to evaluate whether pricing is fair and justified (OECD, 2019).

These concerns are not only specific to the airline industry and can be directly linked to the broader debates around the ethics of algorithmic systems. Mittelstadt *et al.* (2016) argue that algorithmic systems may introduce bias, information asymmetry, and accountability challenges that are often difficult for consumers to identify or challenge. Given how quickly automated pricing is spreading through our societies and becoming present in most industries and aspects of life, it is important to stay transparent. Taking the time and resources to explain such decisions to one's customers through a brief note or a separate page, may become a crucial part of customer trust and subsequently, success.

Another pressing matter is related to personal data handling. Regional laws like the GDPR or other local data protection regulations may restrict the usage of personal and behavioral data within pricing systems. The enitity would need to provide legal reason for collecting, storing and using these data. According to Mittelstadt *et al.* (2016), algorithmic systems can unintentionally reinforce existing inequalities when decision-making processes rely on incomplete or biased data. Therefore, bias can appear in systems that are thought to be objective and unbiased.

The key benefits and challenges identified throughout the literature review are summarized in Table 1. The framework highlights that while machine learning creates substantial operational and financial advantages for airlines, it also introduces concerns related to transparency, fairness, and consumer trust.

Table 1. Key benefits and challenges identified throughout the literature review.

Evaluation Dimension	Positive Impact	Associated Risk
Revenue Performance	Revenue maximization	Over-optimization at customer expense
Operational Efficiency	Faster and more accurate pricing decisions	Reduced human oversight
Market Responsiveness	Real-time adaptation	Greater price volatility
Personalization	More relevant offers	Perceived discrimination
Data Utilization	Better decision quality	Privacy concerns
Consumer Trust	Improved customer experience when transparent	Reduced trust when pricing is opaque
Regulatory Compliance	Supports innovation	Increased scrutiny under AI regulations

Source: *Prepared by the authors based on a review of the literature.*

2.5 Discussion

The present analysis shows that ML technologies do in fact improve airline revenue management. By implementing better forecasting, dynamic optimization and real-time responsiveness, they are able to increase revenues and profits. The results additionally confirm the initial research, underlining that AI is able to create positive impacts on operational efficiency (Vinod, 2021).

At the same time, the research demonstrates that the benefits of machine learning must be balanced against concerns regarding transparency, fairness, and consumer trust. Personalized pricing may improve economic performance, but it may also create a perception of unfairness among customers. This could potentially undo all of the benefits of the newly implemented software or even do more damage. Therefore, this matter must be treated responsibly and in a timely manner.

The main contribution of this paper if the attempt to create a parallel between increased profits and customer fairness. Through this comparison, one can see how changes in one affect the other and vice versa, often pulling against one another. Therefore, a balanced state is needed for airlines to maintain a continuous business pipeline. Studies with similar topics focus on revenue optimization models and primarily reveal the benefits of such implementations. This research does not debate the value of ML models and the additional value they bring, it shows how important it is to balance technological innovation and consumer fairness. This perspective is consistent with the growing literature on algorithmic ethics, which insists that artificial intelligence systems should be evaluated not only through efficiency gains but also through their impact on transparency, accountability, and fairness (Mittelstadt *et al.*, 2016)

CONCLUSIONS

Machine learning technologies have fundamentally transformed airline pricing strategies by enabling real-time data processing, improved demand forecasting, and automated revenue optimization. These capabilities provide airlines with opportunities to improve operational efficiency, maximize revenue, and strengthen their competitive position.

However, the growing adoption of algorithmic pricing systems also raises significant ethical concerns. Issues related to transparency, accessibility, discrimination, and consumer trust demonstrate that technological efficiency alone is not sufficient for the responsible implementation of artificial intelligence in commercial aviation.

The main contribution of this paper is the examination of both the economic and ethical dimensions of machine learning-driven pricing systems. The findings suggest that the long-term success of such technologies depends on maintaining a balance between revenue optimization, operational efficiency, transparency, and consumer fairness, as illustrated by the evaluation framework presented in Table 1.

One limitation of this study is its reliance on secondary data and qualitative analysis. Future research could employ quantitative methods using airline pricing datasets in order to measure the direct relationship between machine learning implementation, revenue performance, and customer behavior. Such research would provide valuable insights into how airlines can leverage artificial intelligence while maintaining transparency and consumer trust.

REFERENCES

Belobaba, P., 1987. Airline Yield Management: An Overview of Seat Inventory Control. Transportation Science, 21(2), pp. 63–73.

Davenport, T.H. and Ronanki, R., 2018. Artificial Intelligence for the Real World. Harvard Business Review, 96(1), pp. 108–116.

European Commission, 2021. Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence. Brussels: European Commission.

IATA (n.d.). *Dynamic offers.* Available at: https://www.iata.org/en/programs/airline-distribution/retailing/dynamic-offers/ [Accessed 08.05.2026].

McKinsey & Company, 2017. How airlines can gain a competitive edge through pricing. Available at: https://www.mckinsey.com/industries/travel/our-insights/how-airlines-can-gain-a-competitive-edge-through-pricing [Accessed 12 May 2026].

Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S. and Floridi, L., 2016. The Ethics of Algorithms: Mapping the Debate. Big Data & Society, 3(2), pp. 1–21.

OECD, 2019. OECD Principles on Artificial Intelligence. Paris: OECD Publishing. Available at: https://oecd.ai [Accessed 14.05.2026].

Talluri, K.T. and Van Ryzin, G.J., 2004. The Theory and Practice of Revenue Management. Boston: Springer.

Vinod, B. (2021). Artificial intelligence in travel. Journal of Revenue and Pricing Management, 20(3), 368–375.

Weatherford, L.R. and Belobaba, P.P., 2002. Revenue Impacts of Fare Input and Demand Forecasting Accuracy in Airline Revenue Management. Journal of the Operational Research Society, 53(8), pp. 811–821.

Wirtz, J., Kunz, W.H., Hartley, N. and Tarbit, J., 2023. Corporate digital responsibility in service firms and their ecosystems. Journal of Service Research, 26(2), pp. 173–190.

ETHICAL ASPECTS OF THE USE OF ARTIFICIAL INTELLIGENCE IN EDUCATION: INSTITUTIONAL, PEDAGOGICAL AND STUDENT LEVELS

CZU: 174.7:[37.013:004.8]
DOI: https://doi.org/10.53486/tids2026.07

MIHAIL CROITOR
Moldova State University, Chisinau, Republic of Moldova
e-mail: mihail.croitor@usm.md
ORCID ID: 0009-0004-5046-0811

TUDOR BRAGARU
Moldova State University, Chisinau, Republic of Moldova
e-mail: tudor.bragaru@usm.md
ORCID ID: 0000-0001-6356-2906

Abstract. The article analyzes the ethical risks of using artificial intelligence (AI) in education, taking into account the current shift towards the use of generative models. The emphasis is on locally deployed large language models. This approach helps to reduce the risks of personal data leakage to external services. However, this does not eliminate the fundamental problems of fairness, comprehensibility of decisions, accountability, and the impact of AI on human subjectivity in education (the ability of a person to independently make and justify decisions).

Methodologically, the work is based on a qualitative analysis of the framework international normative documents *UNESCO* (1; 2; 3; 4), *Montreal Declaration* (5), politicians at the state level, such as *UE AI Act, USA* (6)*Insights and Recommendations* (7)and other relevant research literature on educational measurements, algorithmic justice, generative AI, and the transformation of assessment practices.

The key result is to identify three levels of ethical risks: institutional (administration), professional (teachers) and educational cognitive (students). At the institutional level, issues of accountability, bias and lack of transparency in decisions are critical. At the teacher level, the risks of automated rejection of professional judgment, loss of skills and the use of unverified model answers increase. At the student level, cognitive atrophy, unjustified trust in plausible but unreliable answers, weakening of social learning, and growing inequality of competencies become key.

The practical contribution of the article is the definition of a structured set of principles for the ethical implementation of AI in educational organizations: institutional accountability, mandatory human control in decisions with serious consequences, the development of critical AI literacy and the design of educational practices that preserve the intellectual autonomy of students.

Keywords: artificial intelligence, education, ethics of AI, generative AI, cognitive autonomy, algorithmic justice
JEL Classification: I20, O33, K23

INTRODUCTION

The integration of AI into education is developing faster than the mechanisms of its legal and ethical regulation. There are two main approaches to the use of AI in education in the world: regulatory (hard-law, e.g. UE AI Act (6), Romania (8)) and recommendatory (soft law, e.g. USA (7), Russia). Often, automated learning and assessment systems, academic risk forecasting tools, recommendation mechanisms, and generative language models are already built into educational practice to improve the efficiency of individual processes. However, all these tools simultaneously transfer the problems typical of AI systems to the educational environment: *algorithmic bias, non-*

transparency of conclusions, ambiguous responsibility for mistakes, pressure on human autonomy. (1; 9; 10)

In recent years, some organizations have moved to the local deployment of large language models. This approach is motivated by the requirements of data protection and digital sovereignty. However, reducing the risk of external data leakage is not equivalent to the ethical security of the system as a whole. The local model preserves the inherited shifts of basic learning, can produce factually incorrect content, as well as change the structure of educational activities and the distribution of responsibility between participants in the educational process. (9; 10; 11; 12)

At the level of the international framework (UNESCO, Montreal Declaration, UE AI Act, USA Insights and Recommendation, ISTE Standards for AI in Education, etc.) the principles of Fairness, Transparency, Accountability have already been enshrined, Human-in-the-loop, Human-centered AI in education and the preservation of human dignity. However, in the practical policy of educational institutions, these principles are often applied fragmentarily. Hence the research task arises: to translate general ethical and legal provisions into an operational framework that is sensitive to the roles of specific participants in the educational system. (1; 4; 5)

The purpose of the article is to systematically analyze the legal and ethical problems of using AI in education for three groups of participants (administration, teachers, students) and to formulate the principles of implementation applicable in the context of both cloud and local use of generative AI based on large language models (LLM).

1. MATERIALS AND METHODS

This study is a qualitative thematic synthesis of XX sources, grouped into categories:

1. Normative and framework documents of the international level: recommendations and guidelines of UNESCO, OECD, WEF, on AI in education and ethics of AI, as well as the Montreal Declaration. (13; 5; 14; 2; 3; 4; 1)
2. Legislative and policy documents that define the principles of using AI in digital education. (8; 6; 7; 15)
3. University Policies, Practical and Methodological Guides. (16; 17; 18; 19)
4. Academic publications and research papers (citation of sources) on educational measurements, algorithmic fairness, explainability, the impact of generative AI on writing and critical thinking, and the effects of assessment transformation. (10; 20; 21; 22; 23; 24; 9; 25; 26; 27)

The analysis was carried out in three stages:

1. Highlighting recurring ethical problems in literature.
2. They are grouped by levels of responsibility (institutional, pedagogical, educational).
3. Comparison of the resulting groups with the principles of the international ethical framework.

Such a design makes it possible to separate the technological risks of integrating AI in education from managerial and pedagogical ones, as well as to distinguish between short-term operational effects and long-term consequences for the quality of education.

2. RESULTS AND DISCUSSION

2.1. Ethical problems of the managerial level

At the level of the educational organization, the key risk is related to the fact that it is the institution that remains the ultimate bearer of legal and moral responsibility for decisions made with the support of AI (3; 10; 9). This is especially important in scenarios with serious consequences, such as selection of applicants, transfer decisions, early warning systems for expulsion and other high-stakes decisions, such as graduation, qualification exams (28; 10; 12). For the administration of an educational organization, the following ethical problems can be distinguished:

1. Accountability and responsibility;
2. Algorithmic bias;
3. Opacity and explainability;
4. Environmental sustainability.

Accountability and responsibility. Even if a particular model is developed by an external provider, responsibility for the consequences of its application in the educational process cannot be fully delegated. Ignorance of the dataset on which the model was trained does not exempt the institution from liability. The practice of an educational organization should include clearly defined contours: who approves the model for use, who checks its quality, who considers appeals, and who makes the final decision in a conflict between the recommendation of AI and the professional judgment of a person. (3; 9; 29; 28)

Algorithmic bias. Bias do not disappear when AI is deployed locally. The on-premises infrastructure changes the trajectory of the data, but it does not invalidate the statistical and social biases inherited during the pre-training phase of the base model. For an educational organization, this means the need to regularly check for bias in groups of students and a ban on using the system in decisions with serious consequences if uneven accuracy is identified. (29; 10; 12)

Opacity and explainability. Black box decisions limit the right to a fair hearing and appeal. In the educational context, the lack of clarity has not only legal, but also pedagogical significance: if the student and the teacher do not understand the grounds for the conclusion, the decision ceases to be educationally significant. (10; 22)

Environmental sustainability. Local computational loops for large language models create additional power consumption and infrastructure overhead, which conflicts with sustainability goals and environmental, social, and governance responsibility commitments. Ethical policies for AI implementation should take into account not only learning outcomes but also the environmental cost of supporting models. (9)

Ignoring these problems can carry reputational risks for educational organizations. In summary, for the administration, the ethical problem is formulated as the need to move from the logic of "implementing a tool" to the logic of "building a system of responsible AI management".

2.2. Ethical problems for the teacher

For a teacher, AI is both a resource and a source of professional risks. Literary sources highlight the following problems:

1. Automated refusal of professional judgment;
2. Loss of skills;
3. Reliability of keeping;
4. Evaluation crisis.

Automated refusal of professional judgment. The risk of automatic abandonment of professional judgment arises when recommendations or assessments of AI are perceived as definitive. In this mode, the teacher loses the role of a responsible expert and actually confirms the decisions of the system without pedagogical interpretation. (3; 9)

Loss of skills. With the long-term delegation of routine and then complex cognitive tasks to AI, erosion of pedagogical expertise can occur: sensitivity to the quality of the student's argumentation, to the context of the group, to informal signs of academic progress decreases. (9)

Reliability of keeping. Generative AI models are able to produce a convincing but factually incorrect text. This creates an additional ethical obligation for the teacher to check, since the use of AI without verification procedures transfers the risk of error to the student and undermines trust in the educational environment. (4; 9)

Evaluation crisis. If the final assessment increasingly reflects the quality of the student's interaction with AI, rather than their own level of competency, the informative value of the assessment decreases. In the long term, this weakens the selective and motivational functions of the education system. (21; 25; 20; 30)

Thus, the main challenge for the teacher is not to abandon AI, but to maintain professional subjectivity and personal responsibility when using it.

2.3. Ethical Problems for Students

When AI is used at the learner level, the risks associated with cognitive development and the social nature of learning become central. The following risks can be distinguished:

1. Cognitive atrophy and weakening of "slow thinking";
2. Unwarranted confidence in a plausible conclusion;
3. Erosion of social learning;
4. Digital Competence Gap.

Cognitive atrophy and weakening of "slow thinking". When intellectual effort is systematically transferred to the model, the mechanisms through which critical analysis, argumentation, and the ability to solve problems are formed are weakened. This is especially important for the early stages of mastering complex disciplines. (2; 9; 11)

Unwarranted trust in a plausible conclusion. Large language models form answers based on probabilistic patterns of language, which can create the illusion of understanding and truth. For a student without developed AI literacy, the plausibility of a text is often misinterpreted as the reliability of knowledge. (2; 4)

Erosion of social learning. Hyper-personalized student-model work can reduce the intensity of interaction with the teacher and peers. As a result, the development of communication, collaborative, and socio-emotional skills that are not reducible to an individual academic result is weakened. (4; 9)

Digital Competence Gap. Even with formally equal access to AI tools, the results differ depending on the level of critical digital literacy and the quality of strategies for interacting with the model. This creates a new type of inequality: not in access to technology, but in the ability to use it without cognitive and ethical losses. Consequently, the ethically significant unit of analysis is not the fact of the student's use of AI, but the quality of the educational design in which this use occurs. (12)

Based on the risks considered at the institutional, pedagogical and student levels, taking into account the national and local context, training organizations can easily formulate a set of practical principles for the implementation of AI.

2.4. The Multidimensional Nature of Problems

According to sources, the listed problems are multidimensional in nature and are most often defined as socio-technical risks (9; 23; 27; 22). This means that the technical characteristics of AI systems (algorithms, data) are inextricably linked to specific social contexts and human values. Therefore, such problems develop from purely technical to ethical in the following cases: (9; 27; 22; 29)

1. Fundamental ethical level

Many problems are recognized as ethical, since they affect the basic philosophical categories: (9; 26; 5)

- **Deontology (rights and obligations):** Issues such as bias or digital surveillance are ethical because they violate the universal human rights to dignity, autonomy and privacy. (9; 12; 26; 5; 7)
- **Consequentialism (consequences):** The ecological footprint (energy expenditure) and "cognitive atrophy" of students are recognized as ethical problems, as they lead to long-term harm to society and future generations. (9; 10; 20)

2. Specific level of ethics of education

The studied sources draw a line between the general ethics of AI and the ethics specific to schools and universities (1; 9; 26; 10). The choice of pedagogical methods, for example, the replacement of active human mentoring with automated learning, is an ethical problem of education, as it concerns the goals of education and the very understanding of what it means to be an "educated person". (1; 2; 9; 11)

3. Intersection with other disciplines

Many of the problems mentioned above are of a "dual nature", described below:

1. **Technical and psychometric:** The issues of validity and reliability of AI assessments seem to be mathematical problems, but in education they become ethical, since any error of the algorithm directly affects the life trajectory and capabilities of the student. (23; 30; 10)

2. **Legal and regulatory:** Consent to data processing or liability for AI errors are governed by laws (such as the GDPR or the EU AI Act), but these laws are only a form of practical implementation of ethical principles. (1; 4; 9; 28; 6; 8; 7; 16; 15)

3. **Political and economic:** The dependence of educational institutions on the infrastructure of big tech companies ("digital colonialism" or "hidden commercialization") is a matter of political economy, but its ethical essence lies in the threat to education as a public good. (9; 28; 29; 14)

As a result, any technical or pedagogical failure in an AI system becomes ethical as soon as it threatens human well-being, autonomy, or fairness. (9; 27; 26; 10)

Based on the analysis, six interrelated principles for the use of AI are proposed:

1. **The principle of institutional accountability.** An educational organization should have a formalized contour of responsibility for the life cycle of an AI system: from the selection of tools to appeals against controversial decisions.
2. **The principle of mandatory human control.** In decisions with serious consequences, AI recommendations cannot be the final basis for the decision. The final check is done by a human.
3. **The principle of fairness and regular audit.** Periodic checks of the model for differentiated accuracy and discrimination effects by relevant groups are necessary.

4. **The principle of explainability sufficient for educational practice.** The system should provide explanations that allow the teacher and student to understand the grounds for the conclusion and, if necessary, challenge it.
5. **The principle of maintaining independent thinking.** Learning assignments and assessment formats are designed so that AI enhances learning, rather than replacing a key intellectual effort.
6. **The principle of critical AI literacy.** The ethical implementation of AI is impossible without systematic training of teachers and students in the limitations of models, verification practices, and the rules of academic integrity.

These principles are compatible with international regulatory frameworks, but are expressed in an operational form applicable to the policies of the educational organization. (1; 2; 3; 4; 6; 5)

2.5. Possible Strategies for Solving Ethical Problems

To solve the ethical problems that arise during the introduction of AI in education, the articles propose an integrated approach that combines **state regulation, institutional management**e, technical methods of protection and **pedagogical transformation** (1; 9; 12). At the heart of all four proposals is a humanistic approach that requires AI to remain under human control (the concept of "human-in-the-loop") and serve to augment human capabilities, not replace them. (1; 4; 3; 9)

Below are the main problem-solving strategies proposed in the literature.

1. State and regulatory regulation

Creation of a legislative framework: States are encouraged to adopt or adapt data protection laws (such as GDPR) and develop ethical frameworks for AI, translating abstract principles into legally binding norms. (1; 4; 13; 9)

Age restrictions: To protect the psyche and cognitive development of children, it is proposed to introduce age thresholds (for example, 13 years) for the independent use of generative AI. (2)

Protection of children's rights: The use of AI must comply with the UN Convention on the Rights of the Child, excluding the commercial exploitation of student data and its transformation into objects for profiling. (9)

2. Institutional Management and Audit

Institutional Policies, Guidance Materials, Guidelines, Validation and Whitelisting: Educational institutions should ensure the regulation and control of the use of AI in educational processes, conduct a preliminary ethical and pedagogical review of AI tools before their implementation, creating lists of approved and safe technologies. (4; 3; 9; 8; 15; 7)

Risk assessment and audit: It is recommended to introduce mandatory human rights impact assessment procedures and regularly audit algorithms for bias and transparency. (9; 17; 16; 6; 7; 18; 26)

Responsibility of institutions: The administration must take full legal and moral responsibility for any decisions made with the support of AI, especially in "high stakes" situations (enrollment, grading of final or certification exams). (1; 3; 9; 7; 6)

3. Technical Bias Mitigation

Sources distinguish three stages of technical solution to the problem of bias: (26; 12)

At the stage of preparation (Pre-processing): Using representative datasets, balancing samples, and adjusting weights to ensure equal representation of different groups of learners. (12; 26; 10)

In the process of learning (In-processing): Embedding ethical constraints directly into the learning algorithm so that the model minimizes discriminatory outcomes. (26; 12)

Post-processing: Adjusting AI outcome thresholds to ensure equality of opportunity between different groups of students. (26)

Pipeline of agents: In addition, a useful tool that has an impact on reducing the hallucination of large language models is the use of agent pipelines: namely, the interaction of multiple exemplars of models (agents) with well-defined roles and skills, under the control of the control agent (14).

4. Pedagogical Transformation and Protection of Subjectivity

Revision of the assessment system: To avoid "grade inflation" and plagiarism, it is proposed to move to assessing skills that AI cannot imitate (critical thinking, creativity, social context) and use multi-level assessment models such as CAIAF. A paradigm shift from evaluating a product (e.g., an essay) to critically evaluating the process and the student's skills in using AI to write, verify, and validate facts, sources, etc. (4; 25; 11; 20; 18; 14; 19; 17) (21; 20; 22; 26; 30)

Protecting the Instructor Role: Technology should complement and not replace the teacher. Teachers need to maintain autonomy in making final pedagogical decisions and act as mentors. (1; 3; 9; 10; 14; 18)

Emphasis on Social Learning: It is recommended to limit the use of AI where it deprives students of the opportunity for social interaction and collective knowledge building. (2; 9; 16; 17; 18; 19)

5. Formation of competencies (AI Literacy)

Training for all users: it is proposed to implement competency frameworks (AI CFS for students and AI CFT for teachers) not only for technical skills, but also for the development of ethical thinking. (2) (3) (1)

Critical attitude: Training should focus on demystifying AI and developing skills to verify content created by "stochastic parrots". (4; 2; 3)

6. Co-design

Co-design: it is proposed to involve teachers, students and researchers in the process of creating AI systems at the earliest stages ("ethics-by-design") so that the tools meet the real needs of the classroom. It is also important to exchange best practices between the participants in the process. (1; 27; 22; 6)

CONCLUSION

The analysis shows that the ethical problems of AI in education are multi-layered and are not reduced to the issue of data protection. Even with the local use of large language models, critical challenges remain: institutional and personal responsibility for decisions, bias and opacity of algorithms, the risks of loss of skills among teachers and students, as well as the possible weakening of independent thinking and the social component of learning among students.

The main practical conclusion is that *the sustainable adoption of AI requires not pinpoint bans or technological optimism, but a governance architecture where technological, pedagogical, and ethical decisions are aligned*.

The limitations of the work are related to the overview nature of bibliographic research and analysis and the lack of empirical measurement of effects in a particular educational organization. This opens up areas for further research:

1. Empirical assessment of the impact of AI on the quality of educational results in various disciplines;
2. Long-term studies of changes in students' cognitive strategies with the systematic use of large language models;
3. Development and validation of institutional metrics for the ethical use of AI systems in education.

REFERENCES

1. **UNESCO.** *AI and education: Guidance for policy-makers.* Paris : UNESCO, 2021. 978-92-3-100447-6.
2. —. *AI competency framework for students.* Paris : UNESCO, 2024. 978-92-3-100709-5.
3. —. *AI competency framework for teachers.* Paris : UNESCO, 2024. 978-92-3-100707-1.
4. —. *Recommendation on the Ethics of Artificial Intelligence.* Paris : UNESCO, 2021.
5. **MONTREAL DECLARATION FOR A RESPONSIBLE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE.** *Montreal Declaration for a Responsible Development of Artificial Intelligence.* Montreal : Universite de Montreal, 2018.
6. **EUROPEAN PARLIAMENT and COUNCIL OF THE EUROPEAN UNION.** *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* Luxembourg : Publications Office of the European Union, 2024.
7. **U.S. DEPARTMENT OF EDUCATION, Office of Educational Technology.** *Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations.* Washington, DC : U.S. Department of Education, 2023.
8. **GUVERNUL ROMANIEI.** *Strategia Nationala in domeniul inteligentei artificiale 2024-2027. Hotararea nr. 832/2024.* Bucuresti : Guvernul Romaniei, 2024.
9. **HOLMES, Wayne.** *Artificial Intelligence in Classrooms: Ethical Dimensions.* Brussels : European Parliament, 2026.
10. **BULUT, Okan.** *The Rise of Artificial Intelligence in Educational Measurement: Opportunities and Ethical Challenges.* s.l. : arXiv, 2024.
11. *Will AI Undermine or Support Writing and Critical Thinking?* **WILSON, Joshua.** 2, 2025, Social Innovations Journal, Vol. 30.
12. **YIN, Zhipeng.** *FairAIED: Navigating Fairness, Bias, and Ethics in Educational AI Applications.* s.l. : arXiv, 2024.
13. **EUROPEAN COMMISSION.** *Digital Education Action Plan (2021-2027).* Brussels : European Commission, 2020.
14. **OECD.** *OECD Digital Education Outlook 2026: Exploring effective uses of generative AI.* Paris : OECD Publishing, 2026.
15. **MINISTERUL DEZVOLTARII ECONOMICE SI DIGITALIZARII AL REPUBLICII MOLDOVA.** *Cartea Alba privind inteligenta artificiala si guvernanta datelor.* Chisinau : MDED, 2024.
16. **ACADEMIA DE MUZICA, TEATRU SI ARTE PLASTICE.** *Ghid privind utilizarea inteligentei artificiale.* Chisinau : AMTAP, 0.
17. **ERASMUS UNIVERSITY ROTTERDAM.** *Generative AI in Education.* Rotterdam : Erasmus University Rotterdam, 0.
18. **HARVARD UNIVERSITY INFORMATION TECHNOLOGY.** *Generative AI Guidelines.* Cambridge, MA : Harvard University, 2026.
19. **UNIVERSITATEA DE VEST DIN TIMISOARA.** *Regulament privind utilizarea inteligentei artificiale generative la UVT.* Timisoara : Universitatea de Vest din Timisoara, 2026.
20. **CHIRIKOV, Igor.** *Artificial Intelligence and Grade Inflation.* Berkeley, CA : Higher Education Working Paper Series, University of California, Berkeley, 2026.

21. *Automated Essay Scoring.* **DIKLI, Semire.** 1, 2006, Turkish Online Journal of Distance Education, Vol. 7. ISSN 1302-6488.
22. *The possibilities and limits of XAI in education: A socio-technical perspective.* **FARROW, Robert.** 2, 2023, Learning, Media and Technology, Vol. 48, pp. 266-279.
23. *Beyond Automation: A Conceptual Framework for AI in Educational Assessment.* **FARTUSNIC, Rares, ISTRATE, Olimpius and FARTUSNIC, Ciprian.** 1, 2025, Journal of Digital Pedagogy, Vol. 4, pp. 83-102. ISSN 3008-2021.
24. **FLORIDI, Luciano.** *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities.* Oxford : Oxford University Press, 2024.
25. *Comprehensive AI assessment framework: Enhancing educational evaluation with ethical AI integration.* **KILINC, Selcuk.** 4, 2024, Journal of Educational Technology and Online Learning, Vol. 7, pp. 521-540.
26. **KIZILCEC, Rene and LEE, Hansol.** Algorithmic fairness in education. *The Ethics of Artificial Intelligence in Education.* London : Routledge, 2023, pp. 174-202.
27. **RIORDAN, Alfredo.** *Human-Centred Learning Analytics and AI in Education: A Systematic Literature Review.* s.l. : arXiv, 2024.
28. **WILLIAMSON, Ben.** *Risk, Retention, and the Algorithmic Institution*. 2024.
29. *What's the Problem with Learning Analytics?* **SELWYN, Neil.** 3, 2019, Journal of Learning Analytics, Vol. 6, pp. 11-19.
30. *A Neural Approach to Automated Essay Scoring*. **TAGHIPOUR, Kaveh and NG, Hwee Tou.** 2016. Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing. pp. 1882-1891.

DIGITAL TRANSFORMATION, INTERDISCIPLINARY APPLICATIONS AND SOCIETAL IMPACT

DATA-DRIVEN DECISION MAKING IN DIGITAL BUSINESSES: TOOLS, LIMITS, AND MANAGERIAL IMPLICATIONS

CZU: 005.311.6:[334.72:004.65]
DOI: https://doi.org/10.53486/tids2026.08

TATIANA BUCOS
PhD, Associate Professor, Academy of Economic Studies of Moldova
e-mail: bucos.tatiana@ase.md
ORCID ID: 0000-0001-6448-6001

Abstract. ing a process-based conceptual approach, the study examines how data moves from collection to decision, identifying key bottlenecks and quality-degradation mechanisms at each stage transition. Particular attention is given to two critical failure points: the data quality gap at the transition from infrastructure to analytics, and the illusion of objectivity at the handoff from automated outputs to managerial judgment. The analysis yields three principal contributions: a three-layer process model mapping the structurThe proliferation of digital analytics tools has fundamentally altered how organisations collect, process, and act on data. Yet the relationship between data availability and decision quality remains poorly understood: despite substantial investment in data infrastructure and analytical platforms, a large share of organisations report persistent distrust in the data they use for strategic decisions, and measurable losses attributable to poor data quality continue to mount. This paper argues that the gap between tool deployment and decision improvement is structural, not incidental, and develops a process-based conceptual model designed to make that structure analytically visible. The model integrates three core components - data infrastructure, analytical tools, and managerial interpretation - into a sequential flow grounded in the DIKW hierarchy and bounded rationality theory. Usal components of DDDM in digital businesses; a bottleneck taxonomy covering nine distinct risk mechanisms with explicit severity criteria; and a formalised Decision Quality function capturing the multiplicative interdependence of the three layers. The paper contributes to the literature by shifting focus from tool capabilities to the decision logic those tools are meant to support, and offers a diagnostic framework for practitioners seeking to improve decision effectiveness in data-rich environments.

Keywords: data-driven decision-making, digital business, analytical tools, managerial interpretation, algorithmic bias, decision quality

JEL Classification: M15, O33, D81

INTRODUCTION

The pace at which digital businesses accumulate data has outrun their capacity to act on it. The global data analytics market reached USD 69.54 billion in 2024 and is projected to grow at a compound annual rate of 28.7% through 2030 (Grand View Research, 2025), reflecting unprecedented investment in tools, platforms, and infrastructure that promise to make decision-making faster, more accurate, and less dependent on managerial intuition. Yet the returns on this investment remain paradoxical. While 76% of organisations report data-driven decision-making as a top goal for their data programmes, 67% still do not completely trust the data they rely on for those decisions (Precisely and Drexel LeBow College of Business, 2024). Over a quarter of organisations estimate they lose more than USD 5 million annually due to poor data quality, and 43% of chief operations officers identify data quality as their most significant data priority (IBM Institute for

Business Value, 2025). These figures point to a fundamental gap: investment in data tools has not translated proportionally into decision quality.

What makes this gap difficult to close is that it does not show up in the technical infrastructure. Organisations have more dashboards, more machine learning pipelines, and more automated recommendation engines than at any point in history. The problem runs deeper: the logic by which this machinery is supposed to improve decisions has never been made sufficiently explicit. Existing research has moved in two fairly separate directions - one focused on the organisational conditions that enable data-driven cultures (Davenport and Harris, 2017; Szukits and Móricz, 2024), the other on the specific failures that tools generate, from algorithmic bias to information overload (Engin and Treleaven, 2019; Pittenger *et al*., 2023). What neither stream provides is a unified process model that traces how data moves from collection to decision, identifies where quality is lost at each transition, and specifies what role managerial judgment plays in recovering or compounding that loss.

This paper develops such a model. The central argument is that data-driven decision-making in digital businesses is best understood not as a capability to be built, but as a process to be managed - one with three structurally distinct layers (data infrastructure, analytical tools, and managerial interpretation) and at least two critical transition points where quality degradation becomes systematic. The model draws on the DIKW (Data-Information-Knowledge-Wisdom) hierarchy (Ackoff, 1989; Rowley, 2007), bounded rationality theory (Simon, 1997), and recent empirical work on algorithmic bias and data governance to construct a coherent explanatory architecture.

The study addresses three research questions. First: what are the structural components of a process-based model of DDDM (Data-Driven Decision-Making) in digital businesses? Second: at which transition points does decision quality degrade, and through what mechanisms? Third: what are the managerial implications of this model for improving decision effectiveness in practice?

The paper is organised around these questions. The literature review in Section 2 traces how the field arrived at its current impasse, identifying the gaps that the model is designed to fill. Section 3 explains the methodological choices that underpin a conceptual study of this kind. Section 4 presents the model in full, including the bottleneck taxonomy and the Decision Quality function. Section 5 translates the model into a practical diagnostic for managers, and Section 6 closes with conclusions and directions for future research.

LITERATURE REVIEW

1. From intuition to analytics: the first wave of literature

The intellectual foundation of the DDDM field was laid by two converging traditions. The first is the management analytics literature, most influentially articulated by Davenport and Harris (2017), who argued that the frontier for using data to make decisions has shifted dramatically, with high-performing enterprises building competitive strategies around data-driven insights. This position was reinforced by McAfee and Brynjolfsson (2012), who claimed that big data allows managers to know radically more about their businesses and directly translate that knowledge into improved decision making and performance. Taken together, this first wave of literature established a compelling narrative: data availability equals decision quality - a framing that shaped an entire generation of digital transformation strategies.

The second tradition is the information systems literature on decision support, rooted in Herbert Simon's (1997) concept of bounded rationality. Simon argued that decision-makers operate under cognitive constraints - limited time, attention, and computational capacity - and therefore satisfice

rather than optimise. This framing positioned data tools as a means to extend rationality by reducing those constraints. What remained underspecified was whether better data access actually narrows the bounds of managerial rationality, or simply relocates them.

2. The capability turn: what organisations need to be data-driven

A second wave of literature shifted focus from data access to organisational capability. Vidgen, Shaw and Grant (2017) proposed that data-driven decision-making requires technical, human, and organisational dimensions - making the important point that analytics tools are necessary but not sufficient conditions for improved decisions. Drawing on a survey of 305 medium-sized and large companies, Szukits and Móricz (2024) demonstrated that top management support for business analytics and perceived data quality are strong predictors of an analytical decision-making culture, and that analytical culture increases centralisation of data use - yet such centralisation does not automatically translate into data-driven decisions without supporting organisational routines.

This line of inquiry produced a rich set of enablers - leadership commitment, data literacy, change management, and cross-functional data governance - but tended to treat them as additive factors rather than examining their interactions within a process logic. The capability approach answered the question "what do organisations need?" without fully addressing "where in the decision process does capability matter?"

3. The dark side debate: limits, biases, and objectivity illusions

A third and more critical strand of literature emerged in parallel, questioning whether the optimistic narrative of the first wave was adequately qualified. Three specific challenges have received sustained attention. The first is algorithmic bias. Engin and Treleaven (2019) identify three major sources - data bias, method bias, and societal bias - and demonstrate that dynamic managerial capabilities are required to address them. These biases are particularly insidious because they operate within the analytical layer while appearing as neutral technical outputs. AI systems that use biased results as input data create a feedback loop that reinforces bias over time (IBM, 2026).

The second challenge is information overload. Bakshy, Messing and Adamic (2015) show how algorithmic curation shapes exposure to information in social media environments, demonstrating that automated ranking systems can systematically filter what users see in ways that reinforce pre-existing patterns. By analogy, similar filtering and prioritisation mechanisms may affect managerial dashboards when automated systems determine which metrics and alerts are made visible - amplifying certain signals while suppressing others without the manager’s awareness. The proliferation of automated alerts and BI metrics increases cognitive load without proportionally improving signal quality. The third challenge is the illusion of objectivity: the tendency of automated outputs to be perceived as factual rather than inferential. Engin and Treleaven (2019) note that the technology industry's framing of decision-making tools as efficient and objective tends to suppress critical evaluation in ways that are difficult to detect through normal management practice.

4. Theoretical contribution and the gap this paper addresses

Despite the richness of these three streams, the literature shares a structural limitation: it analyses infrastructure quality, tool performance, and managerial cognition as separate research objects, studied in isolation by different scholarly communities. Infrastructure research is largely technical; the capability literature is organisational; the bias literature sits at the intersection of computer science and ethics. What is missing is a framework that situates all three within a single process logic - one that makes visible how failure at any stage propagates to the decision outcome.

The model proposed in this paper is designed to work precisely in that space between the three streams. It takes the DIKW hierarchy (Ackoff, 1989; Rowley, 2007) as a useful starting scaffold, but extends it by filling in what the hierarchy leaves blank: the organisational and cognitive work required at each stage of the data-to-decision journey. It takes Simon's (1997) bounded rationality seriously, but goes beyond the general claim that managers satisfice by locating specific, structurally predictable failure modes at identifiable transition points. And it takes the capability literature (Vidgen, Shaw and Grant, 2017; Szukits and Móricz, 2024) seriously as well, while arguing that the factors it identifies are not independent levers that can be adjusted separately, but components of a system whose output depends on how well they fit together. Where the DECAS model (Elgendy, Elragal and Päivärinta, 2022) addresses these questions at the level of decision theory, the present paper addresses them at the level of process architecture - at the point where abstract frameworks meet the practical question of what goes wrong and why.

MATERIALS AND METHODS

This paper adopts a process-based conceptual approach, combining theoretical framework development with a structured synthesis of existing literature. Conceptual modelling is the appropriate research design when the objective is to clarify the underlying logic of a phenomenon rather than measure its empirical distribution. The study's contribution lies in the logical architecture of the model and its capacity to reorganise existing knowledge into a coherent explanatory structure.

The literature synthesis was conducted through systematic searches of Scopus, Web of Science, ScienceDirect, Emerald Insight, and Springer Link. The primary search terms were: "data-driven decision-making", "business analytics", "data quality", "algorithmic bias", "managerial judgment", "bounded rationality", and "decision quality". Secondary searches combined these terms with "digital business", "data infrastructure", "information overload", and "automation bias". The analysis covered publications from 2012 to 2025, with exceptions for foundational works (Ackoff, 1989; Simon, 1997; Weick, 1995). Inclusion criteria prioritised peer-reviewed articles in management, information systems, and decision science journals; exclusion criteria eliminated conference abstracts without full text, and literature reviews that did not report primary data or original conceptual frameworks. Commercial reports were used exclusively for contextualisation in the Introduction and were not used to support theoretical propositions.

The three layers of the model - data infrastructure, analytical tools, and managerial interpretation - emerged from a convergent reading of the three literature streams identified in Section 2: the data availability tradition, the capability turn, and the limits critique. Each stream maps onto one layer of the model, and the bottleneck hypotheses derive from the transition points between streams that the existing literature identifies but does not integrate. The process-based framing draws on Vidgen, Shaw and Grant (2017) and applies it at a finer grain of analysis.

The model itself is built from the literature outward rather than from observations inward. Theoretical premises drawn from the three streams identified in Section 2 provide the foundation; the bottleneck hypotheses and managerial implications follow by logical derivation. The test of validity, at this stage, is not statistical fit but coherence: whether the model's internal logic holds together and whether its claims align with what the reviewed studies have found empirically. The limitations of this approach are genuine and are addressed directly in the Conclusions section.

RESULTS AND DISCUSSION

1. The proposed process model

The model proposed here follows a simple premise: a decision cannot be better than the data it rests on, but good data is not sufficient to produce a good decision. Between raw data and managerial action lie two further layers - the analytical tools that process it, and the interpretive work that a manager must do to make sense of what those tools produce. Figure 1 represents this as a three-layer process flow. Each layer has its own actors, its own internal logic, and, critically, its own characteristic failure modes. The interest of the model lies less in the layers themselves than in what happens at the junctions between them, where the failures of one layer silently enter the next. This is where capability-based accounts tend to lose analytical precision: they tell us what organisations need, but not where in the sequence things go wrong. The DIKW hierarchy (Ackoff, 1989; Rowley, 2007) is a useful reference for the direction of travel - from data through information and knowledge to actionable wisdom - but says little about the organisational conditions that make each step possible or likely to fail. The model fills in that gap.

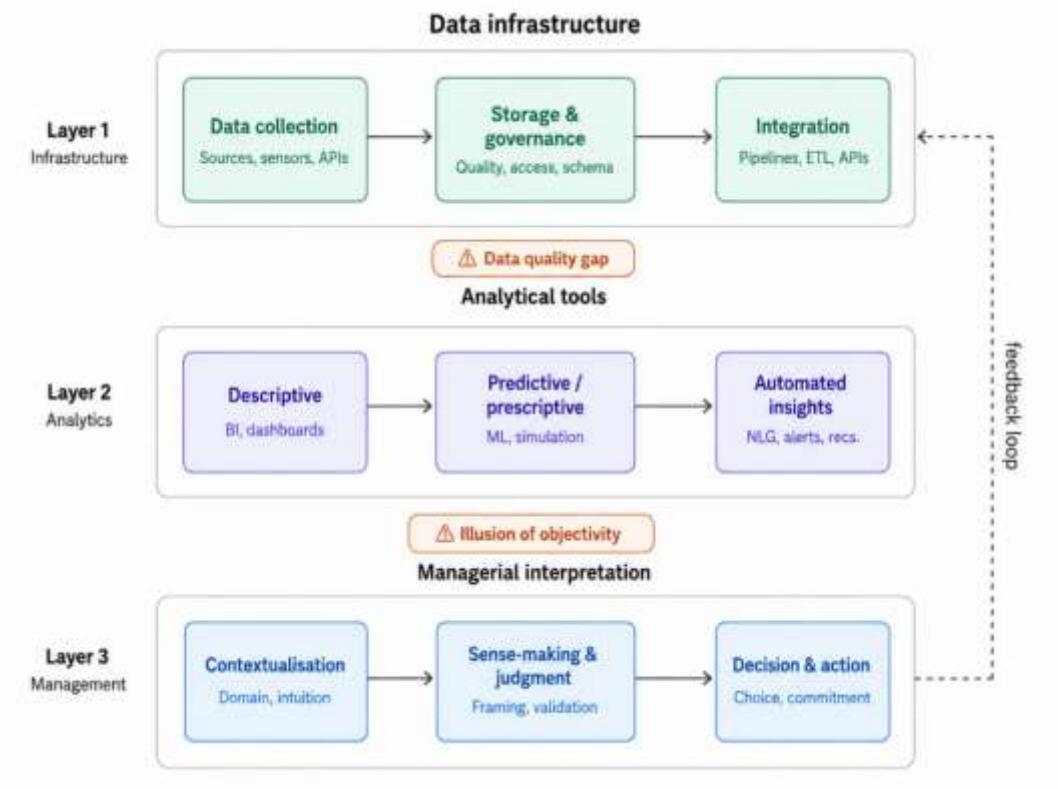


Figure 1. Three-Layer Process Model of Data-Driven Decision-Making in Digital Businesses
Source: *Authors' own elaboration.*

2. Layer 1 – Data infrastructure

The first layer encompasses data collection, storage and governance, and integration. Infrastructure quality (*Iq*) determines the epistemic foundation on which all subsequent layers rest. When this foundation is compromised - through biased sampling, inconsistent schemas, or silent ETL errors - analytical outputs inherit those flaws and carry them into the decision, often invisibly. Industry analysis of over 1,000 data pipelines suggests that 72% of quality issues are detected only after they have already influenced business decisions (Datachecks, 2024) - a figure that, while not from a peer-reviewed source, is consistent with the broader literature on data quality management, which

consistently identifies late detection as a primary characteristic of infrastructure-level failures (Vidgen, Shaw and Grant, 2017). The model identifies the transition from Layer 1 to Layer 2 as the first critical bottleneck: the data quality gap (Table 1). Unlike tool-level failures, infrastructure failures are structurally upstream and cannot be corrected by more sophisticated analytics downstream.

3. Layer 2 – Analytical tools

The second layer covers descriptive analytics (BI, dashboards), predictive and prescriptive models (machine learning, simulation), and automated insight generation (NLG, recommendation engines). Tool effectiveness (*T*e) is not a binary property but a function of fit-to-purpose: a well-calibrated predictive model is highly effective for a specific problem domain and misleading when applied outside it. Three failure modes are characteristic of this layer. Algorithmic bias is the most studied: when training data carries the imprints of historical inequities or measurement errors, the models built on it reproduce and often amplify those distortions, while presenting their outputs in a form that reads as neutral analysis (Engin and Treleaven, 2019). The self-reinforcing dynamic is well documented - biased outputs fed back as inputs accelerate rather than correct the problem (IBM, 2026). Less well studied but equally consequential is metric overload: as the number of active dashboards and KPI streams grows, managers face an environment in which the cognitive work of identifying meaningful signals from noise becomes the limiting constraint on decision quality, regardless of how good the underlying data is (Bakshy, Messing and Adamic, 2015). The third failure mode - what this paper calls the illusion of objectivity - is perhaps the most structurally dangerous: automated insight tools, particularly natural language generation systems, present inferences as facts. A recommendation phrased in declarative language carries a different epistemic weight than the same recommendation presented as a probabilistic estimate with stated assumptions, and that weight tends to suppress rather than invite the critical scrutiny that good judgment requires. This is the hinge point of the second critical bottleneck.

4. Layer 3 – Managerial interpretation

The third layer - contextualisation, sense-making and judgment, and decision and action - is where data-driven logic meets organisational reality. Managerial competence (*M*c) refers specifically to the capacity to receive analytical outputs critically, to supply contextual knowledge that tools cannot access, and to exercise sense-making: the retrospective construction of meaning from ambiguous signals (Weick, 1995). Research confirms that while data is omnipresent in contemporary management, data quality, utility, and value remain inconsistent, and satisficing behaviours persist even in the age of data-at-your-fingertips (Pittenger *et al*., 2023). This finding has a counterintuitive implication: data abundance does not eliminate bounded rationality (Simon, 1997); it reshapes it. Managers now satisfice not from lack of data but from inability to evaluate data critically under time pressure.

5. Bottleneck analysis and severity framework

Table 1 presents a systematic analysis of nine bottleneck and risk mechanisms across the three layers. Severity levels are assigned on the basis of four criteria: (1) impact on decision outcome - the degree to which the risk distorts the final decision; (2) probability of occurrence - how frequently the condition arises in digital business contexts, based on the reviewed literature; (3) detectability - the ease with which the risk can be identified before it reaches the decision; and (4) reversibility - whether the failure can be corrected without structural investment. This multi-criteria framing ensures that severity labels are grounded in explicitly stated logic rather than subjective judgment.

Table 1. Bottleneck and Risk Analysis Across the Three Layers of the DDDM Process Model

Layer	Stage	Bottleneck / risk	Mechanism	Severity criteria
L1	Data collection	Incomplete or biased sampling	Structural gaps propagate downstream and cannot be corrected at later stages	High impact; high probability; low detectability before decision
L1	Storage & governance	Inconsistent schema; poor data lineage	Integration failures reduce analytical reliability at source	High impact; medium probability; reversible only with governance investment
L1	Integration (ETL)	Latency; silent transformation errors	Stale or corrupted data reaches analytics layer undetected	Medium impact; medium probability; moderate detectability
L2	Descriptive analytics	Dashboard overload; metric proliferation	Cognitive load prevents meaningful signal extraction by managers	Medium impact; high probability in mature BI environments; partially reversible
L2	Predictive / prescriptive	Algorithmic bias; overfitting to historical patterns	Model outputs systematically misrepresent future states; bias reinforces over time	High impact; medium probability; low detectability without model audit
L2	Automated insights	Illusion of objectivity in NLG outputs	Framing effects suppress critical managerial evaluation of algorithmic outputs	High impact; high probability; accountability diffuses to algorithm
L3	Contextualisation	Automation bias; over-reliance on recommendations	Managerial judgment displaced rather than augmented by tool outputs	High impact; high probability; undermines strategic responsibility
L3	Sense-making & judgment	Satisficing under data abundance	Data availability does not eliminate bounded rationality under time pressure	Medium impact; high probability; partially reversible via training
L3	Decision & action	Accountability diffusion in algorithm-assisted choices	Unclear human–machine attribution weakens decision ownership and responsibility	Emerging impact; low probability currently; increasing as automation deepens

Source: *Authors' synthesis based on Pittenger et al. (2023); Engin and Treleaven (2019); Davenport and Harris (2017); Simon (1997); Bakshy, Messing and Adamic (2015).*

6. The Decision Quality function

The relationships identified in the preceding sections can be brought together in a single function that captures how the three layers jointly determine decision quality. The formulation is intended as a structural argument, not a measurement tool:

$$\mathbf{DQ = f(Iq, Te, Mc) - \Sigma Ri} \quad \mathbf{(1)}$$

In expanded form:

$$\mathbf{DQ = \alpha \cdot Iq \cdot Te \cdot Mc - \beta \cdot Rbias - \gamma \cdot Roverload - \delta \cdot Robj} \quad \mathbf{(2)}$$

Where *DQ* = Decision Quality; *I*q = Infrastructure quality (0-1); *T*e = Tool effectiveness (0-1); *M*c = Managerial competence (0-1); and *R*bias, *R*overload, *R*obj = conditional risk penalties activated when specific parameter thresholds are breached. The coefficients α, β, γ, and δ are treated as heuristic weights in the current version of the model - they reflect the relative order of magnitude of each component's contribution as inferred from the reviewed literature, but have not been empirically calibrated. Future research should operationalise these coefficients through expert scoring, Delphi consultation, or survey-based measurement across organisational contexts. This transparency is essential: the function's contribution at this stage is structural rather than quantitative, and any future empirical use would require sector-specific calibration.

The choice of a multiplicative rather than additive form is deliberate. Additive models imply that a strength in one area can offset a weakness in another; multiplication does not. A high-performing analytical layer cannot compensate for corrupted infrastructure, and skilled management cannot rescue insights built on biased models. The three factors are complements, and the function reflects that. Three organisational scenarios illustrate the practical significance of this claim. In the first scenario, an organisation with strong infrastructure and capable management deploys limited analytical tools: the binding constraint is *T*e, and DQ remains moderate regardless of the quality of the other two layers. In the second scenario, a digitally mature organisation invests heavily in predictive analytics but data governance is fragmented: even a high-performing analytical layer cannot recover what infrastructure corrupts upstream - the *R*bias penalty is structurally embedded (Davenport and Harris, 2017). In the third scenario, both infrastructure and tools are well-developed but managerial competence in interpreting outputs remains low: high *T*e combined with low *M*c activates the *R*obj penalty, as managers default to algorithmic recommendations as if they were objective facts. Across all three scenarios, the diagnostic implication is the same: improving DQ requires identifying the binding constraint and addressing it through coordinated investment across all three layers.

7. Managerial implications

A model that cannot be used is a model that has not done its job. The decision-logic gap is not visible in ROI metrics on technology investment: an organisation can spend heavily on a BI platform, report high system utilisation, and still be making worse decisions than before, because the binding constraint was never the tooling. Identifying where the real problem lies requires a different kind of audit - one that moves through the process layer by layer. The questions below are designed to support that audit.

For Layer 1 (Data infrastructure): Are data sources documented and their coverage gaps known? Is there a data governance policy that defines ownership, quality standards, and lineage? Are ETL pipeline errors logged and reviewed before analytical runs? A negative answer to any of these questions indicates that *I*q is likely the binding constraint, and that investment in analytical tools will yield limited returns until infrastructure is stabilised.

For Layer 2 (Analytical tools): Are predictive models tested for bias before deployment? Is the number of active dashboards and KPIs reviewed periodically for cognitive load? Are automated recommendations presented with confidence intervals or uncertainty ranges that preserve managerial judgment? Organisations that score poorly on these criteria face *T*e limitations combined with active *R*bias or *R*overload penalties.

For Layer 3 (Managerial interpretation): Do managers have formal training in data literacy and critical evaluation of algorithmic outputs? Are there institutional routines - devil's advocate processes, pre-mortems, or mandatory challenge periods - that require explicit justification before data-driven recommendations are adopted? Is decision accountability clearly assigned to a named individual rather than diffused to "the model"? Low scores here indicate that *M*c is the binding constraint, and that further investment in infrastructure or tools will not translate into improved decisions.

These three diagnostic clusters correspond directly to the bottleneck taxonomy in Table 1. The practical value of the model lies precisely in this mapping: by identifying which layer fails first, managers can prioritise interventions that address root causes rather than symptoms. An organisation that replaces its BI platform because dashboards are not trusted, when the real problem is poor data governance at Layer 1, will reproduce the same failure at a higher cost.

8. Key finding: the decision-logic gap

Running through each of the sections above is a single diagnostic observation, which this paper calls the decision-logic gap. Organisations invest in data tools with the goal of improving decisions, yet the logic connecting tools to decisions has typically not been made explicit. The gap emerges precisely because tool deployment is optimised for data availability and processing speed, while decision improvement depends on something different: the integration of analytical outputs with contextual judgment that only a manager can supply. Szukits and Móricz (2024) find empirically that developing an analytical culture and centralising data use does not automatically produce better decision-making - a result the model explains readily: centralisation strengthens the infrastructure and analytical layers, but cannot reach *Mc* deficiencies at Layer 3. The proposed model directly addresses this gap by making each transition point - and its associated risk - analytically visible, providing a framework that practitioners can apply without requiring proprietary data or specialised measurement instruments.

CONCLUSIONS

The problem this paper started from - that organisations invest heavily in data tools without achieving proportional improvements in decision quality - is not hard to observe, but it has proved difficult to explain precisely. The framework developed here offers one explanation: the gap is structural, and it appears at predictable points in the journey from data to decision. Two junctures stand out. At the transition from infrastructure to analytics, quality failures that accumulated upstream enter the analytical layer undetected, shaping outputs before any manager has a chance to intervene. At the transition from automated outputs to managerial judgment, the framing conventions of algorithmic tools tend to substitute for the critical interpretation they were supposed to support.

The most practically consequential finding concerns the nature of the relationship between the three layers. They are not independent levers. An organisation that treats infrastructure investment, analytical tooling, and management training as separate line items - to be addressed in sequence or traded off against each other - will not get the improvements it expects, because the three factors interact multiplicatively rather than additively. Neglecting data governance while upgrading analytical platforms, or deploying machine learning models while leaving managers without the training to challenge their outputs, reproduces the same structural failure at higher cost. This is a direct implication of the Decision Quality function, and it runs counter to the way digital transformation programmes typically present the problem.

The analysis of Layer 3 also pushes back against a quieter assumption embedded in much of the DDDM literature: that better tools eventually reduce the need for human judgment. The evidence reviewed here suggests the opposite. Managers satisfice not because they lack data but because they face predictable cognitive pressures that data abundance does not relieve (Pittenger *et al*., 2023; Simon, 1997). The model makes this concrete: the binding failure mode is not that managers ignore data, but that they face structurally predictable conditions - automation bias, objectivity illusion, accountability diffusion - at the point where analytical outputs enter their interpretive frames.

Perhaps the most useful thing about the decision-logic gap as a concept is that it is diagnosable. Identifying which layer is the binding constraint in a given organisation does not require proprietary data or specialised instrumentation - it requires a structured audit of the kind outlined in Section 4.7. That auditability is deliberate: the model is designed to be applied, not just cited.

The framework developed here comes with genuine constraints that future research will need to address. The model has not been tested against empirical data: the bottleneck taxonomy and

severity assignments rest on a reading of existing literature, not on primary observation, and may reflect the biases of that literature. The coefficients in the Decision Quality function are heuristic placeholders rather than calibrated estimates; they give the function structural meaning, but any quantitative application would require sector-specific calibration through expert elicitation or survey-based measurement. The model also treats digital businesses as a relatively homogeneous category, which they are not. The infrastructure challenges facing a data-native platform business are different in kind from those of a manufacturing firm mid-way through digital transition, and the model says nothing about how the bottlenecks distribute differently across operational, tactical, and strategic decision contexts - a distinction that matters. Similarly, resource constraints in smaller organisations are likely to affect Layer 1 and Layer 3 far more severely than they affect large corporations, yet the model does not capture this asymmetry. Resolving these gaps would require moving from conceptual framework to empirical programme: operationalising *I*q, *T*e, and *M*c as measurable indices that allow comparative analysis across organisational contexts. What the model contributes at this stage is a process logic precise enough to be tested - a starting point, not an end point.

REFERENCES

Ackoff, R.L., 1989. From data to wisdom. *Journal of Applied Systems Analysis*, 16, pp.3-9.

Bakshy, E., Messing, S. and Adamic, L.A., 2015. Exposure to ideologically diverse news and opinion on Facebook. *Science*, 348(6239), pp.1130–1132. https://doi.org/10.1126/science.aaa1160

Davenport, T.H. and Harris, J.G., 2017. *Competing on Analytics: The New Science of Winning*. Updated ed. Boston: Harvard Business Review Press.

Datachecks, 2024. *The State of Data Quality 2024: Analysis of 1000+ Data Pipelines*. [online] Available at: https://medium.com/datachecks [Accessed 28 May 2026].

Elgendy, N., Elragal, A. and Päivärinta, T., 2022. DECAS: a modern data-driven decision theory for big data and analytics. *Journal of Decision Systems*, 31(4), pp.337–373. https://doi.org/10.1080/12460125.2021.1894674

Engin, Z. and Treleaven, P., 2019. Algorithmic government: automating public services and supporting civil servants in using data science technologies. *The Computer Journal*, 62(3), pp.448–460. https://doi.org/10.1093/comjnl/bxy082

Grand View Research, 2025. *Data Analytics Market Size, Share & Trends Analysis Report*. [online] Available at: https://www.grandviewresearch.com [Accessed 28 May 2026].

IBM, 2026. *What Is Algorithmic Bias?*. [online] Available at: https://www.ibm.com/think/topics/algorithmic-bias [Accessed 28 May 2026].

IBM Institute for Business Value, 2025a. *The 2025 CDO Study: The AI Multiplier Effect*. New York: IBM Institute for Business Value (published 12 November 2025). Summary available at: https://www.ibm.com/think/insights/cost-of-poor-data-quality [Accessed 28 May 2026].

McAfee, A. and Brynjolfsson, E., 2012. Big data: the management revolution. *Harvard Business Review*, 90(10), pp.60–68.

Pittenger, L.M., Glassman, A.M., Mumbower, S., Merritt, D.M. and Bollenback, D., 2023. Bounded rationality: managerial decision-making and data. *Journal of Computer Information Systems*, 63(4), pp.890–903. https://doi.org/10.1080/08874417.2022.2111380

Precisely and Drexel LeBow College of Business, 2024. *2025 Outlook: Data Integrity Trends and Insights*. Philadelphia: Drexel University LeBow College of Business. Available at: https://www.lebow.drexel.edu/sites/default/files/2024-09/drexel-lebow-precisel-data-integrity-trends-insights-2025-outlook.pdf [Accessed 28 May 2026].

Rowley, J., 2007. The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science*, 33(2), pp.163–180. https://doi.org/10.1177/0165551506070706

Simon, H.A., 1997. *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization*. 4th ed. New York: The Free Press.

Szukits, Á. and Móricz, P., 2024. Towards data-driven decision making: the role of analytical culture and centralization efforts. *Review of Managerial Science*, 18(10), pp.2849–2887. https://doi.org/10.1007/s11846-023-00694-1

Vidgen, R., Shaw, S. and Grant, D.B., 2017. Management challenges in creating value from business analytics. *European Journal of Operational Research*, 261(2), pp.626–639. https://doi.org/10.1016/j.ejor.2017.02.023

Weick, K.E., 1995. *Sensemaking in Organizations*. Thousand Oaks, CA: SAGE Publications.

AI-ASSISTED DATA ANALYSIS: THE BALANCE BETWEEN AUTOMATION, ANALYTICAL CONTROL AND HUMAN DECISION IN THE EXCEL ECOSYSTEM

CZU: 004.89:[004.65+004.42]
DOI: https://doi.org/10.53486/tids2026.09

MARIA MORARU
Academy of Economic Studies of Moldova
e-mail: morarumaria924@gmail.com
ORCID ID: 0009-0008-2499-8588

VARVARA TAPCOV
Academy of Economic Studies of Moldova
e-mail: varvara.tapcov@gmail.com
ORCID ID: 0009-0005-1775-3740

Abstract: Data analysis assisted by artificial intelligence has led to the expansion of the use of digital tools, positioning Microsoft Excel as a central element in modern ecosystems of information processing, analysis and visualization. In the context of accelerated digital transformation, organizations manage increasing volumes of data, and the need to automate analytical processes becomes essential for increasing operational efficiency and supporting the decision-making process. The paper examines the integration of artificial intelligence into the Excel ecosystem, with a focus on the interaction between automation, analytical control and human decision.

The research methodology includes a case study on data transformation in the sales field, using Power Query and the M language, assisted by AI tools and conversational models based on artificial intelligence. The study highlights how AI can automatically generate M-code for data transformation, reducing the technical complexity and time required to process information. At the same time, the limitations of automatically generated solutions are analyzed, especially in situations where the data structure evolves and requires further adaptations.

The results obtained highlight the reduction of processing time, the increase of analytical flexibility and the improvement of the process of creating dynamic reports. At the same time, the research confirms the need for validation and human intervention to ensure the scalability, robustness and correctness of analytical solutions.

The conclusions emphasize the importance of maintaining a balance between the efficiency of automation and analytical rigor in the context of business decisions. The paper proposes a practical model of human–AI collaboration in data transformation using Power Query and highlights the relevance of digital skills in modern data analysis processes.

Keywords: Artificial Intelligence; M code, Power Query, Copilot, Excel, human-AI collaboration.

JEL Classification: C88, M15, D83, O33.

INTRODUCTION

In today's economic environment, fast and well-founded decisions are essential for a company's success. Organizations collect huge amounts of data: sales, inventory, employee performance, reports downloaded from other systems or programs, financial data. Effective management and interpretation of this information can generate significant competitive advantages.

In the context of accelerated digital transformation, effective interpretation of information and data analysis is becoming an essential skill for professionals. Microsoft Excel, extended by Power

Query and Power BI, provides a robust ecosystem for data manipulation and visualization. The emergence of artificial intelligence tools (such as Copilot or conversational models) introduces a new level of automation, reducing technical barriers and increasing productivity. This automation raises important questions regarding the control over the analytical process and the validity of the results. Thus, a balanced approach between the use of AI and human expertise is needed, because business context, nuance interpretation, and risk taking cannot be completely outsourced to machines (figure 1).

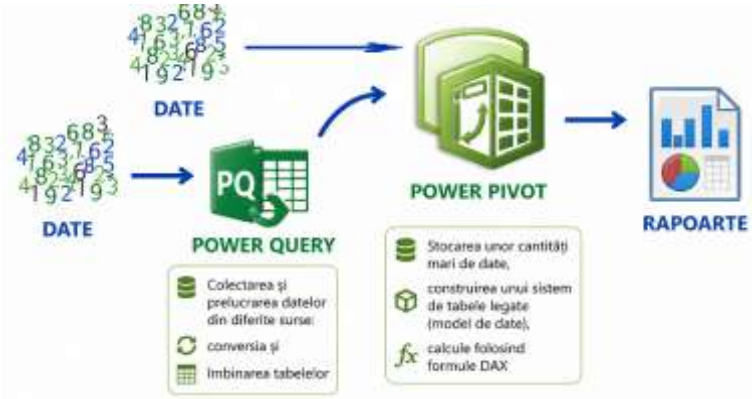


Figure 1. AI process flow in data analysis.
Source: *Authors' view.*

Excel, integrated with Power Query, Power Pivot, and Copilot, is a powerful ecosystem for AI-powered data analysis. With these tools, business professionals can:

- Import and consolidate data from multiple sources (Excel files, databases, cloud, OneDrive/SharePoint).
- Automate data transformation (standardization, elimination of duplicates, automatic calculation of KPI indicators).
- Generate dynamic reports that make it easy to monitor business performance.
- Get analysis and formula suggestions through Copilot, saving time and reducing manual errors.

MAIN CONTENT

The purpose of this article is to present the balance between automation, analytical control, and human decision-making, in the business context, highlighting both theoretical concepts and practical examples, with a focus on data security and integrity in the Excel ecosystem.

1. The role of artificial intelligence in data analysis in Excel

Artificial intelligence contributes significantly to:

- automatic generation of formulas and codes (including M-code for Power Query);
- identifying patterns and anomalies in data sets;
- automation of repetitive processes, report creation and decision making;
- assisting the user in building analytical models.

A major advantage is AI's ability to translate requirements formulated in natural language into concrete technical steps.

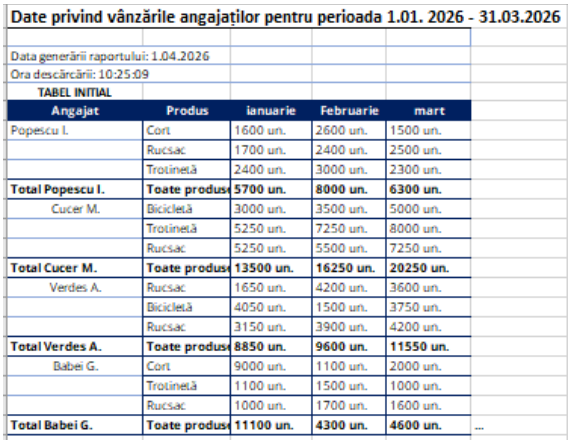
2. Power Query and M language – AI-assisted automation

Power Query is an essential tool for data processing in Excel. The M language allows you to define transformations in a declarative way.

By using AI, the process of writing M-code becomes much more accessible. Instead of manually constructing each step, the user can describe the desired result and the AI generates the script.

3. Automate repetitive processes, create reports and make decisions

The paper proposes a practical model of **human–AI collaboration** in data transformation using Power Query. The analyzed dataset, figure 2, is extracted from an Excel file from an external source and contains information about the sales made by employees of a company for a period of time. The data is presented in a hierarchical structure and has an unsuitable format (wide format) for analysis and reporting.



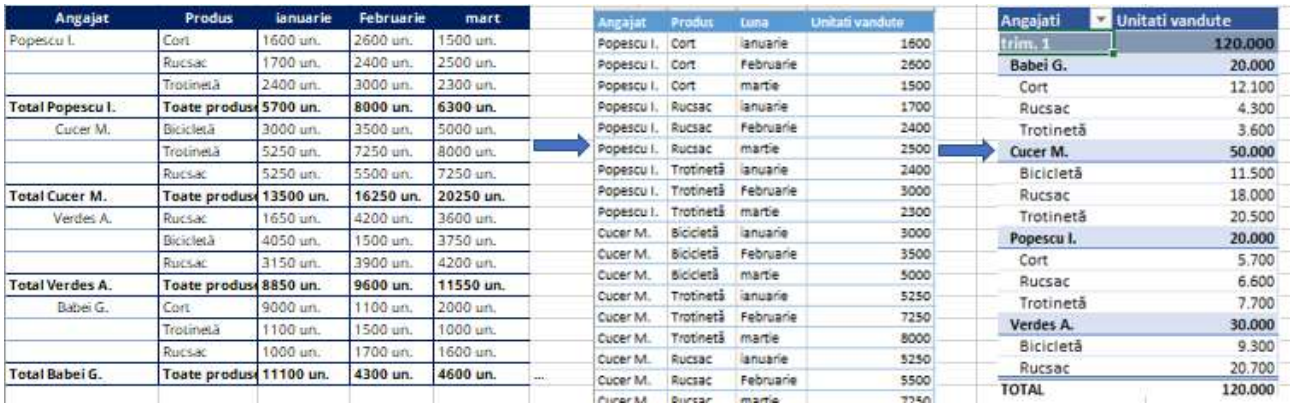
Date privind vânzările angajaților pentru perioada 1.01. 2026 - 31.03.2026

Data generării raportului: 1.04.2026
Ora descărcării: 10:25:09
TABEL INITIAL

Angajat	Produs	ianuarie	Februarie	mart
Popescu I.	Cort	1600 un.	2600 un.	1500 un.
	Rucsac	1700 un.	2400 un.	2500 un.
	Trotinetă	2400 un.	3000 un.	2300 un.
Total Popescu I.	**Toate produs**	**5700 un.**	**8000 un.**	**6300 un.**
Cucer M.	Bicicletă	3000 un.	3500 un.	5000 un.
	Trotinetă	5250 un.	7250 un.	8000 un.
	Rucsac	5250 un.	5500 un.	7250 un.
Total Cucer M.	**Toate produs**	**13500 un.**	**16250 un.**	**20250 un.**
Verdes A.	Rucsac	1650 un.	4200 un.	3600 un.
	Bicicletă	4050 un.	1500 un.	3750 un.
	Rucsac	3150 un.	3900 un.	4200 un.
Total Verdes A.	**Toate produs**	**8850 un.**	**9600 un.**	**11550 un.**
Babei G.	Cort	9000 un.	1100 un.	2000 un.
	Trotinetă	1100 un.	1500 un.	1000 un.
	Rucsac	1000 un.	1700 un.	1600 un.
Total Babei G.	**Toate produs**	**11100 un.**	**4300 un.**	**4600 un.**

Figure 2. Source table exported from the external system.
Source: *Data processed by the authors.*

Based on this table, it is necessary to answer the question: " *What total quantity of goods were sold in the first quarter and what are the sales indicators for the following periods of time (months, quarters, years)? The answer should be reported as in the image, figure 3"*



Angajat	Produs	ianuarie	Februarie	mart
Popescu I.	Cort	1600 un.	2600 un.	1500 un.
	Rucsac	1700 un.	2400 un.	2500 un.
	Trotinetă	2400 un.	3000 un.	2300 un.
Total Popescu I.	**Toate produs**	**5700 un.**	**8000 un.**	**6300 un.**
Cucer M.	Bicicletă	3000 un.	3500 un.	5000 un.
	Trotinetă	5250 un.	7250 un.	8000 un.
	Rucsac	5250 un.	5500 un.	7250 un.
Total Cucer M.	**Toate produs**	**13500 un.**	**16250 un.**	**20250 un.**
Verdes A.	Rucsac	1650 un.	4200 un.	3600 un.
	Bicicletă	4050 un.	1500 un.	3750 un.
	Rucsac	3150 un.	3900 un.	4200 un.
Total Verdes A.	**Toate produs**	**8850 un.**	**9600 un.**	**11550 un.**
Babei G.	Cort	9000 un.	1100 un.	2000 un.
	Trotinetă	1100 un.	1500 un.	1000 un.
	Rucsac	1000 un.	1700 un.	1600 un.
Total Babei G.	**Toate produs**	**11100 un.**	**4300 un.**	**4600 un.**

Angajat	Produs	Luna	Unitati vandute
Popescu I.	Cort	ianuarie	1600
Popescu I.	Cort	Februarie	2600
Popescu I.	Cort	martie	1500
Popescu I.	Rucsac	ianuarie	1700
Popescu I.	Rucsac	Februarie	2400
Popescu I.	Rucsac	martie	2500
Popescu I.	Trotinetă	ianuarie	2400
Popescu I.	Trotinetă	Februarie	3000
Popescu I.	Trotinetă	martie	2300
Cucer M.	Bicicletă	ianuarie	3000
Cucer M.	Bicicletă	Februarie	3500
Cucer M.	Bicicletă	martie	5000
Cucer M.	Trotinetă	ianuarie	5250
Cucer M.	Trotinetă	Februarie	7250
Cucer M.	Trotinetă	martie	8000
Cucer M.	Rucsac	ianuarie	5250
Cucer M.	Rucsac	Februarie	5500

Angajati	Unitati vandute
trim. 1	120.000
Babei G.	**20.000**
Cort	12.100
Rucsac	4.300
Trotinetă	3.600
Cucer M.	**50.000**
Bicicletă	11.500
Rucsac	18.000
Trotinetă	20.500
Popescu I.	**20.000**
Cort	5.700
Rucsac	6.600
Trotinetă	7.700
Verdes A.	**30.000**
Bicicletă	9.300
Rucsac	20.700
TOTAL	120.000

Figure 3. Table transformation.
Source: *Data processed by the authors.*

There are several methodological approaches, which require a knowledge base regarding the method that will be used to transform the hierarchical table:

- Power Query interface, which requires advanced knowledge of this tool
- Writing M code, which requires knowledge of the respective language with all the rules for writing functions distributed across objects
- Creating macros, which requires knowledge of the VBA language

- Using Artificial Intelligence to write M-code, which requires correct prompt writing

4. Using Artificial Intelligence to write M-code

The AI process flow in data analysis boils down to the algorithm: Prompt → AI → M-Code → Result → Human Validation

The text of the request (Prompt) for solving the problem in the case study is:

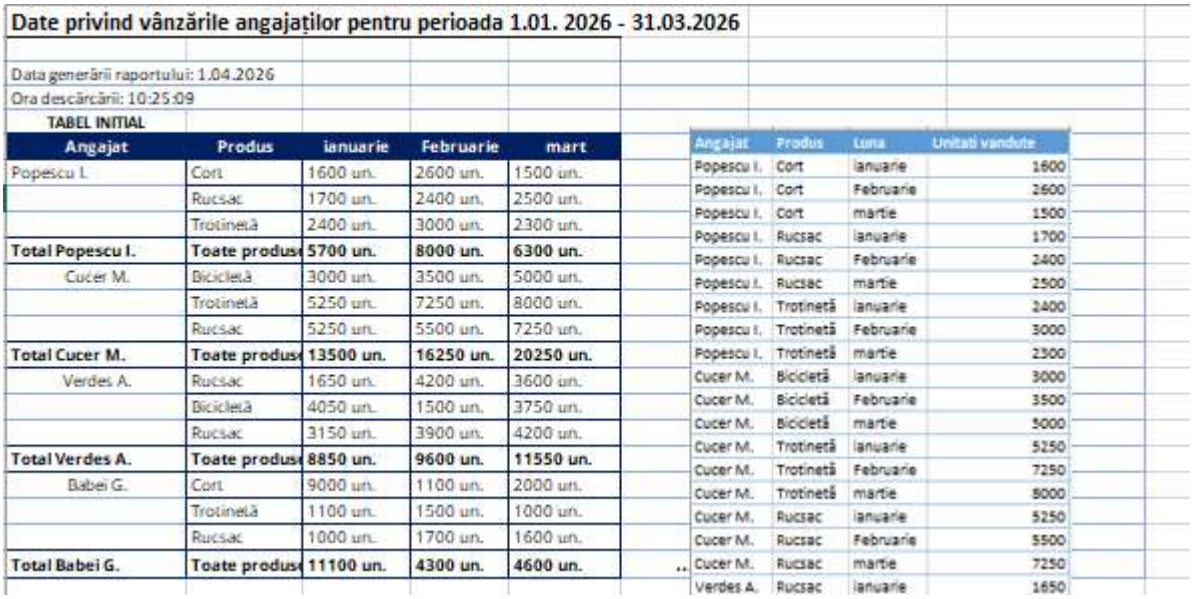
"Write an M code that imports and transforms a table from a hierarchical form to an analytical structure. My file is here: C:\Users\User\file_name.xlsx
Retrieve data from the sheet: [Sheet name: "Sales"].
I want to receive the table with the following structure: Employee, Product, Month, Period, Units sold, and the first row to contain, for example, the values: Popescu I, Cort, January, 01.01.2026, quarter 1, 1600
Code requirements:
Start the query by loading the file and sheet specified above.
It only uses standard functions, even those compatible with Excel 2016.
Avoid new, experimental, or rare functions (e.g. Expression.Evaluate).
Use actions that can be reproduced through the editor interface ("Fill → Down, "Replace, Transform, etc.).
If the logic is short and uses standard functions, embed it directly into the main query.
If the logic is complex, multi-step, or potentially reusable, extract it into a separate query function with a clear name (for example: fnFillDownGroups ".

The resulting AI-generated M-code, figure 4, transforms the case study table into an easy-to-analyze, "flat" format:

```
let
Source = Excel.CurrentWorkbook(){[Name="TabelSursa"]}[Content],
#"Removed Top Rows" = Table.Skip(Source, 4),
#"Promoted Headers" = Table.PromoteHeaders(#"Removed Top Rows", [PromoteAllScalars=true]),
#"Renamed Columns" = Table.RenameColumns(#"Promoted Headers",{
{"ianuarie", "Ianuarie"},
{"Februarie", "Februarie"},
{"mart", "Mart"}}),
#"Filtered Rows" = Table.SelectRows(#"Renamed Columns",
each not Text.StartsWith(Text.From([Angajat]), "Total")),
#"Filled Down" = Table.FillDown(#"Filtered Rows",{"Angajat"}),
#"Filtered Null Products" = Table.SelectRows(#"Filled Down",
each [Produs] <> null and [Produs] <> ""),
#"Unpivoted Columns" = Table.UnpivotOtherColumns(
#"Filtered Null Products",
{"Angajat", "Produs"},"Luna","Unitati_vandute"),
#"Removed Text" = Table.TransformColumns(
#"Unpivoted Columns",
{{"Unitati_vandute",
each Text.Replace(Text.From(_), "un.", ""), type text}}),
#"Trimmed Text" = Table.TransformColumns(#"Removed Text",
{{"Unitati_vandute", Text.Trim, type text}}),
#"Changed Type" = Table.TransformColumnTypes(
#"Trimmed Text",{{"Unitati_vandute", Int64.Type}})
in
#"Changed Type"
```

Figure 4. M-code for transforming the table structure.
Source: *Developed by the authors with AI support.*

This code demonstrates how AI can speed up the technical process, reducing complexity for the user. After implementing the code in the Power Query Editor, the result seems to be obtained, figure 5, but when adding new information, the results become inconsistent in certain scenarios.



Date privind vânzările angajaților pentru perioada 1.01. 2026 - 31.03.2026

Data generării raportului: 1.04.2026
Ora descărcării: 10:25:09

TABEL INITIAL

Angajat	Produs	ianuarie	Februarie	mart
Popescu I.	Cort	1600 un.	2600 un.	1500 un.
	Rucsac	1700 un.	2400 un.	2500 un.
	Trotinetă	2400 un.	3000 un.	2300 un.
Total Popescu I.	**Toate produs**	**5700 un.**	**8000 un.**	**6300 un.**
Cucer M.	Bicicletă	3000 un.	3500 un.	5000 un.
	Trotinetă	5250 un.	7250 un.	8000 un.
	Rucsac	5250 un.	5500 un.	7250 un.
Total Cucer M.	**Toate produs**	**13500 un.**	**16250 un.**	**20250 un.**
Verdes A.	Rucsac	1650 un.	4200 un.	3600 un.
	Bicicletă	4050 un.	1500 un.	3750 un.
	Rucsac	3150 un.	3900 un.	4200 un.
Total Verdes A.	**Toate produs**	**8850 un.**	**9600 un.**	**11550 un.**
Babei G.	Cort	9000 un.	1100 un.	2000 un.
	Trotinetă	1100 un.	1500 un.	1000 un.
	Rucsac	1000 un.	1700 un.	1600 un.
Total Babei G.	**Toate produs**	**11100 un.**	**4300 un.**	**4600 un.**

Angajat	Produs	Luna	Unitati vandute
Popescu I.	Cort	ianuarie	1600
Popescu I.	Cort	Februarie	2600
Popescu I.	Cort	martie	1500
Popescu I.	Rucsac	ianuarie	1700
Popescu I.	Rucsac	Februarie	2400
Popescu I.	Rucsac	martie	2500
Popescu I.	Trotinetă	ianuarie	2400
Popescu I.	Trotinetă	Februarie	3000
Popescu I.	Trotinetă	martie	2300
Cucer M.	Bicicletă	ianuarie	3000
Cucer M.	Bicicletă	Februarie	3500
Cucer M.	Bicicletă	martie	5000
Cucer M.	Trotinetă	ianuarie	5250
Cucer M.	Trotinetă	Februarie	7250
Cucer M.	Trotinetă	martie	8000
Cucer M.	Rucsac	ianuarie	5250
Cucer M.	Rucsac	Februarie	5500
Cucer M.	Rucsac	martie	7250
Verdes A.	Rucsac	ianuarie	1650

Figure 5. The result obtained after installing the code.

Source: *Data processed by the authors.*

Human intervention is necessary here to permanently resolve the problem.

5. Limitations of AI and the need for human intervention

AI-generated solutions may depend on the structure of the data, may require human adjustments and validation, and are not always generalizable.

A key issue observed in practice arises when the data structure evolves. For example, if a new column for the month "April" is added to the original table, the code initially generated by the AI may no longer work as expected and may require adjustments, figure 6.



Date privind vânzările angajaților pentru perioada 01.012026 - 30.04.2026

Data generării raportului: 1.05.2026
Ora descărcării: 10:25:09

TABEL INITIAL

Angajat	Produs	ianuarie	Februar	mart	Aprilie
Popescu I.	Cort	1600 un.	2600 un.	1500 un.	150000 un.
	Rucsac	1700 un.	2400 un.	2500 un.	250000 un.
	Trotinetă	2400 un.	3000 un.	2300 un.	2300 un.
Total Popescu I.	**Toate produs**	**5700 un.**	**8000 un.**	**6300 un.**	**6300 un.**
Cucer M.	Bicicletă	3000 un.	3500 un.	5000 un.	5000 un.
	Trotinetă	5250 un.	7250 un.	8000 un.	8000 un.
	Rucsac	5250 un.	5500 un.	7250 un.	7250 un.
Total Cucer M.	**Toate produs**	**13500 un.**	**16250 un.**	**20250 un.**	**20250 un.**

Angajat	Produs	Luna	Unitati vandute
Popescu I.	Cort	ianuarie	1600
Popescu I.	Cort	Februarie	2600
Popescu I.	Cort	martie	1500
Popescu I.	Rucsac	ianuarie	1700
Popescu I.	Rucsac	Februarie	2400
Popescu I.	Rucsac	martie	2500
Popescu I.	Trotinetă	ianuarie	2400
Popescu I.	Trotinetă	Februarie	3000

Figure 6. The result obtained after adding information.

Source: *Data processed by the authors.*

This highlights an important limitation: AI generates correct solutions for the current context, but not always generalized to future scenarios.

In this case, human expertise comes in, which must adapt the code to become flexible and reusable.

Improved M-code (dynamic and scalable)

To make the solution robust to adding new information (e.g. April, May, ... etc.) or even different years, the code must be adjusted to dynamically identify month columns. The human intervention consists of continuing the dialogue with the AI after detecting that when adding the month " April", the result does not adjust.

The next request to the AI is: *"Rewrite the code so that when adding new periods we automatically obtain the adjusted result for those periods."*

As a result of implementing the new AI-generated code, figure 7, the problem will be solved.

```
let
    Source = Excel.CurrentWorkbook(){[Name="Table1"]}[Content],
    #"Changed Type" = Table.TransformColumnTypes(Source,{{"Angajat", type text}, {
    #"Filtered Rows" = Table.SelectRows(#"Changed Type", each ([Angajat] <> "Total
    #"Filled Down" = Table.FillDown(#"Filtered Rows",{"Angajat"}),
    #"Unpivoted Other Columns" = Table.UnpivotOtherColumns(#"Filled Down", {"Angaj
    #"Replaced Value" = Table.ReplaceValue(#"Unpivoted Other Columns","mart","Mart
    #"Added Prefix" = Table.TransformColumns(#"Replaced Value", {{"Attribute", eac
    #"Added Suffix" = Table.TransformColumns(#"Added Prefix", {{"Attribute", each
    #"Changed Type1" = Table.TransformColumnTypes(#"Added Suffix",{{"Attribute", t
    #"Replaced Value1" = Table.ReplaceValue(#"Changed Type1","un.","",Replacer.Rep
    #"Changed Type2" = Table.TransformColumnTypes(#"Replaced Value1",{{"Value", In
    #"Renamed Columns" = Table.RenameColumns(#"Changed Type2",{{"Attribute", "Data
    #"Inserted Month Name" = Table.AddColumn(#"Renamed Columns", "Month Name", eac
    #"Reordered Columns" = Table.ReorderColumns(#"Inserted Month Name",{"Angajat",
    #"Inserted Quarter" = Table.AddColumn(#"Reordered Columns", "Quarter", each Da
    #"Reordered Columns1" = Table.ReorderColumns(#"Inserted Quarter",{"Angajat", "
    #"Added Custom" = Table.AddColumn(#"Reordered Columns1", "Tip Perioada", each
    #"Merged Columns" = Table.CombineColumns(Table.TransformColumnTypes(#"Added Cu
    #"Reordered Columns2" = Table.ReorderColumns(#"Merged Columns",{"Angajat", "Pr
    #"Renamed Columns1" = Table.RenameColumns(#"Reordered Columns2",{{"Month Name"
in
    #"Renamed Columns1"
```

Figure 7. New M-code for data transformation.
Source: *Developed by the authors with AI support.*

This version no longer depends on a fixed number of months and will work correctly even if new information with months, years, etc. is added, figure 8.

Angajat	Produs	Data	Luna	Perioada	Unitati vandute
Popescu I.	Cort	01.01.2026	ianuarie	trim 1	1600
Popescu I.	Cort	01.02.2026	februarie	trim 1	2600
Popescu I.	Cort	01.03.2026	martie	trim 1	1500
Popescu I.	Cort	01.04.2026	aprilie	trim 2	150000
Popescu I.	Rucsac	01.01.2026	ianuarie	trim 1	1700
Popescu I.	Rucsac	01.02.2026	februarie	trim 1	2400
Popescu I.	Rucsac	01.03.2026	martie	trim 1	2500
Popescu I.	Rucsac	01.04.2026	aprilie	trim 2	250000

Luni	Unitati vandute
ianuarie	39.150
februarie	38.150
martie	42.700
aprilie	438.700
TOTAL	558.700

Figure 8. Result obtained after modifying the M code.
Source: *Data processed by the authors.*

The difference between the two code variants clearly highlights the relationship between AI and user:

- AI offers a quick and functional solution **initially**;
- the user ensures generalization and robustness;
- the collaboration between the two leads to scalable solutions.

This example represents a concrete demonstration of the central idea addressed: the balance between automation (AI) and analytical control (OM), with the following benefits:

- reducing processing time;
- elimination of manual errors;
- scalability;
- easy integration into Power BI.

Although AI simplifies the technical process, analytical control remains essential. The final decision belongs to the user, who must validate the correctness of the transformations, the relevance

of the indicators and the coherence of the obtained results. Tools based on artificial intelligence can quickly generate formulas, M-code or analysis suggestions, but they do not automatically guarantee the contextual accuracy of the processed data.

In practice, the user becomes not only a consumer of the results generated by AI, but also a critical evaluator of them. Thus, analytical skills, professional experience and the ability to interpret information remain determining factors in the decision-making process. AI should be seen as a support mechanism for increasing productivity and automating repetitive operations, not as a complete substitute for human expertise.

In the context of the Microsoft Excel and Power Query ecosystem, AI and user collaboration contribute to the development of a modern data analysis model characterized by flexibility, speed and operational efficiency. At the same time, human validation reduces the risk of transformation errors, incorrect interpretations and erroneous analytical conclusions.

Integrating AI into Excel and Power Query is an important step in democratizing data analysis. The case study demonstrates the effectiveness of using AI to generate M-code and transform data into an analyzable format.

An additional relevant element is the ability to quickly build reports. For example, after transforming the data, an interactive report can be generated that shows the evolution of sales by months, years and products, facilitating the identification of trends, figure 9.

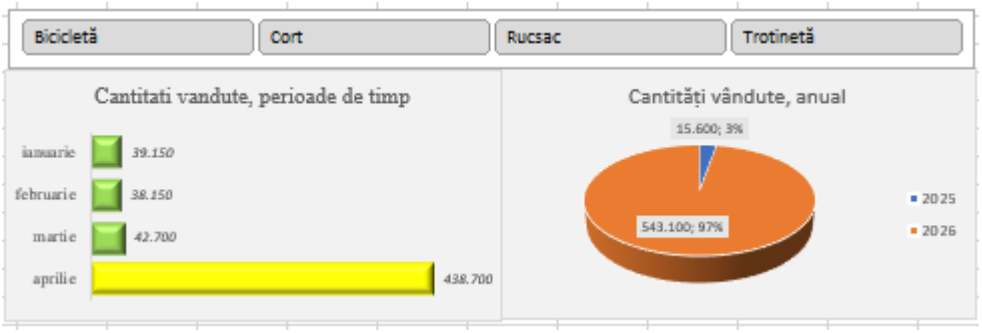


Figure 9. Adjustable ratio.
Source: *Data processed by the authors.*

The future belongs to human-AI collaboration, where automation accelerates processes and human expertise ensures the validity and relevance of decisions.

The main contribution of the paper consists in the practical demonstration of the limits of artificial intelligence-based automation in the data transformation process, as well as in highlighting the critical role of human intervention for the development of scalable, robust and adaptable analytical solutions to structural changes in data.

CONCLUSIONS

The research results demonstrate that integrating Artificial Intelligence tools into the Microsoft Excel and Power Query ecosystem significantly contributes to optimizing the transformation and analysis processes of commercial data. The case study conducted on a report exported from an external source highlighted that the use of AI-assisted generated M-code allows the automation of repetitive data processing steps, reducing the time required to transform the tabular structure and diminishing the risk of operational errors.

A relevant result of the research is the demonstration that AI models can accelerate the development process of ETL (Extract–Transform–Load) solutions, even in the case of unstructured

or partially standardized reports. The originality of the study derives from the combination of AI components with Power Query mechanisms to obtain a reusable and updatable analytical flow through Refresh operations. Thus, the research proposes a practical model of collaboration between the user and AI in the data analysis process, contributing to the development of the concept of augmented *analytics*.

The results confirm the conclusions of recent research on the role of AI in automating analytical processes and increasing business user productivity. However, the study also highlights an important conclusion that partially contrasts with some optimistic approaches in the specialized literature: AI does not eliminate the need for human validation. In the experiment conducted, some automatically generated transformations required manual adjustments to ensure semantic coherence and accuracy of the final results. This observation supports the idea that analytical expertise remains essential in the interpretation and validation of automatically processed data.

Another important result is highlighting the flexibility of Power Query in integrating data streams from heterogeneous external sources. The automatic transformation of a non-uniform report into a normalized tabular structure demonstrated the high potential of Microsoft tools for quickly building analytical models usable in Excel and Power BI.

However, the research has some limitations. The study was conducted on a small set of commercial data and a single tabular transformation scenario, without the integration of Big Data sources or advanced predictive AI models. Also, the performance of the solution may vary depending on the quality of the source data and the complexity of the imported structures.

Future research directions may include extending the proposed model by integrating Microsoft Copilot, Power Automate, and cloud services from the Microsoft 365 ecosystem. The possibilities of using AI for automatic anomaly detection, predictive generation of performance indicators, and development of intelligent reports in Power BI can also be analyzed. Another relevant direction is the assessment of the impact of AI on the digital skills of financial analysts and on the organizational decision-making process.

In conclusion, the research confirms that the combined use of AI, Excel and Power Query is an effective solution for the digital transformation of analytical processes. The benefits obtained are reflected in the increase in processing speed, the flexibility of data updates and the efficiency of reporting activities, but the success of the implementation still depends on the user's ability to critically validate and interpret the automatically generated results.

REFERENCES

Davenport, TH and Ronanki, R., 2018. *Artificial Intelligence for the Real World* . Harvard Business Review, 96(1), pp. 108–116.

Chen, H., Chiang, RHL and Storey, VC, 2012. *Business Intelligence and Analytics: From Big Data to Big Impact* . MIS Quarterly, 36(4), pp. 1165–1188.

Artificial Intelligence: A Modern Approach , Russell, S. and Norvig, P., 2021. *Artificial Intelligence: A Modern Approach* . 4th edition. Harlow: Pearson Education.

Microsoft Power Query Documentation , Microsoft, 2024. *Power Query Documentation*. Available at: Microsoft Learn [Accessed 24 May 2026].

Power Query M Formula Language Reference , Microsoft, 2024. *Power Query M Formula Language Reference* . Available at: Microsoft Learn [Accessed 24 May 2026].

Microsoft Power BI Documentation , Microsoft, 2024. *Power BI Documentation* . Available at: Microsoft Learn [Accessed 24 May 2026].

Data Science for Business , Provost, F. and Fawcett, T., 2013. *Data Science for Business* . Sebastopol: O'Reilly Media.

SUSTAINABILITY OF FREIGHT TRANSPORT COMPANIES IN THE CONTEXT OF INCOME AND EXPENSE INDICATOR ANALYSIS (BASED ON LOCAL COMPANY DATA)

CZU: 502.131.1:338.47(478)
DOI: https://doi.org/10.53486/tids2026.10

EUGENIU STOIAN
Assistant Professor, PhD candidate, Academy of Economics Studies of Moldova
e-mail: stoian@ase.md
ORCID ID: 0000-0002-8569-3584

SERGHEI PORTARESCU
PhD, Assoc. Prof., Academy of Economics Studies of Moldova
e-mail: portarescu@ase.md
ORCID ID: 0000-0001-5720-2488

ION NEGRU
PhD, Assoc. Prof., Academy of Economics Studies of Moldova
e-mail: negru.ion@ase.md
ORCID ID: 0000-0003-0055-7805

Abstract. Today's global economy requires transportation companies to be resilient and flexible. This article examines aspects of sustainability for Moldovan companies within macro-logistics supply chains. Macro-logistics chains are defined as a network of participants, including businesses and transportation companies. Their purpose is to minimize costs, but the existing infrastructure and approaches in the Republic of Moldova are outdated and need to be modernized. The main challenges include the country's limited transport capacity and poor coordination between participants. The development of this sector requires improvements in logistics infrastructure, including investments in warehouses and transport hubs. Based on the example of the company "PRIVAT-TRANS" S.R.L., the dynamics of assets and revenues in the period 2020-2024 are analyzed. The COVID-19 pandemic and rising fuel prices have led to a decline in profit margins, but 2024 has shown signs of recovery. This requires innovation and careful risk forecasting.

Keywords: sustainability, supply chain, macro-logistics chains, economic and financial analysis, international economics

JEL Classification: M1, M2, R4.

INTRODUCTION

The international economy offers vast opportunities to stimulate economic growth through international trade. However, weaknesses in the trade-supporting services sectors of many developing countries generate high transaction costs and a limited capacity to meet the transport and logistics requirements of an increasingly complex global economy, undermining the competitiveness of goods and, therefore, the ability of these countries to take advantage of opportunities offered by foreign markets.

In the era of globalisation of the world economy, in order to increase the competitiveness of industrial and agricultural enterprises, increase the potential of transit transport and expand the foreign trade of the Republic of Moldova, it has become relevant to design and develop macro-logistical supply chains used in the country's foreign economic activity. The Republic of Moldova chose the democratic path of development in 1991, moving from an administrative-communist system

to a market-oriented one. At the same time, foreign trade at that time was oriented towards the USSR and other socialist countries, but with the transition to a market economy, the Republic of Moldova's foreign economic activity expanded and required a new approach, including logistics, for integration into the global economy and international economic relations.

PRIVAT-TRANS S.R.L. is a privately owned company registered on February 27, 2006, whose main activity is international road freight transport. The company owns a fleet of 13 Volvo and 7 Scania vehicles. In addition, the company has 4 semi-trailers and 20 trailers of various models, used depending on the type of goods transported.

PRIVAT-TRANS S.R.L. is a commercial company specializing in road freight transport, offering regular routes to all European countries and shipping services to the countries of the Commonwealth of Independent States (CIS). Since its foundation, the company has evolved steadily, now offering integrated and customized logistics services that are tailored to the requirements and expectations of its customers in an efficient and professional manner.

RESEARCH METHODOLOGY

Logistics supply chains can be viewed as an extensive network of business partners who cooperate to achieve common goals, providing quality products and services at an optimal cost. These may include: supplier relationship management, inventory control, production planning and scheduling, product transportation and distribution, and customer relationship management. The objectives of supply chain management are to improve efficiency, reduce costs, increase customer satisfaction, and develop collaborative relationships with business partners. These objectives can be achieved through the use of modern technologies, such as information and communication systems, as well as through the implementation of efficient processes and appropriate supply chain management practices [4].

Logistics supply chains are sets of processes and activities that deal with the movement and management of materials and information necessary to produce and deliver a product or service to customers. The concept of logistics supply chain includes the following elements:

- Procurement and management of materials and products – involves identifying, selecting, and evaluating suppliers, establishing relationships with them, placing orders, and monitoring deliveries.
- Inventory management – refers to the management of stocks of materials and products to ensure their timely availability, minimize storage costs, and prevent the risk of excessive or inadequate stocks.
- Transportation and delivery – involves planning and managing the transportation of materials and products from suppliers to factories, distribution centers, and customers. It also includes managing storage, handling, loading, and unloading operations.
- Information and communications management – refers to the management and use of information and technology to coordinate and optimize activities within the supply chain. This includes the use of information systems and communication technologies to monitor and manage the flow of materials and information.
- Customer relationship management – involves managing customer relationships and expectations. It includes communicating with customers about the supply process and improving service to meet their needs and expectations [11].

RESULTS AND DISCUSSIONS

Financial analysis is necessary for all economic entities, primarily to determine their own financial strategy. As a rule, if an economic entity has free financial resources, then the question of their efficient use arises. Conversely, if there is a shortage of financial resources to carry out economic operations, then it is necessary to determine from which sources these resources will be allocated and how effectively they will be used. At the same time, in the process of the enterprise's economic activity, in a market economy, there is an increasing need to analyze the financial situation of its partners, as well as the economic agents with which it cooperates [20].

The economic and financial analysis of SC "PRIVAT-TRANS" S.R.L. is carried out on the basis of a set of analytical indicators. These are obtained as a result of combining, transforming, and processing the data used in the research, using means characteristic of economic activity. Like all economic indicators, analytical indicators represent concepts that reflect the volume, level, and efficiency of the economic process of both the entire economic activity of the enterprise and each component separately.

Table 1. Analysis of the size and development of the enterprise's assets for 2020-2024

Indicators	2020	2021	2022	2023	2024	Pace of growth, % (2024/2020)
Total assets, mln. lei	25,969	32,688	30,382	32,549	23,764	-73%
Sales revenues, mln. lei	36,689	39,058	54,738	46,060	46,723	1,014%

Source: *authors based on data provided by the company*

Between 2020 and 2024, the company's assets experienced significant fluctuations. Total assets declined markedly towards the end of the period, indicating a reduction in the asset base and a possible restriction of resources available for economic activity. In contrast, sales revenue showed a generally positive trend, with a notable overall increase, even though there were fluctuations at certain times. This divergence between the dynamics of assets and revenue suggests a more intensive use of existing resources and highlights the need to strengthen financial stability in order to ensure sustainable development.

Table 2. Assessment of efficiency of utilization of technical potential 2020-2024

Indicators	2020	2021	2022	2023	2024	Average growth rate
Value of fixed assets, mln. lei	14,204	18,71	12,147	16,084	12,254	-3,62
Income from sales, mln. lei	36,689	39,058	54,738	46,060	46,723	6,23
Yield, mln. lei (rd.2/rd.1)	2,58	2,09	4,50	2,86	3,81	10,24
Capacity, mln. lei (rd.1/rd.2)	0,39	0,48	0,22	0,34	0,26	-9,64

Source: *authors based on data provided by the company*

During the period 2020–2024, the efficiency of the use of the enterprise's technical potential showed both positive and negative trends. The value of fixed assets decreased from 14.204 million lei in 2020 to 12.254 million lei in 2024, representing an average reduction rate of −3.62% per year. Capacity followed a similar trend, decreasing from 0.39 million lei to 0.26 million lei, marking an average decline of −9.64%. In contrast, sales revenue increased from 36.689 million lei in 2020 to 46.723 million lei in 2024, at an average rate of +6.23%, and profitability rose from 2.58 million lei

to 3.81 million lei, recording the fastest growth of +10.24% per year. Thus, although the technical base has narrowed, economic performance and resource efficiency have shown visible growth, reflecting a more productive exploitation of existing potential.

Table 3. Profitability analysis of S.C. "PRIVAT-TRANS" S.R.L.

Indicators	2020	2021	2022	2023	2024	Absolute deviation	
						2024/2023	2023/2022
Sales revenue, mln. lei	36,689	39,058	54,738	46,060	46,723	0,66	-8,67
Gross profit, mln. lei	7,773	8,039	18,977	12,454	12,618	0,16	-6,52
Profit before tax, mln. lei	0,475	0,682	11,928	3,485	1,585	-1,90	-8,44
Net profit, mln. lei	0,102	0,427	10,480	2,783	0,616	-2,16	-7,69
Total assets, mln. lei	25,969	32,688	30,382	32,549	23,764	-8,78	2,16
Equity, mln. lei	4,719	4,719	4,719	4,719	4,719	0	0
Profitability of sales revenue, %/ (rd.2/rd.1)	0,28	1,09	19,15	6,04	1,32	-4,72	-13,10
Return on sales revenues, % (rd.3/rd.5)	0,39	1,31	34,49	8,55	2,59	-5,95	-25,94
Return on assets, % (rd.4/rd.6)	2,16	9,05	222,08	58,97	13,05	-45,92	-163,10

Source: *authors based on data provided by the company*

During the period 2020–2024, the profitability analysis of S.C. "PRIVAT-TRANS" S.R.L. highlights a complex financial situation, characterized by temporary increases followed by sharp declines. Sales revenues increased overall, but their dynamics were not accompanied by a constant maintenance of profitability. Thus, although 2022 brought a peak in both gross profit (18.977 million lei) and net profit (10.480 million lei), the following years saw drastic reductions, reaching only 0.616 million lei in net profit in 2024. Profitability indicators confirm this trend: return on revenue fell from 19.15% in 2022 to 1.32% in 2024, and return on assets declined from 34.49% to 2.59% over the same period. The strongest fluctuation is observed in financial profitability, which, after a record level of 222.08% in 2022, fell to only 13.05% in 2024. In conclusion, we can say that the company is facing a significant reduction in economic efficiency, which suggests a decline in its ability to capitalize on resources and increased financial vulnerability. In order to consolidate stability and revive profitability, it is necessary to optimize the cost structure, diversify revenues, and manage assets more efficiently.

Table 4. Analysis of economic stability of SC "PRIVAT-TRANS" S.R.L.

Indicators	2020	2021	2022	2023	2024	Absolute deviation %	
						2024//2023	2023/2022
Equity, mln. Lei	4,719	4,719	4,719	4,719	4,719	0	0
Long-term liabilities, mln. lei	4,703	14,046	9,945	14,664	10,229	-4,43	4,71
Short-term liabilities, mln. lei	6,777	6,778	7,042	8,599	6,784	-1,81	1,55
Total financing sources, mln. lei	14,487	11,863	13,395	9,285	6,751	-2,53	-4,10

Indicators	2020	2021	2022	2023	2024	Absolute deviation %	
						2024//2023	2023/2022
Financial autonomy ratio, lei (rd.1/rd.4)	0,291	0,185	0,217	0,169	0,217	0,04	-0,04
Financial stability ratio, lei (rd.1+rd.2)/rd.4	0,582	,0735	0,676	0,693	0,688	-0,005	0,001

Source: *prepared by the authors based on data provided by the company*

The analysis of the economic stability of S.C. "PRIVAT-TRANS" S.R.L. for the period 2020–2024 shows a development marked by fluctuations and imbalances. Equity remained constant, with no changes throughout the period, indicating rigidity in the consolidation of the internal financial base. In contrast, long-term debt has varied significantly, increasing in 2021 to 14.046 million lei, decreasing in 2022 to 9.945 million lei, and in 2024 falling again to 10.229 million lei, with a negative deviation of −4.43 million lei compared to the previous year. A similar trend was observed in short-term debt, which peaked at 8.599 million lei in 2023 but fell to 6.784 million lei in 2024 (−1.81 million lei). This volatility led to a decrease in total sources of financing, which fell from 16.199 million lei in 2020 to only 6.751 million lei in 2024, reflecting a substantial reduction in the capacity to sustain activity. Structural indicators confirm these trends: the financial autonomy rate remained low, fluctuating between 0.185 and 0.291, and returning to 0.217 in 2024. The financial stability ratio also declined slightly, from 0.693 in 2023 to 0.688 in 2024. Overall, the results indicate a marked dependence on attracted sources and instability in the structure of liabilities, which affects the company's financial soundness. To strengthen its economic stability, the company should aim to increase its equity capital, reduce its short-term debt, and shift toward more stable and sustainable sources of finance.

Predictability and consistency are fundamental elements of a competitive transport and logistics system. Trade support service providers need clear, accurate, reliable, and timely information on trade regulations in order to plan and make the necessary decisions regarding the movement of goods from one country to another. In many developing countries, such information on trade legislation, procedures, and documentation is not readily available to international shippers and carriers. This lack of information can have multiple effects:

- Poor explanation and dissemination of rules increase the likelihood of abuse by customs officials;
- Traders may face significant penalties, administrative appeals, or demands for bribes due to "mistakes" resulting from lack of knowledge;
- Delays in shipments and higher cargo detention costs may occur as shippers obtain adequate information and take steps to comply with unexpected documentation and procedures;
- Undisclosed changes to legal and regulatory frameworks expose operators to a high degree of liability, which is transferred to shippers, increasing transaction costs.
- Uncertainty about legal and regulatory structures can delay foreign investment in developing countries and make it more difficult to attract competitive service providers with world-class logistics know-how.

Although the additional costs caused by poor dissemination of regulatory information do not generally vary according to the value of goods or sales volume, they can increase the operating cost per unit. These costs disadvantage firms that have to bear the impact of these information gaps.

In general, macro-logistics supply chains represent a set of links (industrial enterprises, transport companies, storage complexes, repair enterprises, intermediary networks, commercial enterprises and organizations, service centers) concentrated within the borders of a particular state. As a distinctive feature of the macro-logistics chain compared to functional and micro-logistics chains, it should be noted that, in addition to minimizing logistics costs, it solves a number of problems related to the environmental, social, and economic directions of a particular state [19].

Macro-logistical supply chains, depending on their objective-functional characteristics, are divided into several groups:

- Production supply chains, which sell products for production purposes;
- Consumer supply chains, whose objects are consumer goods for various purposes;
- Inter-industry LLA, consisting of enterprises (links in the chain) from one or more branches of material production;
- Departmental and inter-agency LLA, in which economic entities (links in the chain) belong to one department (e.g., service LLA);
- Service LLA, whose links are enterprises and organizations that provide maintenance, preventive maintenance, minor and medium repairs of technical devices for various purposes;
- Service LLA in the packaging industry, which supplies the manufacturing, trade, storage, and transportation industries with packaging and packaging materials;
- Institutional LLA, which provides the necessary logistical resources to institutional structures [20, 21].

The main characteristics of macro-logistics supply chains should include:

– the multiplicity of participants in the movement of goods, acting as links in the chain;
– the significant length of the chain in terms of distance, depending on the geographical location and area of a particular state;
– different combinations of organizational structures formed autonomously in individual links, which require appropriate adaptation;
– specific areas of production and economic activities of participants in the chain, which require the development of common, standardized, and mutually beneficial approaches to ensure a viable process of goods circulation [8].

In the Republic of Moldova, due to its geographical position, the absence of navigable rivers, only two borders with neighboring countries, and its enclave character, three variants of macro-logistical supply chains have historically developed: internal land-based supply chains; international land-based supply chains for imported products; international land-based supply chains for exported products [5].

The macro-logistical domestic supply chains established to date are characterized primarily by the production and commercial activities of Moldovan enterprises, the results of which are products intended for domestic consumption by both industrial enterprises producing materials (manufactured goods) and individual consumers (consumer goods) [2].

The formation of internal macro-logistics chains for the supply of manufactured products and their operation has been and continues to be achieved through an order-based production method – depending on the sequence and timing of the construction of houses and buildings for various purposes, which makes it impossible to plan and predict the delivery time of products to consumers and the number of vehicles required. In addition, this method makes it difficult to organize and control

the movement of products in real time. The operation of internal macro-logistics supply chains - logistics of consumer goods is based on average statistical data on individual consumer demand for this type of product, which creates a number of difficulties in terms of changes in demand, volume of goods stocks, timing of order acceptance, and use of transport resources depending on quantity and transport capacity [10].

International macro-logistics supply chains for imported products are formed and operated by suppliers from different countries – over 19 exporting countries. Some of the manufactured products (machinery, construction materials and structures, petroleum products) are delivered using transit supply – directly to end consumers in the territorial entities. Some consumer products (foodstuffs, tobacco and cigarettes, alcoholic beverages, detergents), supplied simultaneously from several countries, are not regulated in terms of timing, nomenclature, and volumes.

This situation leads, firstly, to considerable additional time for sorting, packing, and shipping import consignments and, secondly, to increased logistics costs [17].

The formation and operation of international supply chains for export products is based, first, on the nomenclature and volume of export products and goods, which include non-ferrous metal ores, equipment, machinery, agricultural crops (industrial products), meat and meat products, leather and leather goods, cashmere, textiles (consumer goods). Secondly, the operation of this type of chain is carried out on a sectoral basis [13].

Supply chains for export products are formed along two lines – production and consumption, depending on the purpose of the products, which have different approaches to the formation of chains and the use of rail and road transport.

As regards the functioning of macro-logistics supply chains for consumer goods intended for export, these are organised on an autonomous-corporate basis and are characterised by a lack of coherence: there is no consolidation of cargo sent to an exporting country by several producers; the product circulation schedule is set without coordination with other export-producing companies; the volume of products loaded into vehicles does not take into account their transport capacity. All these aspects lead to significant losses in the movement of export products and to downtime in transport while waiting for the delivery of goods. Summarizing the various options for the operation of internal and international macro-logistics supply chains, we can construct their existing organizational and functional structural scheme, which includes warehouse and transit forms of supply, depending on the destination of the products and goods, as well as transport and storage facilities that serve the process of goods circulation [23].

Thus, based on the analysis of the functioning of macro-logistical supply chains for various types of international products, we can say that, given the modern development of logistics, efficient information systems, and technologies used in logistics functions, procedures, and operations, the established chains are morally and technologically outdated and do not meet the organizational and economic requirements imposed on them, which leads to operational inefficiency [22].

When building internal and international macro-logistical supply chains for a variety of products, the transport and storage systems operating in a given country are of paramount importance.

Therefore, an analysis of these systems is essential. First, let us analyze the transport system in the Republic of Moldova, which, for objective reasons (lack of access to the sea and navigable rivers), is limited in terms of modes of transport and uses only rail and road transport.

However, these types of chains are formed on the basis of accepted international standards and regulations, including customs procedures. At the same time, standards and regulations must be complied with in terms of product packaging and transport regulations.

Factors determining the high costs of road transport

Road transport has always been an important component of international trade, dominating the movement of goods to and from airports and seaports and representing a key mode of transport for trade between neighboring countries and landlocked countries. The continued growth of intermodal containerised transport has increased the importance of inland road transport as a means of providing a seamless link between ports and inland waterways and rail and road systems [14].

The road transport component of a commercial transaction can have a significant effect on the total transport costs of a commercial transaction. It is estimated that more than half of the door-to-door transit time and costs are spent on moving to and from the coastline for goods moving from the coast to inland locations. One study, for example, indicates that for coffee from Côte d'Ivoire, the added cost from producer to FOB port is nearly 170%; for cocoa beans, it is nearly 60%. These include:

- Domestic road transport conditions;
- Poor road conditions;
- Problems faced by landlocked countries [9].

The actual cost of delivery varies from location to location, ranging from a minimum of $80 in Egypt to a maximum of $215 in Vietnam. Some of the price differences can be explained by the distance traveled. The distance from the port of Haiphong to Hanoi is much greater than the local delivery distance in Egypt. In addition, Egypt's highly competitive road transport sector has contributed significantly to keeping local road transport costs low. The high cost of local delivery in the United States may be surprising given the competitive business environment, but strict environmental standards and safety requirements, plus high labor rates, contribute to higher transportation prices [6, 7].

CONCLUSIONS AND RECOMMENDATIONS

An analysis of the sustainability of transport companies in the Republic of Moldova has revealed significant challenges that hinder their development and integration into global supply chains. Outdated infrastructure and poor coordination between participants in logistics processes reduce competitiveness in international markets. At the same time, economic challenges such as rising fuel prices and the effects of the pandemic are accentuating the need for innovation. Key aspects of improving sustainability include the introduction of modern technologies such as logistics management systems and process digitization. These measures will help optimize inventory management, speed up data processing, and minimize human error. Operational automation also plays an important role in reducing costs and improving the overall efficiency of supply chains.

International supply chains, especially those related to exports and imports, require increased coordination. Clearer delivery schedules, stronger partnerships with foreign suppliers and consumers, and optimized transport routes are needed. These measures will reduce transport costs and time, making Moldovan companies more attractive to international partners. The role of the state in the development of the logistics sector is particularly important. Fiscal incentives, subsidies, and investments in infrastructure modernization are needed to support this sector. Improving the road network, building modern warehouses, and optimizing transport hubs are essential tasks for

increasing the efficiency of logistics processes. Thus, strengthening the resilience of transport companies in the Republic of Moldova requires an integrated approach, including infrastructure modernization, innovation implementation, and active state support. These actions will enable Moldovan companies to strengthen their positions in international markets and ensure the stable development of the national logistics sector.

REFERENCES

1. Albekov, A. U. Logistică / A. U. Albekov, H. Yu. Eldarkhanov. // - Rostov n/a. : Rostov. Universitatea Economică de Stat "RINH", 2009. - 338 p.
2. Amirov, M. Sh., Amirov, S. M. Sistemul unificat de transport: manual / M. Sh. Amirov, S. M. Amirov // - ediția a 2-a, - M. : Knorus, 2017. - 184 p.
3. Amosova V. V. Teoria economică : manual / V. V. V. Amosova, G. M. Gukasian, G. A. Mahovikova. - Moscova : Expo, 2011. - 733 p.
4. Anikin B. A. Logistică: manual / / / editat de B. A. Anikin și T. A. Rodkina // - M. : Prospect, 2008. - 406 p.
5. Anikin B. A. Logistica și managementul lanțului de aprovizionare. Teorie și practică. Subsistemele funcționale de bază și de sprijin ale logisticii / B. A. Anikin // - M. : Prospect, 2013. - 608 p.
6. Anikin B. A. Logistica și managementul lanțului de aprovizionare. Teorie și practică. Fundamentele logisticii: manual / ed. de B. Anikin și T. Rodkina. - Moscova : Prospect, 2013. - 344 p.
7. Analiza și diagnoza activității economico-financiare a întreprinderii: manual / ed. prof. V.Ya. - M. : NITS INFRA - M, 2014. - 617 p.
8. Anikin B. A. Logistică : manual; / editat de B. A. Anikin și T. A. Rodkina // - M. : Prospect, 2008. - 406 p.
9. Barinov V.A. Proiectarea organizațională: Manual /// V.A. Barinov / ed.: Ed. I. Vidyapin.- M. : INFRA - M, 2018. - 384 p.66
10. Bochkareva, A. A. A. Planificarea și modelarea lanțului de aprovizionare / A. A. A. Bochkareva. - M. : Alpha - Press, 2008. - 192 p.
11. Brodetsky, G. L. Modelarea sistemelor logistice. Decizii optime în condiții de risc / G. L. Brodetsky. - M. : Vershina, 2006. - 376 p.
12. Bowersox, Donald J., Kloss David J. Logistica : un lanț de aprovizionare integrat. ed. a 2-a / tradusă din limba engleză - M. : ZAO Olympus - Business, 2006. - 640 p
13. Camera de Comerț Internațională a Rusiei ICC, INCOTERMS - 2010 [Resursă electronică] Mod de acces: http://www.incoterms.iccwbo.ru/
14. COMERȚUL EXTERIOR AL REPUBLICII MOLDOVA: REALIZĂRI ŞI PROBLEME Andrei Blaisovschi, doctor în științe economice, conferențiar universitar. Academia de Administrare Publică, 2008.
15. Gadzhinskiy, A. M. Logistică : manual pentru studenții din învățământul superior / A. M. Gadzhinskiy. / / - ediția a 12-a, revizuită. și suplimentară. - M. : "Dashkov și K0", 2006. - 432 p.
16. Johnson, James, Wood, Donald, F., Wardlow, Daniel, L., Murphy, Jr., Paul, R. Logistică modernă, ediția a 7-a: tradusă din limba engleză / D. Johnson, D. Wood, D. Wardlow, D. Murphy Jr. - M. : Williams Publishing House, 2002. - 624 p.
17. Lysons, K., Gillingham M. Achiziții și managementul lanțului de aprovizionare: trad. Din limba engleză / K. Lysons, M. Gillingham. - M.: INFRA - M, 2005. - 795 p.
18. Nerush, J. M. Logistică: manual / J. M. Nerush // ed. a 4-a. revizuită și suplimentară - M. : N54 Prospect, 2011. - 520 p.
19. Razer, S. M., Rodnikov A. N. Logistică: Dicționar de termeni / S. M. Razer, A. N. Rodnikov // - M. : VINITI RAS, 2007. - 412 p.
20. Semenenko A. I., Sergeyev V. I. Logistică. Fundamentele teoriei : manual / A. I. Semenenko, A. I. Semenenko, V. I. Sergheev. - SPb. : Uniunea, 2001. - 542 p.
21. Țîriulnicova N. „Analiza rapoartelor financiare”, Chișinău, ASEM, 2004.

CHALLENGES FOR YOUTH POLICIES IN THE DIGITAL ENVIRONMENT USING ARTIFICIAL INTELLIGENCE TOOLS

CZU: 37.014-053.6:004.8
DOI: https://doi.org/10.53486/tids2026.11

MONIKA YANAKIEVA
D. A. Tsenov Academy of Economics, Department of Finance and Credit, Bulgaria
e-mail: myanakieva0@gmail.com
ORCID ID: 0009-0003-0490-6598

Abstract. The question of whether artificial intelligence can transform the way the state conducts policies for young people is both a theoretical challenge and a managerial necessity. This report explores this duality from the perspective of a line ministry tasked with designing, financing and evaluating youth programmes. The analysis combines a conceptual overview of the European regulatory framework with a critical reading of empirical experience, including the Scandinavian decisions to partially abandon digitalization in education and return to paper books. The report argues that AI brings real potential in three directions: early identification of vulnerable youth groups through predictive analytics, personalization of services and optimization of employment and mobility programmes. However, serious risks are emerging, expressed in algorithmic bias, digital exclusion, erosion of privacy and cognitive consequences of over-digitalization. The Scandinavian experience with its example and positive consequences, especially Sweden's decision to return to paper textbooks after declining reading scores, serves as a warning that technological enthusiasm cannot replace the evidence base. The conclusion is that the responsible application of AI in youth policies requires not only technical competences, but also institutional maturity: a clear legal framework in line with the EU AI Act, mechanisms for the participation of young people themselves in the design of systems, and a willingness to abandon a given solution when empirical data requires it.

Keywords: artificial intelligence, youth policies, algorithmic governance, digitalization of education, EU AI Act

JEL Classification: I28, O38, J18.

INTRODUCTION

The digital transformation of public administration is no longer a horizon, but a present, posing questions to line ministries for which neither theory nor practice have ready-made answers. Youth policies are a particularly sensitive arena for these questions, because their addressees, such as young people between 15 and 29 years old, are both digital carriers and a vulnerable group whose life trajectories depend on the quality of institutional interventions. This report poses the following central research question: how can a ministry responsible for youth policies use artificial intelligence tools in a way that expands the opportunities of young people, without deepening inequalities or violating their rights? The question is normative, but its answer requires a deep understanding of technological reality. Methodologically, the report relies on three types of sources. First, academic literature in the fields of algorithmic governance (Danaher, 2016; Yeung, 2017), digitalization of education (Mangen et al., 2013; Mangen et al., 2019; Luckin et al., 2016) and youth policies. Second, policy documents of the European Union, including the EU AI Act (European Commission, 2021) and the Council of Europe framework (Council of Europe, 2020). Third, documented national experiences of Scandinavian and Western European countries, including cases of failure of AI systems (Eubanks, 2018; Richardson et al., 2019).

MAIN CONTENT

1. Theoretical overview

1.1. Youth policies in a European context

The concept of "youth policies" is not monolithic. In the European tradition, developed and substantiated in the documents of the Council of Europe and the EU, it covers a wide range of interventions. Among them are the promotion of volunteering, non-formal education, management of transitions to the labour market, as well as the prevention of social exclusion. The EU Youth Strategy 2019–2027 organizes these interventions around three priorities, expressed in actions on engagement, connection and empowerment. As a result, the participation of young people themselves is placed categorically and unconditionally at the focus of policy development (Council of Europe, 2020).

It is important to note that the strategy precedes the massive penetration of generative AI in the public sector. This means that its basic principles of shared governance, evidence-based, as well as inclusion need to be rethought in the light of technological changes, and not simply mechanically applied.

1.2. Algorithmic governance – theories and criticisms

The concept of "algorithmic governance" describes the process by which automated systems take over tasks traditionally performed by humans. Among these tasks we can include classification, profiling, resource allocation, etc. related. John Danaher distinguishes between two models: algorithms as decision-making tools and algorithms as subjects replacing institutional judgment (Danaher, 2016, p. 246). It is the second model that raises the most serious democratic concerns, not because algorithms are necessarily worse than humans, but because they shift responsibility to an opaque system. Karen Yeung introduced the concept of "hypernudging" and defined it as a process in which AI systems do not simply offer options, but structure the environment in a way that makes certain choices practically inevitable (Yeung, 2017, p. 119). In the context of youth policies, this may mean that an algorithm designed to guide young people to appropriate programmes actually limits their real options to predefined frames and corridors for cultivating targeted behaviour. The risks of algorithmic discrimination are further analysed by Zuiderveen Borgesius (2018) in a special report for the Council of Europe.

1.3. A critical review of the digitalisation of education

The issue of digitalisation in education is perhaps the best documented and at the same time the most controversial in the current context. Meta-analyses published since the pandemic period show a mixed picture: while digital tools can increase motivation and access, they do not demonstrate consistent benefits for reading and understanding text in the necessary analytical depth. The work of Anne Mangen and her colleagues on the neurocognitive differences between reading on a screen and reading on paper is particularly revealing: reading on paper promotes longer attention spans, better retention of details, and better navigation of linear narratives (Mangen et al., 2013, p. 65). A subsequent study comparing reading on a book and a Kindle confirmed that readers of paper books showed significantly better results on measures related to the chronology and temporality of the text (Mangen et al., 2019). These findings are not abstract, as they have direct relevance to the debate about digital education that is raging in Scandinavia. The application of AI in an educational context has also been analyzed by Luckin et al. (2016), whose report outlines the real potential of intelligent learning systems. In the educational and scientific degree of the doctorate, findings of a similar nature

are the need to introduce regulation at institutional, national and international levels, which would define the frameworks for the ethical use of AI by young scientists in their research (Zahariev, 2026a).

1.4. The EU regulatory framework

The European Regulation on Artificial Intelligence (EU AI Act), adopted by the European Parliament and the Council of the EU (European Commission, 2021), introduces a risk hierarchy that is directly relevant to line ministries. Systems used for assessing students, managing access to education and social benefits, or profiling vulnerable individuals fall into the "high risk" category. This means mandatory compliance with requirements for transparency, auditing, human oversight and documentation. These are requirements for which most national administrations do not yet have the necessary capacity to implement.

2. The possibilities of AI for implementing youth policies

When talking about AI in the public sector, it is easy to remain at the level of general promises. The task of this section is more demanding and it focuses on identifying specific applications with proven or plausible effects in the field of youth policies. Perhaps the most relevant application is analytics for early identification of so-called NEET youth (Not in Education, Employment, or Training), or those youth who are not in education, employment or training. The Finnish Employment and Economic Development Service (TE Services) uses machine learning to predict which young people are at risk of entering long-term unemployment and to offer targeted support before this happens. Similar systems operate in Austria and Denmark, with results showing a more efficient allocation of consultants' resources compared to the traditional cash approach.

The personalisation of services is a second direction with real potential. Recommendation systems trained on young people's profiles can offer appropriate mobility, volunteering or training programmes in a way that is incomparably more precise than a static catalogue. The Estonian digital infrastructure X-Road, while not specifically targeting young people, demonstrates how integrating data from different state registers can eliminate administrative barriers and make services truly proactive. Hartong and Förschler (2019) analyse how data in education management functions as infrastructures of power, which raises further questions about the way such systems are designed and managed.

Last but not least, AI can support the line ministry itself as an organisation in carrying out certain actions requiring digital capacity. This includes data analysis on programme effectiveness, identifying regional imbalances in access to youth services and scenario modelling in the allocation of limited funding resources.

3. The dangers and critical European experience

The history of technological optimism in public policy is littered with warnings that were ignored until failure became apparent. In the case of AI and youth policies, we have the privilege and responsibility to learn from others' mistakes before repeating them. Perhaps the most immediate risk is digital inequality. When public services migrate to digital platforms, access to them is determined not only by the law but also by the availability of devices, internet and digital skills. For a ministry striving for social inclusion, introducing AI-based services without parallel analogue alternatives is not just a technical oversight but a political mistake. This argument is particularly well developed and defended by Eubanks (2018) in her analysis of automated social policy systems in the US. Algorithmic bias is more complex because it is more difficult to see. The Dutch case of the SyRI (Systeem Risico Indicatie) system is illustrative. Thus, a system originally designed to identify

welfare recipients de facto profiles poor neighbourhoods and ethnic minorities disproportionately, leading to flawed subsequent policies and a relevant disproportionate allocation of resources. The risks of such systems are theoretically substantiated by Zuiderveen Borgesius (2018) and empirically supported by Richardson *et al.* (2019), whose analysis of "dirty data" in predictive analytics for police patrols shows how historical biases are encoded in algorithms claiming objectivity. Data protection is a third, formally regulated but practically complex area. The GDPR provides special protection for data of persons under 16 years of age, and the processing of sensitive categories of data requires an explicit legal basis. These sensitive data include data on health, social origin and ethnicity. In reality, many AI systems in the public sector are trained on aggregated administrative data. The question of whether and to what extent this processing is lawful in each specific case remains open.

Perhaps the most eloquent warning about the risks of hasty digitalization comes from countries considered leaders in this field. Scandinavia, and in particular Sweden, has conducted a large-scale natural experiment with consequences that go beyond educational policy. In the early 2010s, Sweden invested significantly in the digital transformation of classrooms. As a result, the country is a leader in providing students with tablets instead of textbooks, and classrooms are becoming spaces saturated with interactive whiteboards and access to online learning platforms. The reality revealed by the results in PIRLS 2021 (Skolverket, 2023) expressed in the international study of reading comprehension of fourth-graders is different. Sweden has registered a significant decline in results, unlike Finnish students, whose education system is more conservative in terms of digitalization.

Research by Mangen *et al.* (2013; 2019) provides a neurocognitive basis for understanding these results: reading on paper promotes deeper comprehension, especially with linear texts and when reconstructing chronology. The Swedish Agency for Education (Skolverket, 2023) has published reports linking the decline to the reduced use of paper materials. This has led to a correction in the initial policy for classroom digitization – Sweden is introducing mandatory paper textbooks in primary education from 2023. The lesson from the Scandinavian experience, however, is not that digitalization is wrong. It is that digitalization without a sufficient evidence base is risky, even when carried out by well-intentioned and well-resourced governments.

4. Framework for action at the ministry level

The insights and examples from the previous sections should lead to concrete management conclusions. In this section, we propose a framework that is not a technical manual, but rather a set of principles and institutional conditions.

The first and most fundamental condition is regulatory compliance with the EU AI Act (European Commission, 2021). Ministries working with vulnerable groups, among which we place young people, should assume that any system that profiles, assesses or refers young people falls into the “high risk” category. This means a mandatory ex ante risk assessment before implementation, registration in the European database for AI systems and a permanent mechanism for in medias monitoring.

The second condition is the systematic involvement of young people in the design of the systems. The EU Youth Strategy explicitly calls for shared management (co-management), but in the context of AI this takes on an additional dimension. The Council of Europe (2020) provides a framework for youth participation that can be adapted to the digital context.

The third condition is the willingness to abandon a technological solution when the evidence requires it. The Scandinavian experience shows that even politically committed and well-funded governments can make mistakes when implementing digital tools (Skolverket, 2023). Data from

monitoring education systems should serve as a real correction mechanism, not just for accountability, which is confirmed in the results of the analysis by Hartong and Förschler (2019). Finally, any AI-based solution should be introduced with a parallel analogue alternative. Not because analogue is better, but because digital exclusion is a reality, a process that has been extensively documented by Eubanks (2018).

CONCLUSIONS

Artificial intelligence is not a neutral tool. It carries within it the values of the data on which it is trained, the goals set by its designers, and the institutional context in which it is implemented (Danaher, 2016; Yeung, 2017). For the line ministry responsible for youth policy, this means that the question is not "whether to use AI", but "under what conditions and with what responsibility". This report argues that these conditions are achievable, but require consistent institutional work. Predictive analytics to identify vulnerable youth, personalize services, and optimize programs are real possibilities (Luckin et al., 2016)—but only if they are accompanied by transparency, audit, and participatory mechanisms. The Scandinavian experience with the digital transformation of education (Skolverket, 2023; Mangen et al., 2013; 2019) is not an argument against technology, but an argument for an evidence-based approach.

Specific recommendations follow. The ministry should carry out an inventory of all AI or algorithmic systems currently used in the field of youth policy and assess them against the criteria of the EU AI Act (European Commission, 2021). Where systems fall into the "high risk" category, a compliance assessment should be carried out immediately. The risks of discrimination analysed by Zuiderveen Borgesius (2018) and Richardson et al. (2019) should serve as a guide for this assessment.

Last but not least, the ministry should lead a national dialogue on digital education, analogous to the Scandinavian one. The question of the balance between paper and digital learning, of screen time in educational environments, and of the cognitive consequences of over-digitalization deserves an open political debate, driven by data, not by technological enthusiasm or conservative reflex.

REFERENCES

Council of Europe. (2020). Youth policy in Europe: Country information. Council of Europe. Available at: https://www.coe.int/en/web/youth/youth-policies [Accessed 25.04.2026].

Danaher, J. (2016). The threat of algocracy: Reality, resistance and accommodation. Philosophy & Technology, 29(3), pp. 245–268. https://doi.org/10.1007/s13347-015-0211-1

Eubanks, V. (2018). Automating inequality: How high-tech tools profile, police, and punish the poor. St. Martin's Press. [ISBN: 978-1250074317]

European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). COM/2021/206 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 [Accessed 25.04.2026].

Hartong, S. and Förschler, A. (2019). Opening the black box of data-based school monitoring: Data infrastructures, flows and practices in state education agencies. Big Data & Society, 6(1), pp. 1–12. https://doi.org/10.1177/2053951719853311

Luckin, R., Holmes, W., Griffiths, M. and Forcier, L. B. (2016). Intelligence unleashed: An argument for AI in education. Pearson. Available at: https://edu.google.com/pdfs/Intelligence-Unleashed-Publication.pdf [Accessed 25.04.2026].

Mangen, A., Olivier, G. and Velay, J. L. (2019). Comparing comprehension of a long text read in print book and on Kindle: Where in the text and when in the story? Frontiers in Psychology, 10, p. 38. https://doi.org/10.3389/fpsyg.2019.00038

Mangen, A., Walgermo, B. R. and Brønnick, K. (2013). Reading linear texts on paper versus computer screen: Effects on reading comprehension. International Journal of Educational Research, 58, pp. 61–68. https://doi.org/10.1016/j.ijer.2012.12.002

Richardson, R., Schultz, J. M. and Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. NYU Law Review Online, 94, p. 192. https://doi.org/10.2139/ssrn.3333423

Skolverket [Swedish National Agency for Education]. (2023). PIRLS 2021: Läsförmågan hos svenska elever i årskurs 4 i ett internationellt perspektiv [Reading ability among Swedish students in Year 4 in an international perspective]. Skolverket. Available at: https://www.skolverket.se/sok-publikationer/publikationsserier/rapporter/2023/pirls-2021 [Accessed 25.04.2026].

Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. Information, Communication & Society, 20(1), pp. 118–136. https://doi.org/10.1080/1369118X.2016.1186713

Zahariev, A. (2026a). Artificial Intelligence in the Educational and Scientific Degree „Doctor“: Digitalization, Regulation and Credit Acceleration. Fourth national scientific-practical conference with international participation digital transformation of education - issues and solutions (Book of abstracts), p. 6. https://www.conf-dte.bg/proceeding-abstracts.html

Zahariev, A. (2026b). Artificial Intelligence in the „Doctor“ Degree (Presentation). Fourth national scientific-practical conference with international participation digital transformation of education - issues and solutions, ResearchGate, 30 pages, https://doi.org/10.13140/RG.2.2.15951.65446

Zuiderveen Borgesius, F. J. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe, Directorate General of Democracy. Available at: https://www.rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73 [Accessed 25.04.2026].

SOME INFORMATIONAL ASPECTS OF DECISION-MAKING IN MONOPOLISTIC PRODUCTION SYSTEMS

CZU: [330.44+330.47+519.86]:[005.53:658.155]
DOI: https://doi.org/10.53486/tids2026.12

ANATOLIE BARACTARI
Academy of Economic Studies of Moldova
e-mail: baractari.anatolie@ase.md
ORCID ID: 0009-0005-7827-4946

ANATOL GODONOAGĂ
Academy of Economic Studies of Moldova
e-mail: godonoaga@ase.md
ORCID ID: 0000-0001-7459-9536

Abstract. This paper addresses a decision problem of a monopolist producer that aims to maximize profit and operates under three distinct information conditions: certainty, risk or uncertainty. The mathematical model is formulated as the maximization of a profit function $R^{\circ}(x, u, y)$ that depends on two sets of controllable factors - the resource acquisition vector x and the supply volume vector u - and the uncontrollable demand vector y. The model constraints express the technological interdependence between consumed and purchased resources, along with upper and lower bounds for all decision variables. The analysis is structured around three hypotheses determined by the demand-supply relationship for each good j. According to the first hypothesis, where demand exceeds supply, the optimal decision is to offer the maximum available quantity. The second hypothesis where supply exceeds demand: a particular case with a linearly decreasing price function is analyzed and a double inequality is obtained that must be satisfied by the coefficient k_j that expresses the ratio between the maximum and minimum price, ensuring that the optimal solution remains within the admissible range. The third hypothesis addresses the intermediate case in which demand falls between the limits of supply; here, the generalized gradient of the profit function is used, providing the calculation basis for numerical optimization algorithms. For each situation, numerical algorithms are developed to determine the optimal supply variants. Under risk conditions, the mathematical expectation of profit is analyzed. For uncertain conditions, where a finite set of states of nature is operated, the Savage criterion for minimizing regrets is applied and a parallel iterative algorithm is described that executes $L + 1$ simultaneous processes per iteration, with guaranteed convergence under certain conditions.

Keywords: monopolist producer, stochastic demand, optimal decisions, generalized gradient, regret function

JEL Classification: C02, C61, D42, D81.

INTRODUCTION

Monopoly represents the economic agent (called monopolist producer) that operates in the space of large-scale business and within which goods are produced to satisfy the most stringent and widespread needs [1]. Namely, monopoly is that economic system that offers standardized consumer products. In economic theory and practice, it is known that the producer-monopolist can reduce product prices with the increase in quantities offered for sale. Of course, through his activity he tends to achieve certain objectives of his own. One of these objectives, but also the most frequently encountered, consists in determining such policies (decisions), which would ensure obtaining

maximum profit. It is precisely in this direction that the present paper attempts to investigate the behavior of the monopolistic producer.

MODEL FORMULATION AND DESCRIPTION

The profit function is required to be maximized.

$$R°(x,u,y) = \sum_{j=1}^{n}\left[c_j(u_j)\cdot min\{u_j,y_j\} - p_j(u_j)max\{0,u_j-y_j\}\right] - \sum_{i=1}^{m} r_i(\cdot)\ x_i \quad (1)$$

dependent on controllable factors $x=(x_1,\dots,x_i,\dots,x_m)$, $u=(u_1,\dots,u_j,\dots,u_n)$ and those of an uncontrollable nature $y=(y_1,\dots,y_j,\dots,y_n)$.

Model restrictions, in relation to control factors x and u, have the appearance:

$$\sum_{j=1}^{n} a_{ij}.u_j = x_i,\ \ i=\overline{1,m} \quad (2)$$

$$x\in X=\{x\in E^m: 0\le \underline{x_i}\le x_i\le \overline{x_i}, i=\overline{1,m}\} \quad (3)$$

$$u\in U=\{u\in E^n: 0\le \underline{u_j}\le u_j\le \overline{u_j}, j=\overline{1,n}\} \quad (4)$$

Meaning of the notation:

u_j – volume of the product type j, $(j=\overline{1,n})$– quantity supplied of the good j;

x_i – the quantity of the production factor i, $(i=\overline{1,m})$– the demand for resources of the type i;

y_j – the volume of demand for the product j, $(j=\overline{1,n})$;

$c_j(u_j)$ – the unit price of the good j, $(j=\overline{1,n})$ – depends on the quantity supplied u_j;

$p_j(u_j)$ – unit losses (expressed in monetary units), conditioned by the "overproduction" phenomenon (when $(u_j>y_j)$;

$r_i(x_i)$ - the unit price of the resource i – may depend on the quantity of the resource procured in volumex_i units;

a_{ij} – technological coefficient – expresses the quantity of resource $i$used to produce a unit of good j – constant size.

Constraints (2) express the balance between the resources used in the production process and those procured. Therefore, instead of the function $R°(x,u,y)$ in (1), the function can be considered:

$$R(u,y)=\sum_{i=1}^{n} R_j(u_j,y_j), \quad (5)$$

where $R_j(u_j,y_j)$ the expression is denoted by:

$$R_j(u_j,y_j)=c_j(u_j)\cdot min\{u_j,y_j\} - p_j(u_j)max\{0,u_j-y_j\} - \left(\sum_{i=1}^{m} a_{ij}\cdot r_i(\cdot)\right)u_j, j=\overline{1,n} \quad (6)$$

Obviously, the function $R_j(u_j,y_j)$ is presented in two analytical aspects, depending on the relationship between $u_j$and y_j (i.e. between supply and demand for the good j):

$$R_j(u_j, y_j) = \begin{cases} \left(c_j(u_j) - \sum_{i=1}^{m} a_{ij} \cdot r_i(\cdot)\right) u_j, & if\ u_j \le y_j \\ \left(c_j(u_j) + p_j(u_j)\right) y_j - \left(p_j(u_j) + \sum_{i=1}^{m} a_{ij} \cdot r_i(\cdot)\right) u_j, if\ u_j \ge y_j \end{cases} \quad (7)$$

Next, we analyze three hypotheses concerning different interdependencies between demand and supply.

Hypothesis I. Let $y_j \le \underline{u}_j$.

In this case the value $\frac{max}{uj} R_j(u_j, y_j)$ is reached for $u_j^* = \underline{u}_j$ and $\frac{max}{u} R(u, y) = R(\underline{u}, y)$, that is, it is rational for the monopolistic decision-maker to focus on the optimal offer option$u^* = \underline{u}$ and the optimal decision regarding the procurement of resources in terms of $x_i^* = \sum_{j=1}^{n} a_{ij} \cdot \underline{u}_j$.

*Hypothesis II*_. Let $y_j \ge \bar{u}_j$. From (7), it obviously follows that:

$$R_j(u_j, y_j) = (c_j(u_j) - \sum_{i=1}^{m} a_{ij} \cdot r_i(\cdot)) \cdot u_j$$

The first order derivative of this function is:

$$\frac{dR_j(u_j, y_j)}{du_j} = \left(c_j(u_j) - \sum_{i=1}^{m} a_{ij} \cdot r_i(\cdot)\right) + \left(\frac{dc_j(u_j)}{du_j} - \sum_{i=1}^{m} a_{ij} \frac{\partial r_i(\cdot)}{\partial u_j}\right) \cdot u_j$$

The expression $\sum_{i=1}^{m} a_{ij} \cdot r_i(\cdot)$ describes the cost of all the resources needed to obtain one unit of product j. To obtain real profit in relation to the good j, obviously, it is necessary that the difference between price and cost be strictly positive:

$$c_j(u_j) - \sum_{i=1}^{m} a_{ij} \cdot r_i(\cdot) > 0 \quad (8)$$

If the equation $\frac{dR_j(u_j, y_j)}{du_j} = 0$ has the size as its solution $\tilde{u}_j$ then it obviously satisfies the equality:

$$\tilde{u}_j = \frac{\left(c_j(\tilde{u}_j) - \sum_{i=1}^{m} a_{ij} \cdot r_i(\cdot)\right)}{\left(\sum_{i=1}^{m} a_{ij} \frac{\partial r_i(\cdot)}{\partial u_j} - \frac{dc_j(\tilde{u}_j)}{du_j}\right)}.$$

Because the size $\tilde{u}_j > 0$ requires the expression $\sum_{i=1}^{m} a_{ij} \frac{\partial r_i(\cdot)}{\partial u_j} - \frac{dc_j(\tilde{u}_j)}{du_j}$ to be greater than zero.

In particular, if resource prices are fixed, it follows that $\frac{dc_j(u_j)}{du_j} < 0$ and therefore, as supply increases, the price of the good must decrease.

Second order derivative:

$$\frac{d^2 R_j(u_j, y_j)}{du_j^2} = 2\left(\frac{dc_j(u_j)}{du_j} - \sum_{i=1}^{m} a_{ij} \frac{\partial r_i(\cdot)}{\partial u_j}\right) + \left(\frac{d^2 c_j(u_j)}{du_j^2} - \sum_{i=1}^{m} a_{ij} \frac{\partial^2 r_i(\cdot)}{\partial u_j^2}\right) \cdot u_j \quad (9)$$

Remark 1. Analyzing (9), we can conclude: if the price function $c_j(u_j)$ is concave and decreasing on the interval $[\underline{u}_j, \overline{u}_j]$, and the function $r_i(\cdot)$ is convex and increasing (or is a constant quantity), then the profit function with respect to the good j, $R_j(u_j, y_j)$, is concave on $[\underline{u}_j, \overline{u}_j]$, (figure 1). Under these conditions, the respective second-order derivative is negative on $[\underline{u}_j, \overline{u}_j]$.

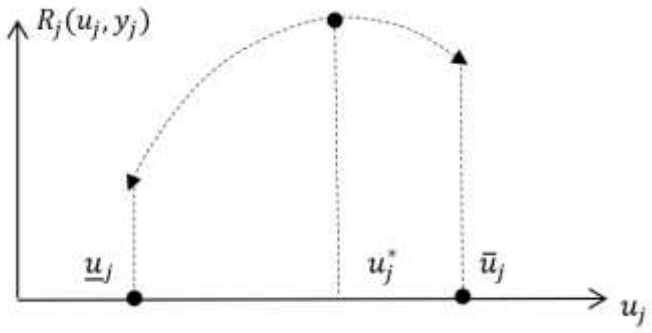


Figure 1. Concave representation of the function $R_j(u_j, y_j)$;u_j^* - the maximum point.

Particular case. Let the price $c_j(u_j)$ be a decreasing linear function with respect to $u_j$on the interval $[\underline{u}_j, \overline{u}_j]$, (figure 2).

$c_j(u_j) = \overline{c}_j - (\overline{c}_j - \underline{c}_j) \cdot (u_j - \underline{u}_j)/(\overline{u}_j - \underline{u}_j)$

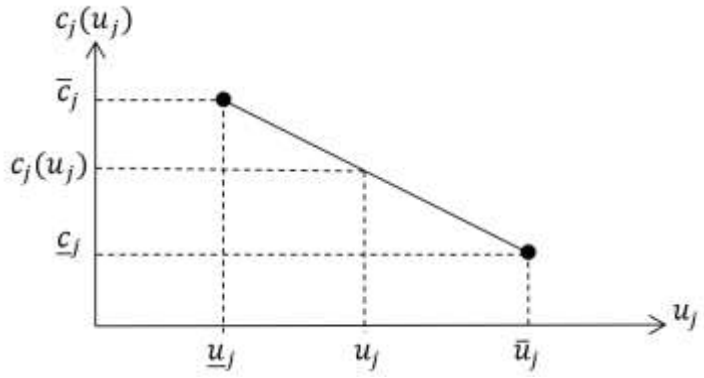


Figure 2. Graphical representation of price $c_j(u_j)$ as a linear function over the interval $[\underline{u}_j, \overline{u}_j]$

Also, it will be assumed that price $r_i(\cdot) = r_i = constant$ and $y_j \geq \overline{u}_j$.

Thus, the function $R_j(u_j, y_j) = \left(c_j(u_j) - \sum_{i=1}^{m} a_{ij} r_i(\cdot)\right) \cdot u_j$ takes on the following appearance:

$$R_j(u_j, y_j) = \left(\frac{\overline{c}_j \overline{u}_j - \underline{c}_j \underline{u}_j}{\overline{u}_j - \underline{u}_j} - \sum_{i=1}^{m} a_{ij} r_i(\cdot)\right) \cdot u_j - \frac{\overline{c}_j - \underline{c}_j}{\overline{u}_j - \underline{u}_j} \cdot u_j^2$$

Let us denote $A_j = \left(\frac{\overline{c}_j \overline{u}_j - \underline{c}_j \underline{u}_j}{\overline{u}_j - \underline{u}_j} - \sum_{i=1}^{m} a_{ij} r_i(\cdot)\right)$, $B_j = \frac{\overline{c}_j - \underline{c}_j}{\overline{u}_j - \underline{u}_j}$

The derivative of the function $R_j(u_j, y_j)$ with respect to u_j is $A_j - 2B_j \cdot u_j$.

$$\frac{dR_j(u_j, y_j)}{du_j} = \left(\frac{\overline{c}_j \overline{u}_j - \underline{c}_j \underline{u}_j}{\overline{u}_j - \underline{u}_j} - \sum_{i=1}^{m} a_{ij} r_i(\cdot)\right) - 2\frac{\overline{c}_j - \underline{c}_j}{\overline{u}_j - \underline{u}_j} \cdot u_j$$

Considering the equation $\frac{dR_j(u_j,y_j)}{du_j} = 0$, its solution (denoted by u_j^*) is determined elementary:

$$u_j^* = A_j/2B_j.$$

Assuming the values $\overline{u}_j$ and are known $\underline{u}_j$, we will study the correlation between the quantities $\overline{c}_j$ and $\underline{c}_j$ so that the quantity u_j^* falls within the interval [$\overline{u}_j$, $\underline{u}_j$]. Obviously,

$$u_j^* = \left[\left(\overline{c}_j\overline{u}_j - \underline{c}_j\underline{u}_j\right) - \left(\overline{u}_j - \underline{u}_j\right)\sum_{i=1}^{m} a_{ij}r_i\right]/2\left(\overline{c}_j - \underline{c}_j\right) \quad (10)$$

So, according to what was mentioned, u_j^* it must respect the inequality:

$$\underline{u}_j \le u_j^* \le \overline{u}_j \quad (11)$$

From (10) and (11) the inequality follows:

$$2\left(\overline{c}_j - \underline{c}_j\right)\underline{u}_j + \left(\overline{u}_j - \underline{u}_j\right)\sum_{i=1}^{m} a_{ij}r_i \le \overline{c}_j\overline{u}_j - \underline{c}_j\underline{u}_j \le 2\left(\overline{c}_j - \underline{c}_j\right)\overline{u}_j + \left(\overline{u}_j - \underline{u}_j\right)\sum_{i=1}^{m} a_{ij}r_i \quad (12)$$

Without loss of generality, it can be considered that $\overline{c}_j = k_j \cdot \underline{c}_j$ for some value of $k_j \ge 1$. Thus, from (12) it can be deduced that:

$$\frac{\left(\overline{u}_j - \underline{u}_j\right)\sum_{i=1}^{m} a_{ij}r_i}{k_j\overline{u}_j - \left(2k_j - 1\right)\underline{u}_j} \le \underline{c}_j \le \frac{\left(\overline{u}_j - \underline{u}_j\right)\sum_{i=1}^{m} a_{ij}r_i}{\left(2 - k_j\right)\overline{u}_j - \underline{u}_j} \quad (13)$$

Inequality (13) can occur if the following relationship is satisfied:

$$k_j\overline{u}_j - \left(2k_j - 1\right)\underline{u}_j \ge \left(2 - k_j\right)\overline{u}_j - \underline{u}_j > 0 \quad (14)$$

To ensure (8) it is also necessary that:

$$\frac{\overline{u}_j - \underline{u}_j}{k_j\overline{u}_j - \left(2k_j - 1\right)\underline{u}_j} \ge 1 \text{ and } \frac{\overline{u}_j - \underline{u}_j}{\left(2 - k_j\right)\overline{u}_j - \underline{u}_j} \ge 1, j = \overline{1,n}, \quad (15)$$

From (14) follows the inequality $k_j(\overline{u}_j - \underline{u}_j) \ge \overline{u}_j - \underline{u}_j$ or $k_j \ge 1$.

From the fact that $\left(2 - k_j\right)\overline{u}_j - \underline{u}_j > 0$ we obtain $k_j < 2 - \underline{u}_j/\overline{u}_j$. So (14) leads to the double inequality:

$$1 < k_j < 2 - \underline{u}_j/\overline{u}_j \quad (16)$$

From the first inequality (15) it follows that the coefficient k_j again must satisfy relation (16), except when $\overline{u}_j < 2\underline{u}_j$. So, if $\overline{u}_j < 2\underline{u}_j$ it is obtained that: $1 < k_j < \underline{u}_j/(2\underline{u}_j - \overline{u}_j)$.

The second inequality in (15) implies inequality (16). Summarizing what has been obtained, it is found that k_j must respect the inequality:

$$1 < k_j < \min\left\{\frac{\underline{u}_j}{2\underline{u}_j - \overline{u}_j}; 2 - \frac{\underline{u}_j}{\overline{u}_j}\right\},$$

if $\overline{u}_j < 2\underline{u}_j$. It is easy to deduce that also for the case $\overline{u}_j < 2\underline{u}_j$, k_j will comply with (16). In other words, even in the situation $\overline{u}_j < 2\underline{u}_j$, $\min\left\{\frac{\underline{u}_j}{2\underline{u}_j - \overline{u}_j}; 2 - \frac{\underline{u}_j}{\overline{u}_j}\right\} = 2 - \frac{\underline{u}_j}{\overline{u}_j}$.

Indeed, considering the difference (and noting with $\alpha = \underline{u}_j/\overline{u}_j$) $\underline{u}_j/(2\underline{u}_j - \overline{u}_j) - (2 - \underline{u}_j/\overline{u}_j) = 1/(2 - 1/\alpha) - (2 - \alpha) = 2(\alpha - 1)^2/(\alpha\left(2 - \frac{1}{\alpha}\right)) > 0$ because $\alpha \in \left(\frac{1}{2}; 1\right)$.

From this it follows that $2 - \underline{u}_j/\overline{u}_j < \underline{u}_j/(2\underline{u}_j - \overline{u}_j)$ for $\overline{u}_j < 2\underline{u}_j$.

Thus, regardless of whether the relationship $\overline{u}_j < 2\underline{u}_j$ or $\overline{u}_j \geq 2\underline{u}_j$, the coefficient k_j must respect inequality (16).

Remark 2. If the decision maker applies a policy of decreasing the price linearly over the interval $[\underline{u}_j, \overline{u}_j]$ and the maximum price (which corresponds to the supply volume $\underline{u}_j$) is $\bar{c}_j$, then, for the maximum supply of $\overline{u}_j$units, he can set the minimum price $\underline{c}_j = \bar{c}_j / k_j$, where k_j he cannot exceed the quantity of $(2 - \underline{u}_j/\overline{u}_j)$ units. Otherwise, he would not obtain the expected result.

Therefore, according to the analytical study, condition (16) determines the range (13) for setting the minimum price $\underline{c}_j$, to ensure that the optimal offer u_j^* falls within the a priori indicated range $[\underline{u}_j, \overline{u}_j]$.

Remark 3. If the demand for the good $j$were known a priori y_j, then one could choose the prices $\underline{c}_j$ and $\overline{c}_j$ (i.e. the coefficient k_j) so as to analytically determine the optimal supply u_j^* and the respective demand for the resource $x_i^* = \sum_{j=1}^{n} a_{ij} \cdot u_j^*$.

Hypothesis III. $\underline{u}_j \leq y_j \leq \overline{u}_j$ From the overview of the function:

$$R_j(u_j, y_j) = c_j(u_j) \min\{u_j, y_j\} - p_j(u_j) \max\{0, u_j - y_j\} - \left(\sum_{i=1}^{m} a_{ij} r_i(\cdot)\right) u_j,$$

it results that for the case $y_j \in [\underline{u}_j, \overline{u}_j]$ the following concrete presentation is obtained:

$$R_j(u_j, y_j) = \begin{cases} \left(c_j(u_j) - \sum_{i=1}^{m} a_{ij} r_i(\cdot)\right) u_j, & if\ u_j \leq y_j \\ \left(c_j(u_j) + p_j(u_j)\right) y_j - \left(p_j(u_j) + \sum_{i=1}^{m} a_{ij} r_i(\cdot)\right) u_j, & if\ u_j > y_j. \end{cases}$$

Thus, the generalized derivative [2]:

$$dR_j(u_j, y_j) = \begin{cases} \left(c_j(u_j) - \sum_{i=1}^{m} a_{ij} r_i(\cdot)\right) + \left(\frac{dc_j(u_j)}{du_j} - \sum_{i=1}^{m} a_{ij} \frac{dr_i(\cdot)}{du_j}\right) \cdot u_j, & if\ u_j \leq y_j \\ \left(\frac{dc_j(u_j)}{du_j} + \frac{dp_j(u_j)}{du_j}\right) \cdot y_j - \left(p_j(u_j) + \sum_{i=1}^{m} a_{ij} r_i(\cdot)\right) - \left(\frac{dp_j(u_j)}{du_j} + \sum_{i=1}^{m} a_{ij} \frac{dr_i(\cdot)}{du_j}\right) \cdot u_j, & if\ u_j \geq y_j \end{cases} \quad (17)$$

The above expressions (17) represent the calculation formulas of the generalized gradient components [2], necessary for the subsequent implementation of numerical algorithms for solving the monopolist problem under conditions of certainty and under conditions of risk.

In the deterministic situation (the demand is known) the algorithm looks like this:

$$u^{k+1} = P_U\left(u^k - h_k g(u^k, y)\right), k = 0,1, \ldots,$$

where the *jth component* of the vector $g(u^k, y)$is calculated according to the rule:

$$g_j(u_j^k, y_j) = \begin{cases} \dfrac{dR_j(u_j^k, y_j)}{du_j}, & if\ \varphi(u^k) \leq \delta_k \\ \dfrac{d\varphi(u^k)}{du_j}, & if\ \varphi(u^k) > \delta_k \end{cases}$$

The functions $\varphi(u^k) = \max\{\varphi_i^1(u), \varphi_i^2(u)\}$, where:

$$\varphi_i^1(u) = \sum_{i=1}^{n} a_{ij} u_j - \overline{x_i}, \qquad \varphi_i^2(u) = \underline{x_i} - \sum_{i=1}^{n} a_{ij} u_j$$

Remark 4. Tolerance threshold [4] δ_k can be taken equal to zero, because, as follows from the definition of the functions φ_i^1 and φ_i^2, the function $\varphi(u)$ satisfies the Slater condition.

In the risk situation, where the information regarding the demand y has a random nature, the distribution law $Q_y(t) = Prob\{y_1 < t, \dots, y_j < t_j, \dots, y_n < t_n\}$ on a certain area $Y = \{y = (y_1, y_j, y_n): \underline{y_j} \le y_j \le \overline{y_j}\}$, and the goal of the monopolist producer consists in determining such a level of supply u^*, for which the average total profit would reach the maximum value:

$$M_y[R(u^*, y)] = max M_y[R(u, y)] ,$$

where is $M_y[R(u, y)]$ the mathematical expectation of profit for the offer variant represented by the vector $u = (u_1, \dots, u_j, \dots, u_n)$, the algorithm represents a modification of the direct stochastic programming method (stochastic gradient projection method). Namely:

$$u^{k+1} = P_U\left(u^k + h_k g(u^k, y^k)\right), k = 0,1,2, \dots, \dots$$

The sequence $y^0, y^1, \dots, y^k, \dots$ is made up of independent simulations of the random vector y obtained according to the probability distribution $Q_y(t)$. The numerical sequences h_k and δ_k, both in the deterministic and risk situations, must meet the following requirements:

$$h_k > 0, h_k \to 0, \delta_k \ge 0, \delta_k \to 0,$$

$$\sum_{k=0}^{\infty} h_k \delta_k = \infty, \frac{h_k}{\delta_k} \to 0$$

In the condition, where uncertainty prevails, regarding the behavior of demand, it will be assumed that the vector y, which represents demand, is associated with a finite number of states $y^1, y^2, \dots, y^l, \dots, y^L$ of nature. These being de facto all possible variants of manifestation of demand. Likewise, it will be admitted that the monopolist as a decision maker, tries to avoid considerable deviations between the expected and the real result. Therefore, it is about the regret function, defined in terms of profit. For the demand variant $y^l = (y_1^l, \dots, y_j^l, \dots, y_n^l)$ the function $R(u, y^l) = \sum_{j=1}^n R_j(u_j, y_j^l)$, and

$$R_j(u_j, y_j^l) = c_j(u_j) \cdot min\{u_j, y^l\} - p_j(u_j) \cdot max\{0; u_j - y_j^l\} - \left(\sum_{i=1}^m a_{ij} \cdot r_i(\cdot)\right) u_j, l = \overline{1, L}.$$

For each $l = \overline{1, L}$ will be denoted by: $R^l = \max\limits_{u \in U} R(u, y^l)$, $\overline{R}(u, y^l) = (R^l - R(u, y^l))$ - the regret function that corresponds to the demand y^l, $R_s(u) = \max\limits_{1 \le l \le L} \overline{R}(u, y^l)$ – called Savage's regret function. So, $R_s(u)$ it is the maximum deviation between the expected and the real profit, if the supply were to occur u and the demand were to be realized in the most unfavorable variant. In the vision of the criterion of minimizing regrets, the monopolist is to determine such a variant of supply $u^* \in U$, for which the Savage function would be realized with the minimum possible variant:

$$R_s(u^*) = \min_{u \in U} R_s(u).$$

Description of the algorithm for determining the optimal offer variant u^* and the minimal regret value $R_s(u^*)$.

The algorithm consists of carrying out, at each iteration, $L+1$ processes, in parallel, of the form:

$$\begin{cases} u_{(l)}^{k+1} = \Pi_U\left(u_{(l)}^k + h_{(l)k} \cdot \eta_{(l)}^k\right), l = \overline{1,L} \\ u^{k+1} = \Pi_U(u^k - h_k \cdot \eta^k), \end{cases} \tag{18}$$

$$\text{where: } \eta_{(l)}^k = \begin{cases} R_u'\left(u_{(l)}^k, y^l\right) / \left\| R_u'\left(u_{(l)}^k, y^l\right) \right\|, \text{for } R_u'\left(u_{(l)}^k, y^l\right) \neq 0 \\ 0, \text{ otherwise.} \end{cases} \tag{19}$$

$$\eta^k = \begin{cases} \left(R_S^k(u^k)\right)_u' / \left\| \left(R_S^k(u^k)\right)_u' \right\|, \text{ for } \left(R_S^k(u^k)\right)_u' \neq 0 \\ 0, \quad \text{otherwise.} \end{cases} \tag{20}$$

Here $R_u'\left(u_{(l)}^k, y^l\right)$ represents some generalized gradient of the function $R(u, y^l)$ for $u = u_{(l)}^k$, and $\left(R_S^k(u^k)\right)_u'$ - the generalized gradient of the function:

$$R_S^k(u) = \max_{1 \le l \le L} \left\{ R\left(u_{(l)}^k, y^l\right) - R(u, y^l) \right\}$$

calculated for the case $u = u^k$.

What about the strings $h_{(l)k}$, $l = \overline{1,L}$ and h_k, it is necessary to satisfy the requirements:

$$h_{(l)k}, h_k \ge 0 \,;\; h_{(l)k}, h_k \to 0 \,;\; \sum_{k=0}^{\infty} h_{(l)k}, \sum_{k=0}^{\infty} h_k = \infty. \tag{21}$$

If the domain U * - is the set of minimum points of the function $R_s(u)$, and all the conditions indicated above hold, then it can be stated [4] that:

$$\lim_{k \to \infty} \min_{u^* \in U^*} \|u^k - u^*\| = 0 \text{ and } \lim_{k \to \infty} R_S^k(u^k) = R_s(u^*) \tag{22}$$

Conditions (18)-(21) ensure the convergence of the iterative process in the following sense. With the increase of k, performing the iterations after $l = \overline{1,L}$, estimates are determined that are increasingly closer to the values of R^l. These estimates help to ensure convergences of the form (22). So, if U^* consists of several variants, then convergence towards one of the optimal variables is ensured. At the same time, the estimates $R_S^k(u^k)$ approach, with the increase of k, the minimum value of the regret function.

CONCLUSIONS

The results obtained would be a justified scientific support for the rigorous mathematical substantiation of the monopolist's decision and provide operational analytical and algorithmic tools for optimizing the offer across the entire spectrum of information environments encountered in monopolistic markets.

REFERENCES:

1. Michael D. Intriguing. Econometric Models, Techniques, and Applications. Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1978, 638p.
2. Shor N.Z. Nondifferentiable optimization and polynomial problems. Boston, Kluwer Academic Publishers, 1998.
3. Godonoagă A., Baractari A. Non-differentiable economic models. Decisional aspects. ASEM Publishing House, Chișinău 2011. ISBN 978-9975-75-575-7
4. Godonoagă A., Blanuța Șt., Ciumacov B. Methods for minimizing the Savage function with various constraints. "Cybernetics and Computer Technologies" magazine. Kyiv: Ин-т кибернетики имени В.М. Глушкова НАН Украины. March 2024. P. 18-26.

DIGITAL TRANSFORMATION IN TOURISM: LEVERAGING PRACTICAL DIGITAL GUIDES FOR PROMOTING THE REPUBLIC OF MOLDOVA AS A TOURIST DESTINATION

CZU: 338.486:[004.771+004.8](478)
DOI: https://doi.org/10.53486/tids2026.13

VALENTINA CAPAŢINA
Associate Professor,
Academy of Economic Studies of Moldova
e-mail: valentina@ase.md
ORCID ID: 0009-0007-9767-7243

IRINA ISPIR
e-mail: ispiririna7@gmail.com
Bevent Production, Republic of Moldova

ADRIANA PROCA
e-mail: adrianaproca13@gmail.com
Vector Academy, Republic of Moldova

Abstract. Digital transformation of the tourism sector represents one of the most significant changes in how destinations are promoted, experienced, and managed in the 21st century. The Republic of Moldova, as an emerging tourist destination in Eastern Europe, faces the dual challenge of increasing its international visibility while adapting to the digital expectations of modern travelers, especially Millennials and Generation Z.
The aim of the paper is to investigate the role of practical digital guides as tools of tourism promotion and destination management, with a specific focus on the Republic of Moldova.
The research question addressed is: how can digital guides increase tourist awareness, improve visitor experience, and contribute to sustainable tourism development in Moldova?
The study uses a *mixed methods* approach, combining a review of the specialized literature on digital tourism, analysis of national digital platforms (including Village Travel Bot, Moldova.travel, and "Discover Moldova: Practical Guide") and secondary data from national and international tourism statistics.
The results indicate that digital guides significantly improve navigation, cultural engagement, and economic activity in both urban and rural areas. "Discover Moldova: Practical Guide", published as an interactive digital brochure via Simplebooklet, illustrates how structured, user - friendly digital content can serve as a bridge between the destination's cultural heritage and the international traveler.
The article also highlights key trends, including AI-based travel assistants, augmented reality in cultural heritage sites, and predictive mobility maps as essential technologies for the future of Moldovan tourism.
The conclusions underscore the need for institutional support, collaboration among various stakeholders, and ongoing digital innovation to position Moldova competitively on the European and global tourism map.

Keywords: digital tourism, digital guide, tourism promotion, destination management, digital transformation.

JEL Classification: L83, O33, Z32

INTRODUCTION

The rapid expansion of mobile devices and internet connectivity has fundamentally changed the way tourists plan, experience, and share travel experiences. According to a global study conducted by American Express Travel, approximately 70% of Millennial and Gen Z travelers choose

destinations based on the quality of the anticipated experience, not just the destination itself (InfoEra, 2025). At the same time, recent trends in European tourism indicate a paradigm shift: away from mass tourism and towards a form of tourism that emphasizes value, quality, and sustainability. According to an analysis published by the Employers' Association of the Tourism Industry in Moldova (APIT) (2026), the competitiveness of destinations is no longer determined exclusively by the number of visitors, but by their ability to offer relevant experiences, engage the local economy, and use digital technologies to personalize services. This shift is of crucial importance for emerging destinations such as the Republic of Moldova, which can leverage their authenticity and flexibility to position themselves strategically on the European tourism market.

This behavioral change exerts enormous pressure on destination management organizations and other tourism stakeholders, driving them to adopt digital tools capable of providing personalized, engaging, and accessible travel information.

The Republic of Moldova, located in Eastern Europe and endowed with a rich cultural heritage, award winning wine routes, and diverse natural landscapes, has historically faced limited international visibility. The tourism sector contributes approximately 3% to Moldova's GDP, and technology enhanced experiences have been identified as a key driver for extending visitor length of stay and expenditure (NBS). Between 2020 and 2026, the adoption of digital mapping tools by tourists visiting Moldova grew by 78%, with 72% of tourists currently using digital maps for navigation and visit planning (AboutMoldova, 2025).

Several national digital tourism initiatives have emerged to address this gap. Village Travel Bot, an interactive Telegram based chatbot, was designated the most innovative tourism solution in 2024 for its contribution to the digitalization of rural tourism experiences (IPN, 2024). Moldova.travel, the national tourism promotion portal, offers itineraries, virtual tours, and information on over 500 tourist attractions. Additionally, digital content such as "Discover Moldova: Practical Guide" published on the Simplebooklet platform demonstrates grassroots efforts to aggregate and disseminate practical destination information for international audiences.

The ***research problem*** underlying this paper concerns how practical digital guides can serve as effective tools for the promotion and sustainable development of tourism in the Republic of Moldova.

The ***relevance of the research*** derives from the need to adapt the tourism sector of the Republic of Moldova to new international digital trends and from the importance of using modern technologies to increase the competitiveness of the tourist destination.

The ***aim*** of this article is to investigate the role of practical digital guides in the process of digital transformation of tourism and to highlight their contribution to the promotion of the Republic of Moldova as a tourist destination.

Furthermore, the research underlines the ***importance of digital innovation*** for increasing competitiveness and supporting the sustainable development of the national tourism sector.

***Main Objectives*:**

1. Analyzing the role of digital guides within the broader context of digital transformation of tourism;
2. Evaluating the impact of existing digital platforms and guides on the tourism sector in the Republic of Moldova;
3. Identifying the main technological trends that can contribute to strengthening Moldova's competitiveness as a tourist destination.

MAIN CONTENT

1. Materials and Methods

The research uses a mixed methodological approach, combining qualitative content analysis with secondary quantitative data. The main documentary sources include:

1. "Discover Moldova: Practical Guide", an interactive digital brochure published on the Simplebooklet platform (2025), which provides structured information for international visitors;
2. The official thematic framework of the TIDS 2026 conference, focused on digital transformation, interdisciplinary applications, and societal impact;
3. Publicly available reports and articles on digital tourism platforms in the Republic of Moldova.

Secondary quantitative data were extracted from national tourism statistics provided by the National Bureau of Statistics of the Republic of Moldova, reports of the National Tourism Office, and analyses published by independent digital research agencies. The landscape of digital platforms was assessed through a structured content analysis of three key platforms: Village Travel Bot, Moldova.travel, and the Discover Moldova digital guide.

The literature review focused on peer reviewed articles and industry reports on digital transformation in tourism, smart destination management, and the role of information technology in destination marketing. Searches were conducted using Google Scholar, ResearchGate, and institutional digital archives. The Harvard referencing system was applied co„nsistently throughout the paper.

2. Results and Discussions

The analysis of Moldova's digital tourism ecosystem reveals a rapidly evolving landscape. The National Bureau of Statistics reported that in the period January–September 2025, collective tourist accommodation structures were visited by 400,000 tourists, signaling a continuation of the sector's post pandemic recovery (statistica.gov.md, 2025). The results confirm trends identified at the European level, where the emphasis is shifting from quantitative to qualitative tourism growth. According to the Employers' Association of the Tourism Industry in Moldova, competitive destinations are those that manage to attract tourists with greater economic value, extend the length of stay, and distribute benefits throughout the region. In this context, the digital guides analyzed in this study directly contribute to achieving these objectives, facilitating access to personalized information and promoting authentic experiences. Digital tools are increasingly identified as drivers of this recovery, with 54% of local businesses in Moldova reporting increases in visitor numbers attributable to digital mapping platforms and guides, and the average length of stay having increased by 26% among tourists who used digital tools to plan their visit (AboutMoldova, 2025).

"Discover Moldova: Practical Guide", created as an interactive digital brochure, exemplifies the potential of user generated digital content. Unlike static PDFs or traditional printed guides, interactive digital brochures hosted on platforms such as Simplebooklet allow the integration of rich media content, hyperlink navigation, and accessibility across multiple devices. These features align directly with the needs of Millennial and Gen Z travelers, who increasingly rely on mobile information sources for planning and navigating travel experiences.

A comparative assessment of the four analyzed platforms is presented in Table 1. The results indicate that Moldova.travel offers the broadest content coverage, while Village Travel Bot excels in conversational interactivity and personalized recommendations. The "Discover Moldova Guide",

although narrower in scope, demonstrates high accessibility and serves as an effective introductory information resource for first time visitors to Moldova.

Table 1. Comparative assessment of the main digital tourism platforms in Moldova.

Platform	Content Accessibility	Multilingual Support	Interactive Functionality	Booking Integration
Moldova.travel	High	English, Romanian, Russian	Virtual tours, itineraries	Partial
Village Travel Bot	Medium	Romanian, English	AI Chatbot, real time Q&A	Activity bookings
Discover Moldova Guide	High	Romanian, English	Hyperlinks, rich media	None
Cahul.travel	Medium	Romanian	Basic	Accommodation

Source: *Authors' own elaboration based on platform content analysis (2025–2026).*

The digitalization of heritage sites represents another high-impact opportunity. Digital storytelling through augmented reality (AR) features for example, at the Orheiul Vechi monastic complex increases cultural engagement by 25% and supports the conservation of Moldova's intangible heritage (AboutMoldova, 2025). Rural areas such as the Purcari wine region, Codrii Forest, and Saharna Waterfall have recorded increases in digital map usage of up to 120% over the last two years, demonstrating that digital tools are not limited to urban tourism but are equally transformative for rural tourism circuits and ecotourism (AboutMoldova, 2025).

Despite these advances, a number of significant challenges persist. Limited internet connectivity in remote areas of the Republic of Moldova continues to affect the real time functionality of digital tourism platforms, particularly those based on interactivity such as chatbots or virtual tours. However, certain resources, such as "Discover Moldova: Practical Guide", offer the option to download content in PDF format, which allows its use even in the absence of an internet connection, thereby increasing accessibility for tourists.

Furthermore, as shown in the table data, the analyzed platforms present different levels of accessibility and functionality. For example, Moldova.travel offers diversified content and extensive multilingual support, but booking integration is only partial. In contrast, AI based applications such as Village Travel Bot facilitate real time interaction but depend directly on internet connectivity. Other platforms, such as Cahul.travel, offer basic functionality and limited booking options, highlighting the need for continued development of digital tourism infrastructure.

Looking ahead, the InfoEra report (2025) identifies ten major digital trends that will shape global tourism by 2026, several of which are directly applicable to Moldova:

1. Personal AI assistants ("Travel Concierge") for complete trip planning: recommendations, bookings, route optimization, full personalization.
2. Augmented and virtual reality (AR/VR) for interactive tours, digital museums, 3D reconstructions, increased tourist engagement.
3. Digital Twin for tourist destinations 3D digital replicas of cities for visitor flow management and personalized experiences.
4. Robots in hotels, airports, and museums for automated check-in, guidance, and robotic hospitality services.
5. Web3 Tourism for NFTs, tokenized tickets, digital reputation, and blockchain payments.

6. Predictive maps and smart mobility for optimized routes based on traffic, weather, and tourist flow.
7. Autonomous hotels (fully self-service): digital check-in, smart rooms, AI based dynamic pricing.
8. Digital culinary tourism: personalized culinary itineraries + AI recommendations + integrated bookings.
9. Biometric security and digital travel identity: facial scanning, automated airport access, and integrated services.
10. "City-as-a-Service" platforms: cities as integrated digital ecosystems (transport, restaurants, guides, events).

At the local level, the EkoApp Moldova application, launched by the National Tourism Office in July 2025, marks a significant institutional commitment to digital tourism development (financialcontent.com, 2025).

To better understand the current position of digital guides in promoting tourism in the Republic of Moldova, a **SWOT** analysis (*S – Strengths*; *W – Weaknesses*; *O – Opportunities*; *T – Threats*) is presented below, highlighting the main strengths, weaknesses, opportunities, and threats in this area.

***Strengths*:** Internal characteristics and resources supporting a successful outcome

- Digital tourism platforms exist (e.g., Moldova.travel);
- Tourists are increasingly using smartphones and online maps for travel;
- Useful and easily accessible digital guides exist, such as "Discover Moldova".

Weaknesses: Internal characteristics and resources impeding a successful outcome

- Not all tourism platforms are interconnected;
- Some areas of the country have poor internet connectivity;
- Some websites do not have full booking functionality.

***Opportunities*:** External factors that can be leveraged to the project's or business's advantage

- New technologies (AI, smart applications) are developing rapidly;
- More and more tourists are seeking authentic experiences, and Moldova can offer these;
- Rural tourism can be developed through digital promotion.

Threats: External factors that may have a potentially damaging effect on the project or business

- Other countries already have more advanced digital tourism systems;
- Technology changes very rapidly and requires constant investment;
- Tourists have increasingly high expectations of digital services.

The SWOT analysis highlights the fact that the Republic of Moldova has significant potential for the development of digital tourism, supported by increased use of mobile technologies and the emergence of digital platforms dedicated to destination promotion. At the same time, the existence of limitations related to digital infrastructure and the integration of tourism services demonstrates the need for coordinated investments and strategies at the institutional level. Leveraging the opportunities offered by new technologies and the growing interest in authentic experiences can contribute to strengthening the Republic of Moldova's competitiveness on the international tourism market.

CONCLUSIONS

In line with European trends, the future of tourism in the Republic of Moldova depends on the capacity to build a model based on value, technology, and institutional coordination. Practical digital guides can become an essential tool in this transition, contributing to the creation of a coherent, smart, and competitive destination. This paper has demonstrated that practical digital guides play an essential role in the promotion and sustainable development of tourism in the Republic of Moldova. Three main conclusions emerge from the research.

Firstly, the digital transformation of Moldova's tourism sector is already underway, evidenced by the growing adoption of mobile applications, interactive chatbots, and digital portals. Between 2020 and 2026, the adoption of digital tools among tourists visiting Moldova grew by 78%, with measurable positive effects on visitor satisfaction, average length of stay, and revenues of local businesses.

Secondly, student and community produced digital content, such as "Discover Moldova: Practical Guide", complements official tourism platforms by providing accessible, English language, practically oriented information for international visitors. The novelty and originality of such grassroots digital resources lie in their agility they can be updated quickly, distributed through social networks at negligible cost, and adapted to specific visitor profiles that institutional platforms may overlook.

Also, the study identifies augmented reality, AI based travel assistants, and integrated smart mobility platforms as the most promising technological frontiers for Moldova's tourism sector. Future research should focus on measuring the real economic and behavioral impact of these technologies through the collection of primary data (surveys and field experiments) at major tourist attractions in Moldova. A significant limitation of the present study is its reliance on secondary data; long term primary research would strengthen the evidence base for policy makers.

In summary, Moldova possesses the digital resources, cultural wealth, and institutional momentum necessary to position itself as a competitive, technology-driven travel destination. Sustainable collaboration among various stakeholders, including the National Tourism Board, academic institutions, IT developers, and content creators will be crucial to transforming this potential into measurable growth.

REFERENCES

AboutMoldova, 2025. How Digital Mapping Tourism Moldova is Revolutionizing the Moldova Travel Guide Map Experience. AboutMoldova, 9 September. Available at: https://aboutmoldova.md/en/view_articles_post.php?id=3314 [Accessed 20.04.2026].

Employers' Association of the Tourism Industry in the Republic of Moldova – APIT, 2026. The new European tourism code: why 2026 is unlike anything that came before. Facebook post, 15 April. Available at: https://www.facebook.com/APITRM/posts/noul-cod-al-turismului-europeande-ce-2026-nu-mai-seam%C4%83n%C4%83-cu-nimic-din-ce-a-fost-/1288190076745005/ [Accessed 20.04.2026].

financialcontent.com, 2025. Moldova Forges a Future in Tourism: Blending Heritage, Eco-Adventures and Tech Innovation. Market Minute, 6 October. Available at: https://markets.financialcontent.com/stocks/article/marketminute-2025-10-6-moldova-forges-a-future-in-tourism-blending-heritage-eco-adventures-and-tech-innovation [Accessed 22.04.2026].

InfoEra, 2025. How Innovations Are Transforming Tourism. InfoEra Blog, 12 December. Available at: https://infoera.md/en/blog/57 [Accessed 22.04.2026].

Interreg Europe, 2024. Tourism Strategies and Roadmaps for Supporting SMEs in Moldova. Interreg Europe, 23 July. Available at: https://www.interregeurope.eu/find-policy-solutions/expert-support-reports/tourism-strategies-and-roadmaps-for-supporting-smes-in-moldova [Accessed 25.04.2026].

IPN, 2024. Free Tourist App Village Travel Bot, Innovation in Digital Rural Tourism. IPN News Agency, 8 October. Available at: https://www.old.ipn.md/en/free-tourist-app-village-travel-bot-innovation-in-digital-rural-tourism-7967_1107862.html [Accessed 22.04.2026].

Moldova.travel, 2026. Official National Tourism Portal of the Republic of Moldova. Available at: https://moldova.travel [Accessed 22.04.2026].

simplebooklet.com, 2025. Discover Moldova: Practical Guide (1). Simplebooklet. Available at: https://simplebooklet.com/discovermoldovapracticalguid1 [Accessed 25.04.2026].

statistica.gov.md, 2025. Statistics on tourist accommodation, January–September 2025. National Bureau of Statistics. Statistical indicator details. Available at: https://statistica.gov.md/ro/statistic_indicator_details/11 [Accessed 22.04.2026].

VillageTravel.md, 2024. Village Travel Bot – Interactive Telegram Chatbot for Rural Tourism in Moldova. Available at: https://www.villagetravel.md [Accessed 25.04.2026].

World Bank, 2025. From Queues to Clicks: Digitalization Transforms Moldova's Public Services. World Bank Feature Story, 2 December. Available at: https://www.worldbank.org/en/news/feature/2025/12/02/from-queues-to-clicks-digitalization-transforms-moldova-s-public-services [Accessed 22.04.2026].

ANALYSIS OF THE PUBLIC WARNING SYSTEM

CZU: 614.8:004.78(478)
DOI: https://doi.org/10.53486/tids2026.14

SERGHEI PEANCOVSCHII
The Free International University of Moldova
e-mail: an_stern@hotmail.com
ORCID ID: 0000-0002-7414-1127

Abstract. Modern public safety paradigms require an immediate, resilient, and ubiquitous mechanism for emergency notification. This paper analyzes the digital transformation of Public Warning Systems (PWS) within the Republic of Moldova, transitioning from obsolete analog sirens to centralized digital platforms.

The core research question examines how modern digital standards and wireless technologies can overcome the delivery latency, institutional fragmentation, and regulatory limitations inherent in legacy analog notification networks. Utilizing a comprehensive systems framework and comparative-legal analysis aligned with the newly enacted Law of the Republic of Moldova No. 72 "On Electronic Communications" (2025), a central component of this study is the development of a technical and regulatory verification matrix that evaluates public notification success probabilities within specific timeframes.

Based on United Nations vulnerability assessments and the General Inspectorate for Emergency Situations (IGSU) data, the analytical results demonstrate that digital point-to-area Cell Broadcast configurations fundamentally outperform legacy infrastructures by distributing geo-fenced alerts within 5 to 10 seconds without inducing cellular network congestion or violating subscriber privacy.

Furthermore, the study evaluates the integration of the Common Alerting Protocol (CAP) as a universal XML data standard to completely automate message processing and eradicate manual dispatch delays. The primary practical contribution of this research is that its findings served as the foundational basis for the official technical documentation and project blueprints of the "MD-ALERT" national initiative.

Ultimately, the paper concludes that robust civil protection requires a strict architectural separation between multiple hazard-detecting Early Warning Systems (EWS) and a single, unified national Public Warning System (PWS), delivering a conflict-free technological shield.

Keywords: Public warning systems, Cell Broadcast, Common Alerting Protocol, Digital Security, Moldova, Emergency Notifications.

JEL Classification: O32, H56.

INTRODUCTION

The digital security and technological modernization of public safety infrastructure represent critical components for protecting national security and achieving digital transformation. In the modern information society, traditional public notification mechanisms face severe structural obsolescence. Legacy methods—such as traditional acoustic sirens, wired broadcasting, analog radio, and linear television—fail to ensure total population coverage during localized crises.

This systemic failure is further compounded by the structural shift from analog to digital telecommunications and the total transformation of domestic media consumption habits. Historically, national public warning frameworks relied on centralized analog television interception and mandatory urban wired radio networks (radio-outlets) installed in every household, ensuring baseline resilience even during power grid failures. In the modern post-transition landscape, the migration to digital multiplexes, fragmented IP-TV streaming platforms, and the complete domestic extinction of linear radio receivers have created an institutional decoupling. Consequently, legacy mass-media

interception has lost its operational ubiquity, leaving a significant portion of the population completely isolated from traditional real-time emergency broadcasts inside their residences.

Under escalating climate, technological, and geopolitical threats, public notification practices require an urgent modernization toward advanced digital technologies and internet platforms that ensure immediate data dissemination (United Nations Moldova, 2024; Karaman *et al.*, 2024). For the Republic of Moldova, this technological shift must align directly with national security frameworks and European integration strategies.

Global public warning frameworks in nations such as the United States, Japan, and Romania rely heavily on Cell Broadcast technology, which utilizes a point-to-area functional design and delivers alerts within 5 to 10 seconds over dedicated radio channels (IGSU, 2026; United Nations Moldova, 2024; Kim *et al.*, 2021).

Building on previous research regarding the efficiency of digital platforms, Peancovschii (2024, pp. 17–27) utilizes a systems approach to demonstrate that digital point-to-area configurations fundamentally outperform legacy analog alert networks by eliminating their inherent limitations in transmission speed, geographic precision, and operational stability, thereby drastically reducing notification latency.

Existing research points to the importance of Cell Broadcast technologies in building resilient emergency communication infrastructure. Compared to conventional SMS-based architectures, 5G Public Warning Systems provide higher dissemination speeds and greater geographic precision (Kim *et al.*, 2021). Similarly, LTE-based Cell Broadcast Services offer scalable, congestion-free notification capacity when mobile networks experience peak traffic during large-scale emergencies (Suryandari et al., 2020). Disaster management strategies increasingly rely on these communication channels to address climate-related, technological, and geopolitical hazards (Karaman *et al.*, 2024).

Despite these operational advantages, implementing modern public warning solutions involves substantial structural challenges. Deploying national systems requires addressing technical, financial, regulatory, and institutional constraints that vary across countries. As a result, technical adoption cannot follow a uniform template; it must adapt to existing domestic operator networks and the specific legislative frameworks governing emergency communications.

In response to these challenges, this study develops a methodological framework to identify and mitigate deployment barriers facing the Republic of Moldova's national Cell Broadcast network (MD-ALERT).

MAIN CONTENT

1. Materials and Methods

The methodological framework combines systems analysis with comparative legal assessment to examine Public Warning Systems (PWS) operating under complex crisis conditions. The study evaluates the integration of public notification infrastructure into national security policy, digital transformation initiatives, and the Republic of Moldova's European integration agenda.

The assessment focuses on four notification mechanisms: acoustic sirens, linear broadcasting, Cell Broadcast technology, and automated data exchange protocols. Their performance is evaluated against three technical criteria: transmission latency, geographic targeting accuracy, and network reliability under peak-load conditions. Technical parameters provided by mobile network operators are analyzed alongside domestic telecommunications regulations governing emergency alerting.

To examine the technological architecture of the warning process, information flows are traced from environmental monitoring systems to end-user mobile devices. The Common Alerting Protocol (CAP v1.2) serves as the reference interoperability standard for analyzing data exchange between system components (OASIS, 2010; ITU-T X.1303). Geographic delivery performance is evaluated by combining population vulnerability indicators with mobile network coverage maps, allowing the assessment of warning capabilities in areas exposed to different levels of risk.

To evaluate alert dissemination performance, the verification model incorporates empirical telecommunications data alongside existing regulatory requirements. This model estimates the probability of successful alert delivery within predefined time intervals ranging from 10 to 300 seconds under different emergency scenarios.

The proposed approach was applied during the preparation of technical and project documentation for Moldova's national MD-ALERT initiative (IGSU, 2026). Population exposure and network topology were analyzed to identify the main technical and organizational constraints affecting deployment and to assess their implications for system implementation.

2. Results and Discussion

Analytical assessments confirm that legacy notification methods face structural obsolescence. Traditional acoustic sirens, linear television, and analog radio networks fail to ensure total population coverage in modern information societies. Data from the United Nations vulnerability report for Moldova indicate that infrastructure developments, such as improved structural insulation and double-glazed windows, severely decrease the indoor penetration index of acoustic sirens (United Nations Moldova, 2024). Furthermore, shifting media consumption habits isolate a significant portion of the population from linear television and radio broadcasts during localized crises.

Digital technologies and internet platforms resolve these operational limitations through immediate data dissemination. Evaluating international public warning practices established the baseline for this technological transition. Frameworks in most countries that have already implemented this technology, including the United States, Japan, the Netherlands, Canada, New Zealand, South Korea, Israel, and Romania, rely heavily on the deployment of Cell Broadcast technology (IGSU, 2026; United Nations Moldova, 2024).

According to technical documentation, Cell Broadcast bypasses the standard point-to-point architecture of conventional short message services (SMS) (IGSU, 2026; United Nations Moldova, 2024; ETSI TS 122 268, 2024; 3GPP, 2026; Suryandari *et al.*, 2020). Instead, it utilizes a point-to-area functional design. This specific design avoids network congestion because the transmission does not require an active subscriber telephone database. The system distributes messages, transmitting communication over a technically dedicated radio channel, to all mobile devices within a single cell tower sector inside 5 to 10 seconds (IGSU, 2026; United Nations Moldova, 2024).

Despite these substantial technological advantages, the large-scale implementation of modern public warning infrastructures remains operationally complex.

The implementation of digital warning systems reveals distinct structural challenges (Karaman et al., 2024). The research isolates five main global barriers to this integration:

Infrastructural barrier: The urgent necessity to modernize digital infrastructure and existing communication systems.

Financial barrier: The deficit of financial resources required for total technology deployment and further maintenance of this technology.

Regulatory barrier: The urgent necessity to improve the legislative and technical frameworks of the Republic of Moldova to establish a legal baseline for new public warning technologies.

Institutional barrier: The localized ambition of individual emergency monitoring departments to develop proprietary Early Warning Systems (EWS) instead of integrating into a unified national Public Warning System (PWS).

Socio-technological barrier: The critical requirement to improve public digital literacy, as even the most advanced technology fails without basic user adaptation.

The regulatory provisions of the new Law of the Republic of Moldova No. 72 "On Electronic Communications", enacted on April 10, 2025, directly incorporate the specific recommendations of this study (Law of the Republic of Moldova No. 72, 2025). This research determines the enforcement mechanisms to mandate technical cooperation between state emergency departments and commercial telecommunication providers. Concurrently, amendments to other regulatory and legal frameworks are expected in the near future.

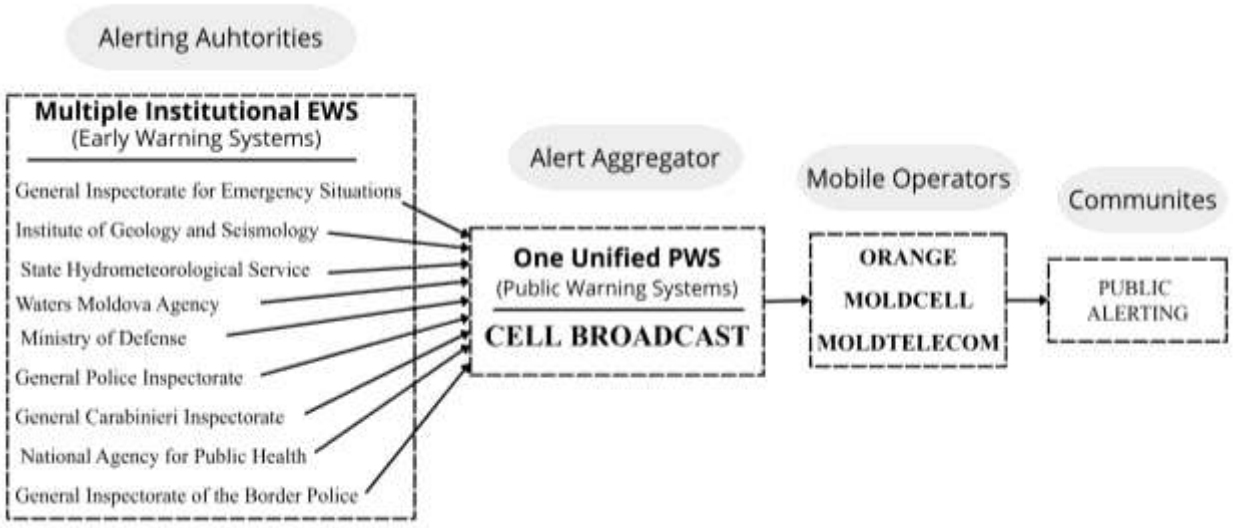


Figure 1. MOLDOVA PUBLIC WARNING STRATEGY: Method to Overcome Institutional Barriers (EWS vs. PWS)

Source: *Compiled by the author*

As a strategic method to overcome the institutional barrier, the emergency management framework of the Republic of Moldova must clearly distinguish between localized and unified platforms. Within this framework, numerous institutional Alerting Authorities operate their own Early Warning Systems (EWS) tailored to monitor and analyze specific hazards. While these analytical systems can be numerous to process distinct environmental and security data, the national Public Warning System (PWS) must remain strictly unified as a single platform. This clear architectural separation guarantees real-time alert dissemination without technical conflict, as EWS and PWS operate on entirely different algorithms to serve distinct purposes: while the former focus on data analysis and threat detection, the latter is dedicated exclusively to immediate, mass public notification. This institutional interaction model is illustrated in Figure 1.

The quality of public warning directly depends on the speed of interaction between threat detection platforms Early Warning Systems (EWS) and the Public Warning System (PWS). To ensure their coordinated operation, the implementation of the national Public Warning System (PWS) must

strictly prioritize technologies that natively support the Common Alerting Protocol (CAP). Concurrently, all institutional Early Warning Systems (EWS)—both currently operational and newly developed—must dynamically support this protocol to ensure seamless integration into the unified national PWS, providing a standardized data exchange between systems at both national and international levels. To achieve automated data processing, the CAP data standard uses an XML structure to digitize critical alert parameters, including threat type, geographical boundaries, and precise safety protocols (OASIS Standard, 2010; ITU-T Recommendation X.1303, n.d.). This digital format links real-time environmental sensors and geographic information systems directly with mobile operator switches. The automation removes manual dispatch delays, decreases notification latency, and creates a unified technological shield to protect citizens. This interoperability is essential for maintaining synchronized communication between multiple institutional Early Warning Systems and the unified national Public Warning System.

Table 1 summarizes the comparative technological and regulatory differences between legacy public warning infrastructures and the proposed national PWS (MD-ALERT). The comparative matrix highlights how the enforcement of Law No. 72 'On Electronic Communications' and the integration of the Common Alerting Protocol (CAP) systematically eliminate the delivery latency, network congestion, and structural limits inherent in the old public notification mechanisms of the Republic of Moldova (IGSU, 2026).

Table 1. Comparative Matrix of Legacy and Modern Public Warning Systems

Evaluation Metric	Legacy Warning Systems	Modern PWS / MD-ALERT
Technical Baseline	Analog networks, sirens, wired broadcasting, linear television, and traditional SMS-cell broadcasting.	Digital Cell Broadcast infrastructure utilizing specific network nodes (BSC, RNC, MME, AMF) across 2G, 3G, 4G, and 5G networks.
Notification Latency	**High latency.** Sequential SMS dispatching creates severe network bottlenecks, taking from tens of minutes to several hours.	**Near real-time (5–10 seconds).** Simultaneous broadcast transmission to all active devices within the targeted coverage area.
Geographical Precision	Broad/macro-level broadcasting (regional or nationwide) without the capability for localized geo-fencing.	Highly precise target alerting based on the cell sector architecture of mobile network operators (Geo-fencing).
Network Congestion	High risk of cellular network collapse and congestion due to massive, concurrent traffic loads on standard signaling channels.	**Zero network impact.** Does not utilize public signaling channels; operates via a dedicated Cell Broadcast frequency.
Data Standard	Non-standardized text or voice messages requiring manual dispatching and administrative intervention.	Standardized XML data structures fully compliant with the international **Common Alerting Protocol (CAP).**
Regulatory Framework	Outdated civil protection acts that lack mandatory technical integration requirements for commercial telecom operators.	Direct compliance and enforcement under the new **Law of the Republic of Moldova No. 72 "On Electronic Communications"** dated April 10, 2025.

Evaluation Metric	Legacy Warning Systems	Modern PWS / MD-ALERT
B2G Integration	Absence of legally binding or automated technical cooperation mechanisms between state agencies and private operators.	Contractually and legally mandated technical interaction architecture with major operators: Orange, Moldcell, and Moldtelecom.
User Awareness & Literacy	Requires active user adaptation (tuning in to radio/TV, waiting for SMS) or triggers mass panic (analog sirens).	Guaranteed, high-priority pop-up push notifications with distinct audio overrides, delivering actionable safety protocols.

Source: *Compiled by the author based on the cited technical and legal sources*

CONCLUSIONS

The digital security and technological modernization of the public safety infrastructure in the Republic of Moldova require a systematic transition from legacy notification methods to an advanced, unified platform. This research addresses the critical institutional, legal, and technological barriers to the deployment of the national cell broadcast public warning network (MD-ALERT).

Based on the results of this study, several primary conclusions can be drawn:

- **Institutional Integration via Architectural Separation:** The study establishes a strategic method to overcome the institutional barrier by clearly separating localized **Early Warning Systems (EWS)** from the unified **Public Warning System (PWS)**. While individual alerting authorities must operate multiple decentralized platforms for deep data analysis and hazard detection, the mass notification infrastructure must remain strictly unified under a single PWS. This architectural division prevents technical conflicts, leverages distinct algorithms for specific tasks, and guarantees rapid, non-interfering message delivery.
- **Regulatory Adaptation and Harmonization:** The regulatory provisions of the new Law of the Republic of Moldova No. 72 "On Electronic Communications," enacted on April 10, 2025, directly incorporate the specific recommendations and enforcement mechanisms determined by this research. This framework establishes the necessary statutory authority to mandate technical cooperation between state emergency departments (such as IGSU) and commercial telecommunication providers (Orange, Moldcell, and Moldtelecom). Concurrently, rapid amendments to adjacent civil protection regulatory frameworks are expected in the near future to fully adapt the legal ecosystem to new digital capabilities.
- **Technological Standardization through CAP:** To eliminate operational latency and network congestion inherent in legacy systems, the implementation of the MD-ALERT infrastructure must strictly prioritize technologies natively supporting the **Common Alerting Protocol (CAP)**. Ensuring that both currently operational and future EWS platforms utilize this standardized XML data structure allows for complete automation. This configuration bypasses public signaling channels, eliminates manual dispatch delays, and reduces response latency to a critical baseline of **5–10 seconds**.

Ultimately, the technical and regulatory verification matrix developed in this study confirms that the cross-platform integration of MD-ALERT effectively mitigates structural infrastructure limits. By harmonizing state administrative mandates with the network nodes of private mobile operators, this research delivers a comprehensive, automated technological shield capable of ensuring rapid, geo-fenced public safety notification across the Republic of Moldova.

REFERENCES

3GPP (2026). *3GPP Technical Specifications Cloud and Download Portal*. Available at: https://portal.etsi.org/new3g/specs/download.htm (Accessed: 20 May 2026).

ITU-T Recommendation X.1303 (2014). Common Alerting Protocol (CAP 1.2). Available at: https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/2020/T-REC-X.1303bis-201403-.pdf (Accessed: 20 May 2026).

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. *Official Journal of the European Union*, L 321, pp. 1–181. Available at: https://eur-lex.europa.eu/eli/dir/2018/1972/oj (Accessed: 20 May 2026).

ETSI TS 122 268 (2024). Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Public Warning System (PWS) requirements (3GPP TS 22.268 version 18.2.0 Release 18). European Telecommunications Standards Institute.

European Telecommunications Standards Institute (ETSI) (n.d.). ETSI: Welcome. Available at: https://www.etsi.org (Accessed: 20 May 2026).

IGSU (2026). Feasibility Study on the Deployment and Implementation of the National Public Warning Network "MD-ALERT" in the Republic of Moldova. *General Inspectorate for Emergency Situations (IGSU) of the Ministry of Internal Affairs of the Republic of Moldova*. Available at: https://igsu.gov.md/sites/default/files/media/documents/2026-02/Feasibility%20Study%20-%20MD-ALERT.pdf (Accessed: 20 May 2026)

Karaman, B., Basturk, I., Taskin, S., Zeydan, E., Kara, F., Beyazit, E.A., Camelo, M., Björnson, E. and Yanikomeroglu, H. (2024). "Solutions for Sustainable and Resilient Communication Infrastructure in Disaster Relief and Management Scenarios", *arXiv preprint, arXiv:2410.13977.* Available at: https://arxiv.org/pdf/2410.13977 (Accessed: 20 May 2026)

Kim, M., Lee, S. and Park, J. (2021). "Design of Public Warning System using Cell Broadcast Service in 5G Network", *Proceedings of the 23rd International Conference on Advanced Communications Technology (ICACT 2021)*, pp. 245-248. Available at: https://icact.org/upload/2021/0151/20210151_finalpaper.pdf (Accessed: 20 May 2026).

Law of the Republic of Moldova No. 72 "On Electronic Communications", enacted on April 10, 2025. Monitorul Oficial al Republicii Moldova, Nr. 213-216 [in Romanian]. Available at: https://www.legis.md/cautare/getResults?doc_id=152659&lang=ro (Accessed: 20 May 2026).

OASIS Standard (2010). Common Alerting Protocol Version 1.2. *OASIS Standard Open*, Approved 1 July 2010. Available at: http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html (Accessed: 20 May 2026).

Peancovschii, S. (2024). Analysis of modern population alert technologies in emergency situations. *Journal of Engineering Science*, XXXI (2), pp. 17-27. https://doi.org/10.52326/jes.utm.2024.31(2).02 (Accessed: 20 May 2026)

Suryandari, A., Astuti, R.P. and Salsabila, S. (2020). "Design of Public Warning System Based on Cell Broadcast Service in LTE Network", *2020 International Conference on Inventions in Computing and Industry (ICICI)*, pp. 1-5. Available at: https://ieeexplore.ieee.org/abstract/document/9370504 (Accessed: 20 May 2026).

United Nations Moldova (2024). Feasibility Study on Public Warning and Population Vulnerability Assessment in the Republic of Moldova. Chisinau: UN Moldova. Available at: https://moldova.un.org/sites/default/files/2024-02/Feasibility%20study%20Moldova.pdf (Accessed: 20 May 2026).

ARTIFICIAL INTELLIGENCE, PRODUCTIVITY GROWTH, AND UNIVERSAL BASIC INCOME: A THEORETICAL DEBATE IN ECONOMIC THOUGHT

CZU: [004.8:330.341.1+331.101.6]: 330.1
DOI: https://doi.org/10.53486/tids2026.15

MIHAIL CIOBANU
National Institute for Economic Research
Academy of Economic Studies of Moldova (AESM)
e-mail: ciobanu.mihail@ase.md
ORCID ID: 0000-0003-1193-6018

Abstract. There is growing concern within the economics and business communities about the rate of diffusion of new production technologies using AI into mainstream production, leading to surpluses of productivity of unprecedented magnitude and, in the interstitial space between these advances, consequent and profound declines in labor demand across a very wide set of occupations. This so-called 'structural technological unemployment' is being expressed in a series of interrelated challenges to the distributional arrangements of, and the longer-term sustainability of, contemporary market economies, notably declines in labor's share of income, and a growing concentration of capital ownership in the hands of technology companies. In this paper we investigate the thesis that Universal Basic Income (UBI) may function as an appropriate instrument of redistribution to capture such AI-generated productivity. We treat UBI as a concept within the traditional domains of welfare economics, post-Keynesian macro, institutional economics and political economy. We engage in a critical review of the distributional implications of UBI-as-redistribution, laying out the core theoretical architecture of the argument, identifying its critical weaknesses and main contrary arguments as they appear in current literature. We report on empirical experience from around the world of the small number of experiments with UBI as it has been tried in Finland, the US and Kenya, with due recognition of the associated limitations of all such work as they are essentially partial-equilibrium experiments which lack necessary and sufficient bearings for scalably implementing such policies universally. We then assess three of the canonical financing models of UBI which have received most attention: a robot tax; a capital dividend; and a consolidated value-added tax. We go on to set out the core of the argument about UBI within the broader and associated debate on the post-work society and on the future of the labor contract in the AI economy and, more broadly, on the necessary social foundations to be supplied in any market economy to achieve and preserve economic citizenship and to underpin the economy's work repository in between episodes of technologically driven crisis. Our preliminary view, traversed as this is by a number of key contingencies, is that UBI has the potential to function as a very coherent redistributive instrument within an AI economy but that its desirability and efficacy are contingent upon a host of matters including, notably, the institutional design chosen for its implementation and the associated required set of complementary policies and the successful socio-political governance of the new technologies in question. The article was developed within the framework of Subprogram 030101 „Strengthening the resilience, competitiveness, and sustainability of the economy of the Republic of Moldova in the context of the accession process to the European Union", institutional funding.

Keywords: artificial intelligence, universal basic income, productivity redistribution, robot tax, post-work economics, welfare state.

JEL Classification: D63, E25, H53, I38, J24, O33.

INTRODUCTION

The intersection of artificial intelligence and distributional economics is now one of the most contested terrains in contemporary economic theory. For the first time since the mechanization debates of the early nineteenth century, serious economists entertain the proposition that technological progress may generate structural, not merely frictional, unemployment - displacing not only routine manual tasks but cognitive and creative functions once considered immune to automation (Frey, and Osborne, 2017; Acemoglu, and Restrepo, 2019). The political economy question that follows is not merely technical: if AI systems appropriate an ever-larger share of productive output while the owners of those systems constitute a shrinking fraction of the population, by what mechanism should the resulting gains be redistributed? Universal Basic Income - a periodic, unconditional cash transfer paid to all members of a political community - has re-emerged as a proposed answer. Proponents locate UBI within a tradition stretching from agrarian justice to negative income tax and to real libertarianism. Critics, spanning orthodox public finance economists, post-Keynesian structuralists, and feminist political economists, challenge UBI on grounds of fiscal affordability, work incentive effects, inflationary risk, and its substitution logic relative to existing categorical benefits. This paper does not adjudicate definitively between these positions. Rather, this article sets out to systematically map and reconstruct the current theoretical debate with due attention to the core premises, the key moves and relevant empirical uncertainties of opposing arguments.

MAIN CONTENT

1. Materials and Methods

This study undertakes a systematic review of current literature, drawn from leading scientific databases. Sources include contemporary as well as classical contributions, as well as theoretical and empirical work. The reports of institutions and of policies, lacking a peer-reviewed counterpart, were also considered suitable sources. A combination of a comparative analysis of current theories and an assessment of the current empirical evidence was employed to analyze the competing views on UBI. The constitutive propositions of each view were decomposed and analyzed for internal consistency within each of the relevant theoretical traditions. Evidence from existing UBI pilot programs was reviewed and analyzed with due consideration to the limitations of partial-equilibrium studies designed to test for the effects of UBI in particular circumstances, as opposed to its implications for universal application. The financing models of UBI were analyzed with respect to four criteria: revenue adequacy, allocative efficiency, distributional effects, and political sustainability.

2. Literature review

Frey and Osborne (2017) were amongst the first to forecast high risk of automation for about 47% of US employment over the twenty years to the mid 2030s. However, in reducing this to the level of individual jobs, other studies found that task heterogeneity within jobs on average reduced the share of jobs highly exposed to automation to only around 9% across 21 OECD countries (Arntz, Gregory and Zierahn, 2016). Other studies focused on the tasks that composed jobs, classifying those as largely routine in either a cognitive or manual sense as most susceptible to automation and those of an largely non-routine analytic or interactive nature as less susceptible to substitution by algorithms (Autor, Levy and Murnane, 2003). However, there is also more recent research highlighting how large language models, in particular, are starting to affect a whole range of knowledge-intensive jobs, including legal research, finance and even software development (Eloundou et al., 2023). Much of this automation is creating so-so technologies that displace workers without boosting overall

productivity in ways that raise wages for the average worker, and so lead to negative welfare effects (Acemoglu, 2021). A plurality of intellectual traditions trace back to the idea of Universal Basic Income. There is a libertarian version of UBI, looking for a market-efficient alternative to current welfare bureaucracies. There is also a republican egalitarian version of UBI, grounding a share in the resources collectively produced by all members of society on the rights of individuals. Finally, there is a social dividend version of UBI, that traces back to the intellectual traditions of George (the Georgist) and Paine (the Paineite), viewing the surplus generated by AI as a socially produced rent to be allocated to all members of society. There is also a post-Keynesian case for UBI, in that it would function to maintain effective demand in times of economic downturn (Srnicek and Williams, 2015). They site UBI as a means to support a post-capitalist society where income is decoupled from work, in order to support a fundamental transformation of society in which the wage relation is transcended. Experiments are increasingly conducted to test the theoretical framework of UBI, such as the Finnish Basic Income Experiment (BIEX, 2017–2018) that provided a basic income to 2,000 unemployed individuals. In terms of wellbeing, BIEX found modest positive effects. It found no significant effect on labor supply but did find slightly better employment outcomes than in the control groups of the experiment (Kangas et al., 2019). A similar effect on employment was found for recipients of Basic Income in the Stockton SEED program in California (2019–2021), in addition to increased full-time employment and reduced income volatility (West, and Castro, 2023). The large-scale randomised controlled trial of GiveDirectly in Kenya (Haushofer, and Shapiro, 2016) found that recipients' asset values, consumption, and household income increased in the nine months after the transfers. Although the experiments reviewed above have considerable value at partial equilibrium, they do not allow for an assessment of the general equilibrium effects in a macroeconomic setting of universal implementation of UBI.

3. Results and Discussion

First, there is the channel of capital deepening: As with other capital, the deployment of AI systems to raise labor productivity will increase the capital-labour ratio. Then, as in the case of other factors of production, there will be an increase in labour productivity, given that the other factors (which are, by assumption, held constant) remain unchanged. The resulting total output can then be analyzed further to determine the extent to which Total Factor Productivity (TFP) has increased in addition to the gains from capital deepening. And, in addition to these two channels of influencing productive capacity, there is also the possibility of a dynamic effect. For, in addition to the enhanced use of the existing stock of capital (as in the case of other forms of capital), the introduction of AI can also facilitate an increase in TFP by more speedily coming up with novel hypotheses for testing, speeding up the process of experimentation, and facilitating the codification of knowledge. The distributional effects of all three channels through which AI can enhance economic output—capital deepening, TFP, and dynamic innovation—depend heavily on the structure of ownership of capital that is being used by AI. In other words, if the owners of AI capital are mostly a diffuse set of owners of pension funds, of sovereign wealth funds, or of cooperative enterprises then the increased productivity of the existing stock of capital will translate into increased economic output for all of the distribution of income. However, if the owners of AI capital are mostly a small group of technology firms and a small group of very rich individuals then the TFP increase in the output of capital will lead to a massive shift in the functional distribution of income from wages and labor to capital income. Since the production functions of many service activities have not yet increased in efficiency through the use of AI, growth in total factor productivity (TFP) for the whole economy has not yet increased.

Several explanations are possible. The first is that there are a series of 'complementarities' which need to be put in place, to extract high productivity gains from the use of AI. These are major restructurings of organizations; the retraining of workers; changes in regulations to enable use of AI in a safe and transparent manner. While these may be installed in short order, there will be large lags as they work their way through the system. A second possibility is that the rising output of digital services has so far not been properly measured by existing national accounts and this 'black box' is at the frontier of a few big firms. A third possibility is that the current vintage of AI systems are not yet general-purpose technologies but rather incremental improvements to existing capital. How large are the AI-driven productivity surpluses going to be in the economy as a whole? In other words, will they materialize at all? The answer to this question is far from clear and is currently experiencing strong acceleration in its diffusion through the form of generative AI. If they do in fact materialize, the distributional implications of AI are then an urgent question of considerable importance; if not then the related fiscal space to consider UBI is severely weakened. A key economic fact about advanced economies has been the declining labor share of national income, from about 65% in the early 1980s to less than 58% in the OECD average (Dao et al., 2017, 1). The causes of this decline are well known and pre-date the current phase of AI. There is, however, good reason to expect that in the near term, automation will drive the labor share down further, as productivity gains translate into increased capital income. Furthermore, as highlighted by Karabarbounis and Neiman (2014) the falling labor share has gone hand in hand with a decline in the relative price of investment goods—i.e. capital deepening—something we would expect from increased productivity enabled by automation. The share of labor in national income is thus the single most important economic fact to understand the distributive implications of AI, and the basis for a UBI as a redistributive measure. The case for using UBI as an instrument of distribution to capture the gains from the further rise of AI productivity proceeds along three grounds: the surplus, the incidence, and the mechanism. The first grounds the case on the size of the economic surpluses that can be captured with a minimum of deadweight loss to fund an unconditional income floor for all citizens. The incidence grounds the case for using UBI on the distributional consequences of the economic surplus generated by the further rise of AI productivity: it is to be captured by owners of capital, leading to further increase in wealth inequality between owners of capital and labor. The mechanism grounds the case for UBI over and above other means-tested social cash transfers on the grounds of greater efficiency and justice in the face of the considerable administrative costs of other forms of social transfers. One other argument to consider is that there is a lot of productive potential in the stock of knowledge that has been collectively produced by all members of society including language, all scientific discoveries, all cultures, all arts, etc. This is the knowledge that AI systems are trained on. So in some sense the surplus value produced by these systems is a form of rent on this common inheritance. Thus every citizen would have a legitimate claim to a share of this collectively produced technological surplus, and so a justice-theoretic basis for UBI that is independent of any attempt at consequentialist welfare maximisation. This theory of the state is associated with a number of older ideas about the common resources of natural, intellectual and technological wealth that could be guarded by the state on behalf of its citizens. There is an active program of the distribution of returns from the sovereign wealth fund of the Alaska Permanent Fund to all residents of the state since 1982 (Jones, and Marinescu, 2022). To summarize briefly: From a post-Keynesian perspective, UBI can also function as an automatic stabilizer and so increase aggregate demand in an economy where the wage bill is being decreased by automation because it has a high income multiplier among the recipients who are primarily low-

income. So it can counteract the decrease in aggregate demand due to income concentration caused by automation. The above three perspectives thus all suggest that the welfare loss due to AI-induced inequality could be greater than the gains to individuals from more leisure, if the gains to individuals from more leisure were not offset by negative external effects such as reduced aggregate demand due to income concentration caused by automation. Therefore, from a purely economic perspective, the most important purpose of UBI in an AI economy is to act as an automatic stabilizer. Although the disincentive effect on labor supply is the most persistent argument against UBI, it is not a strong objection in the context of the rising structural underemployment in an AI-driven labor market. The reduction in labor supply on the part of workers with UBI is likely to be small, both in terms of absolute numbers and as a share of labor supply. This is especially the case in a scenario in which the UBI is set at a moderate level in order to achieve its redistributive purposes. Moreover, for structural underemployment in an AI-driven economy, a small reduction in labor supply by some workers could be socially beneficial. It could allow for work-sharing in order to maintain employment of all who wish to work and enable others to increase their leisure time and engage in nonmarket activities of value. Thus, there is no reason to consider the disincentive effect as a strong objection to UBI in an AI-driven economy. Much of the evidence, however, does not show any significant reduction in labor supply at UBI levels that are considered to be 'moderate'. There is also a new and significant structural underemployment in labor market. As a result of AI, there is the possibility that even a marginal reduction in labor supply could be socially beneficial in compensating for other labor supply shortfalls, and allowing people to work less while consuming as much as before, or more, through productively using more leisure time to engage in non-market productive activities and in other activities that raise their human capital. A second set of concerns regards the potential for UBI to fuel inflation. The money-financed version of UBI is likely to have some degree of inflationary impact, as it represents additional aggregate spending by recipients with high MPCs (consumption out of income). A tax-financed version of UBI would have a similar net effect on aggregate spending if the taxes are levied on households with high incomes and low MPCs (such as the top 10% of households in many countries), and the transfers go to households with low incomes and high MPCs. In supply-constrained local markets (e.g., for housing and for certain services), this could manifest as higher prices. But this would be offset by greater-than-proportional growth of supply as productivity rises with AI. But there are problems with use of UBI as a replacement for existing benefits. From a progressive left viewpoint, the level of UBI required to make a reasonable difference in living standards is likely to be above the poverty line for most countries. But a benefit above that level for all would be expensive and most would not need it. The level of existing means-tested benefits for different groups with special needs (the disabled, the elderly, single parents etc.) is generally set with reference to their needs. Categorical benefits are likely to be more efficient than UBI of the same cost. The equivalence rating of benefits is a measure of the worth of non-cash and in-kind benefits in terms of their purchasing power for consumers. For a given level of total benefit expenditure, a system of means-tested, non-universal cash and in kind benefits is likely to generate a more equal distribution of equivalent benefit expenditure than a system of universal cash benefits. The distributional consequences of different ways of financing a given level of UBI also need to be considered. A particularly pressing issue for the left is, however, the unequal distribution of risks from automation, as well as the differing needs of citizens with different ages, health conditions, education levels, family situations, geographical location etc. Treating all citizens equally by distributing a constant sum, no matter how it is distributed, will necessarily fail to address the specific needs of individuals

with greater requirements. While UBI as a universal program has the advantage of generating cross-class alliances stronger than those generated by targeted programs, it is likely to generate intense pressure to cut the benefit in the face of any fiscal constraint, such as a recession. In such a context the institutional sustainability of a UBI set at a sufficient level to be a true floor against the risks of AI-induced precarity is far from guaranteed. In addition, the political acceptability of the required taxes and tax reforms to fund UBI, including above-average taxes on capital and possible "robot levies," is likely to face intense opposition from concentrated economic interests with disproportionate political power to block the policies that impinge upon their interests—drawing on the theory of extractive institutions (Acemoglu, and Robinson, 2012). A more convincing theoretical case for the robot tax has recently been set out by Guerreiro, Rebelo and Teles (2022). They show that during the transition period between now and the time when all workers with experience of work in routine occupations have retired a temporary tax on robots could have a positive welfare effect. The key point is that as the automation cost falls the inequality it amplifies is also shifted. As such the optimal tax on robots would fall to zero once all workers with experience of work in routine occupations have retired. A robot tax can function as a corrective Pigouvian tax to deal with two externalities of automation of a fiscal and social nature that are not fully internalized by the firms undertaking it: fiscal erosion and an increase in unemployment and in the number of people on benefits. One major theoretical objection to the taxation of robots is the problem of allocative distortion. If the productivity gain from a robot is positive then by definition there must be be some level of robots that is socially optimal. But then taxation of robots at the margin would reduce the level of robots in the economy below the social optimum. Acemoglu and Restrepo (2020) develop a detailed welfare analysis of the taxation of robots. Their results show that whether or not the taxation of robots is welfare improving depends on whether or not the level of automation in the economy is excessive (i.e. above the social optimum) or not. The capital dividend model is that of Atkinson (2015). Under this model, the public sovereign wealth fund is capitalized by means of a progressive tax on wealth, by a technology firm issuing shares to the public, or by the proceeds from natural resources. Returns on the investment in the fund are distributed to all citizens as a universal dividend. Some examples of such funds include Alaska's Permanent Fund, Norway's Government Pension Fund Global, and Singapore's Temasek Holdings. There are several interesting examples of institutions today that operate according to the capital dividend model such as the Alaskan Permanent Fund, Norway's Government Pension Fund Global and Singapore's Temasek Holdings. While these examples offer a good site for such an experiment, there are several theoretical and practical difficulties with the model of a capital dividend, particularly in relation to the required scale of funds to make any difference and the important issue of governance to keep such a fund off for periods of time from speculative activity. There is also support for funding UBI through a Value-Added Tax (VAT), first proposed by Yang (2018). Such a tax is technologically neutral in that it will charge the same amount of tax on goods and services regardless of whether they have been produced using AI. Yang believes a VAT is an appropriate form of taxation in a high-tech economy because it will charge a constant percentage of the value added to a product at each stage of production. Importantly, it is consumption-based so that it will fall on the final purchaser of a good rather than on the factors of production. This means that a robot tax, for example, would decrease the price of investment goods and thus lead to an increase in the capital-labor ratio. In contrast, a VAT would leave investment goods prices unchanged and therefore would not reduce the incentive to invest. He notes, however, that such a tax would be regressive in that it would take a larger share of income from poor individuals than

from rich ones. But this problem could be alleviated by exemptions from the tax on certain goods that the poor tend to purchase, by zero-rating (i.e., charging no tax) on necessities, and by allowing for certain income tax reductions (Atkinson, 2015). Much more recent are the 'post-work' arguments of automational affluence that are being developed within a variety of contexts, above all that of generational conflict, the 'crisis of work' (Bastani, 2019). Within such post-work frames, the proposals under consideration to deal with the massive impact of worklessness that is now going to be caused by technological automation of workplaces — i.e. a Universal Basic Income (UBI) — are seen to have the potential to create the basis for a fundamental change of direction in the contemporary social order as a whole — to make possible a complete transition from a 'work society' (Gorz, 2001) to a fully 'post-work' social model (Pariser, 2015). This Post-Work perspective of UBI is theoretically based on the alternative social form of development that challenges the classic heterodox views of the abundance of capital (such as that of Marx in the Grundrisse) and the criticism of the work society (Gorz, 2001). Contemporary versions of the Post-Work approach of UBI are conversant with issues of sustainability. They link the decoupling of human activity from labor in an AI-driven economy to reduced environmental throughput in order to examine whether growth can continue to be sustainable. There are, however, several important issues that need to be addressed in this framework, such as: 1) the AI's productivity dividend may not materialize at the pace and extent expected by its supporters; 2) the distribution of the AI-driven surplus to the citizens would likely to face opposition by powerful classes; and, 3) in this framework unpaid care and reproductive work would not receive the value and would not be distributed that they deserve. As Fraser (2016) pointed out, in this framework, human activities that are not generated by the market would not receive the value they deserve and thus they would be compromised by the AI-driven and UBI-supported productive activities. A middle-of-the-road approach views the interaction between UBI and AI as the basis for a so-called „dualist economy" (Gorz, 2001) that complements a highly productive market economy with a rich and diverse non-market realm of action in which people can organize themselves as much as they want. That UBI is used to make this possible is more or less incidental.

CONCLUSIONS

This paper sets out an exploration of the debate within the theoretical fields of AI-driven productivity and UBI as a redistributive device. The implications of the various arguments within the specified fields have been explored across several different theoretical paradigms and analytical structures. The theoretical case for UBI as a tool to redistribute the generated by AI to capital, labor and other claimants is coherent and sits within several traditions in economics, philosophy and post-keynesian economics on issues of welfare, distribution, work and demand. Decline in labor share, concentration of capital that owns AI, and the demand-side implications of its deployment require a new structural distribution tool. UBI has advantages over traditional benefits in terms of universalism, administrative cost, and in avoiding welfare 'traps'. Furthermore, there are four main theoretical obstacles for UBI, which however are not insurmountable, but rather they need to be designed around: the issue of sufficient financing, the danger of substituting UBI for already existing means-tested benefits, the risk of inflation, and the problem of political sustainability. The normative evaluation of UBI for enabling work in a world with exponentially increasing AI productivity therefore cannot be separated from a broader set of issues around the democratic governance of technological change and the establishment of adequate institutional structures for a fair transition to AI. The really big question for all of us today is: Will we manage to set up adequate governance and political coalitions to fairly

distribute the enormous productive surpluses that AI will surely produce, before they bring about a structural disruption to the social contract of democratic capitalism? One theoretically well-founded approach of how to deal with these enormous future challenges is the introduction of UBI. But there are many more approaches and the task of researchers is to detail and test both the theoretical frame as well as the effects of UBI, in order to be able to make better decisions on the basis of the best available knowledge instead of on the basis of dogmatic prejudices.

REFERENCES

Acemoglu, D., 2021. Harms of AI. *NBER Working Paper* No. 29247. National Bureau of Economic Research.

Acemoglu, D., and Restrepo, P., 2019. Automation and new tasks: How technology displaces and reinstates labor. *Journal of Economic Perspectives*, 33(2), 3–30.

Acemoglu, D., and Restrepo, P., 2020. Robots and jobs: Evidence from US labor markets. *Journal of Political Economy*, 128(6), 2188–2244.

Acemoglu, D., and Robinson, J. A., 2012. *Why Nations Fail: The Origins of Power, Prosperity and Poverty.* Random House.

Arntz, M., Gregory, T., and Zierahn, U., 2016. The risk of automation for jobs in OECD countries: A comparative analysis. *OECD Social, Employment and Migration Working Papers* No. 189. OECD Publishing.

Atkinson, A. B., 2015. *Inequality: What Can Be Done?* Harvard University Press.

Autor, D. H., Levy, F., and Murnane, R. J., 2003. The skill content of recent technological change: An empirical exploration. *The Quarterly Journal of Economics*, 118(4), 1279–1333.

Bastani, A., 2019. *Fully Automated Luxury Communism*. Verso Books.

Dao, M. C., Das, M., Koczan, Z., and Lian, W., 2017. Why is labor receiving a smaller share of global income? Theory and empirical evidence. *IMF Working Paper* No. WP/17/169. International Monetary Fund.

Eloundou, T., Manning, S., Mishkin, P., and Rock, D., 2023. GPTs are GPTs: An early look at the labor market impact potential of large language models. *OpenAI Working Paper.*

Fraser, N., 2016. Contradictions of capital and care. *New Left Review*, 100, 99–117.

Frey, C. B., and Osborne, M. A., 2017. The future of employment: How susceptible are jobs to computerisation? Technological Forecasting and Social Change, *Elsevier*, 114, 254–280.

Gorz, A., 2001. Farewell to the Working Class: An Essay on Post-Industrial Socialism. Pluto Classics Series.

Gough, I., 2019. Universal Basic Services: a theoretical and moral framework. *LSE Research Online Documents on Economics 101051, London School of Economics and Political Science*, LSE Library.

Guerreiro, J., Rebelo, S., and Teles, P., 2022. Should robots be taxed? *NBER Working Papers* 23806, National Bureau of Economic Research, Inc.

Haushofer, J., and Shapiro, J., 2016. The short-term impact of unconditional cash transfers to the poor: Experimental evidence from Kenya. *Quarterly Journal of Economics*, 131(4), 1973–2042.

Jones, D., and Marinescu, I., 2022. The labor market impacts of universal and permanent cash transfers: Evidence from the Alaska Permanent Fund. *American Economic Journal: Economic Policy*, 14(2), 315–340.

Kangas, O., Jauhiainen, S., Simanainen, M., and Ylikännö, M. (Eds.)., 2019. *The Basic Income Experiment 2017–2018 in Finland: Preliminary Results*. Ministry of Social Affairs and Health.

Karabarbounis, L., and Neiman, B., 2014. The global decline of the labor share. *Quarterly Journal of Economics*, 129(1), 61–103.

Lavoie, M., 2015. *Post-Keynesian Economics: New Foundations*. Edward Elgar.

Piketty, T., 2014. *Capital in the Twenty-First Century*. Harvard University Press.

Srnicek, N., and Williams, A., 2015. *Inventing the Future: Postcapitalism and a World Without Work*. Verso Books.

West, S., and Castro, A., 2023. Impact of Guaranteed Income on Health, Finances, and Agency: Findings from the Stockton Randomized Controlled Trial. *J Urban Health*. 2023 Apr;100(2):227-244. doi: 10.1007/s11524-023-00723-0. Epub 2023 Apr 10. PMID: 37037977; PMCID: PMC10160253.

Yang, A., 2018. *The War on Normal People: The Truth About America's Disappearing Jobs and Why Universal Basic Income Is Our Future*. Hachette Books.

PROMOTING INNOVATIVE PRODUCTS IN THE AGRICULTURAL BUSINESS ENVIRONMENT AND EDUCATION FOR DIGITALIZATION: AN ANALYSIS OF THE CURRENT CONTEXT AND SOCIO-ECONOMIC IMPACT

CZU: [631.1:004]:378(498)
DOI: https://doi.org/10.53486/tids2026.16

MIOARA MIHĂILĂ
”Ion Ionescu de la Brad” Iași University of Life Sciences
e-mail: mioara.mihaila@iuls.ro
ORCID ID: 0000-0002-8185-0976

ANDY-FELIX JITĂREANU
”Ion Ionescu de la Brad” Iași University of Life Sciences
e-mail: andy.jitareanu@iuls.ro
ORCID ID: 0009-0002-2654-6813

ANDROMEDA SONEA-PĂTRAȘCU
”Ion Ionescu de la Brad” Iași University of Life Sciences
e-mail: andromeda.sonea@iuls.ro
ORCID ID: 0000-0002-0442-6370

TATIANA BALTAG
”Ion Ionescu de la Brad” Iași University of Life Sciences
e-mail: tatiana.baltag@iuls.ro
ORCID ID: 0009-0007-5726-9456

DAN BODESCU
”Ion Ionescu de la Brad” Iași University of Life Sciences
e-mail: dan.bodescu@iuls.ro
ORCID ID: 0000-0002-2133-6633

Abstract. The transition to digitalization is a current reality present in all areas of economic and social life, including education and the business environment. Agriculture, pillar of economic development, is facing the challenge of adopting the components of digitalization. This is a transition that involves the need for specialists. Current students in the field of agriculture are the future entrepreneurs on whom the adoption of modern technologies and innovative products in their future professional activity depends. This paper aims to outline the profile of future entrepreneurs in agricultural business, from the perspective of their openness to use the digitalization components, innovative products and high-performance technologies in the agricultural business environment. Depending on the profile, the market for the delivery of innovative agricultural products, modern technologies and digitalization components will promote programs so that the results are mutually beneficial. The basic research question is the following: what do future entrepreneurs in agriculture look like in terms of openness to digitalization and what are the determining factors of the adoption of innovative products in agricultural businesses. The research, of a quantitative-descriptive nature, uses as its basic method the ssurvey based on a questionnaire, respectively investigation and synthesis of specialized literature. The subjects, from whom 235 responses were collected, are students of agriculture. The results indicate a great openness towards the adoption of digitalization components, the basic motivations being very objective: costs, results, profit, emphasis on promotion through demonstrations in use, tests, certifications, experiences of other users and less

social media networks. In this way, a program can be developed to train and educate young people for the adoption of modern technologies and innovative, digitalized products in their future professional activity.

Keywords: agricultural business, digitalization, education, promotion, technologies, innovation.

JEL Classification: I25, O15, O33, Q13.

INTRODUCTION

The economic world and human society, in their evolutionary process, are in constant transformation. Currently, we are witnessing the transition - at a rapid pace - to digitalized systems usable in all specific areas of economic development, including agriculture. The current context of the adoption of digitalization indicates promises of performance and superior-level results, sustainable and capable of satisfying consumer needs that have become not only more numerous, but also more refined. All areas of socio-economic life are marked by a profound transformation in innovative and technological terms, and current generations are responsible for how to implement these changes. The transition is proving to be rapid and materialized in the adoption of ultra-modern, high-performance technologies based on digitalization, and the agricultural business environment is no exception to this transformation. For the national economy, it is vital that the implementation of high-performance technologies, digitalized systems and innovative products be supported not only financially, but also by well-trained human resources. Agriculture, a basic branch of the national economy is in the process of adapting because only in this way can it register performance and competitiveness. Innovative products are a more general concept that includes: digital technologies, digital agriculture systems, new inputs, equipment and machinery, modern agricultural practices.

The future entrepreneurs in the Romanian agricultural sector are the current students specializing in agriculture and related fields. This is a main argument for which it is required that they be prepared both in the field in which they have chosen to specialize, and in terms of the pace of adaptation and openness to the new elements offered by modern, innovative agricultural technologies and products. From the point of view of age, the current students and future entrepreneurs in agriculture belong to generation Z, which has a much different profile than previous generations. This is one of the reasons that led to the development of this work: knowing the profile of young people from generation Z, the future specialists who will decide on the adoption of new processes and technologies in the agricultural field, in the direction of ensuring the performance and results expected by the consumer market. The profile of the generation on which the future of sustainable, high-performance and digitalized agriculture depends should not be neglected, but known in detail.

We are interested in this analysis primarily because the performance of the agricultural economy will depend on them, and today's young people must be prepared and trained to support a digitalized and modern agriculture. Therefore, this paper is dedicated to a topic of major interest for forecasting studies on the agriculture of the future, supported by digitalization and innovation. The subject proposed for analysis is: the professional profile of the generations that will work in agriculture, considering current students in specialized specializations. In pop-marketing terms, future employees in the agricultural sector will be recruited from two current generations: generation Z, i.e. people born between 1997 and 2012, and generation Alpha, i.e. people born between 2013 and 2020 (Chaney et al., 2017). Generation Z is characterized as being natively digital, accustomed to technology since childhood, focused on virtual identity and experts in rapid communication. The Alpha generation is represented by the children of the Millennials generation, the smallest category of the population, due to the decrease in the birth rate; this is the first generation that was born exclusively in the era of smart

technology and future artificial intelligence. The specialized literature will be supplemented with this topic, considering that the relationship between the profile of future entrepreneurs and digitalized agriculture deserves to be brought to the forefront.

The supporting question of the research is: what do future entrepreneurs look like in digitalized agriculture and what are the directions they adopt in the educational process of digitalization. The research started from the assumption that the profile of young agricultural students is appropriate for the transition to a modern agriculture, young people being prepared to adapt to the requirements of digitalization and eager to adopt innovation in future agricultural businesses. The relevance of the research is not only theoretical, but also has multiple practical facets.

The novelty of the work consists in bringing to the forefront the new and modern concept of digitalized agriculture, with an emphasis on agricultural innovation, considering one of the most accessed components of the marketing mix - promotion. It is already recognized that innovative products and technologies based on digitalization, usable in agriculture, need an appropriate and field-specific strategic promotion. The local literature on this subject is quite limited, although the current socio-economic context indicates major trends of accelerated orientation towards digitalization and re-technologizing. Especially on the topic of identifying connections between marketing strategies of digitalized agriculture and the profile of users of innovative agricultural products, deficiencies were noted in the specialized literature. The basic approaches in the literature mention that the availability of an innovation does not guarantee its adoption in practice (Rosario et al., 2022) and, even more so, in agriculture the decision to use new products is influenced by the perception of utility, costs, risks, compatibility with current activity, ease of use (Chiriacescu, 2024). Moreover, in the agricultural sector, direct experience, practical demonstration and assessment of economic consequences prevail, agriculture being a pragmatic and objective field (Nagel et. al, 2025; Fahmi, 2020), therefore the way in which a digitalized product is presented, through promotional actions, can significantly influence the willingness to consider it (Addorisio et al., 2025).

We argue the purpose of analyzing the profile of the future entrepreneur in digitalized agriculture including the fact that, based on the analysis of documentation from newly published informative materials on digitalization, confusions were noted between the use of devices or access to social media and the actual transition to digitalization, as the basis for supporting performance in agricultural entrepreneurship. In addition, very easy access to information does not guarantee the use of this information for productive purposes.

MAIN CONTENT

1. Materials and Methods

The relationship to digitalization and innovation has been and remains a purely practical, rational aspect, therefore the analysis of professional development in the digital era is a priority, including for the research environment. In a comprehensive study by Sofianu & Dumitru (2023), the following relevant aspects were highlighted regarding the preparation of future specialists for the adoption of digitalization in the fields of the economic environment:

- there is a significant gap between the skills held by the current labor market and those needed for the future entrepreneurial market;
- 23% of existing jobs will undergo substantial changes in the conditions of the rapid transition to the digitalized environment;

- it is estimated that by 2027, 6 out of 10 employees will need to retrain and improve their skills, so as to cope with the new requirements in the field;
- the categories of skills targeted for improvement are the skills already held and relatively easily usable, such as technical "hard" skills and digital skills, data analysis and foreign languages; to these are added the skills of "soft" area, namely critical thinking and emotional intelligence;
- skills that are in urgent and urgent need of improvement are those that have emerged recently, which are related to artificial intelligence given that only 35% of the current labor market is prepared, and only 25% of employees are prepared for new green technologies.

Another topic of real interest connected to the profile of future entrepreneurs prepared to adopt digitalization in professional fields is that of transformative artificial intelligence, which is considered not to lead to the disappearance of jobs, but to their reinvention (World Economic Forum, 3035). In this context, skills necessary in the future to cope with artificial intelligence in conditions of performance and success are: critical and analytical thinking, flexibility and the ability to select information. Romania is in a position to accelerate the transition to digitalization by ensuring and improving skills, which is a solid reason for young people to be prepared so that digitalization is not confused only with easy access to devices and virtual social networks. According to European Commission data (2023), in Romania basic digital skills are valid for only 28% of the active population, compared to 83% in the Netherlands and 82% in Finland. The expectations of young students, future employees or entrepreneurs who will build and maintain the business environment, are to develop professionally and advance in their careers, to explore new fields of activity, but also to develop personally. The motivations for these aspirations are: the interest in acquiring new professional skills, career advancement, access to secure and profitable fields of activity. The factors that influence the adoption of digitalization components in the agricultural business environment in Romania are: economic-financial, cognitive-informational and social-educational.

The main purpose of the paper is to analyze the openness and interest of current students for the components of digitalization that they will use in their future activity. Given that promotion is connected to the profile of the consumer segment, we used criteria to identify this profile. The objectives of this paper are: O1. Identifying the profile of future specialists in agriculture based on digitalization; O2. Highlighting the role of promotion in the successful transition to digitalized agriculture; O3. Identifying the directions that must be followed in the education process in order to best prepare future entrepreneurs who will work in the agricultural field connected to digitalization.

The research is quantitative in nature, and the basic method used is the survey conducted with the questionnaire instrument that was applied to a sample of 235 respondents. The research universe is limited to students in the field of agriculture. The working variables that supported the questions in survey are: decision-making factors in digitalization in the future profession, factors influencing the decision to use innovative products in agricultural businesses, mentality regarding digitalization, perceived advantages as a result of using digitalization in the future profession, openness to learning and accumulating new information regarding digitalized agriculture. The variables were supported by confirmatory pivots such as: previous experience in working with modern technologies, information sources used to learn about digitalization, trust in new technologies, openness to using digitalized tools, motivation, risks. The questionnaire was structured, with questions grouped into sections: framing the profile of future entrepreneurs in agriculture, perceptions regarding digitalized agriculture, behaviors towards education for digitalization.

2. Results and Discussion

In order to identify the profile of future entrepreneurs in agricultural businesses, considering students preparing for this purpose, the survey followed several parameters, the results of the responses of which will be presented below. The main reference parameters are: the specialization in which the young people study (Figure 1), experience in agricultural business, availability for education for digitalization, motivation for adopting and using digitalization components, perception of information sources about the products and technologies they will use in the future, preferred and appreciated innovative and digitalized products, attitude towards the risk of using these digitalized technologies and trust in promotional programs to stimulate the use of these innovative products and technologies.

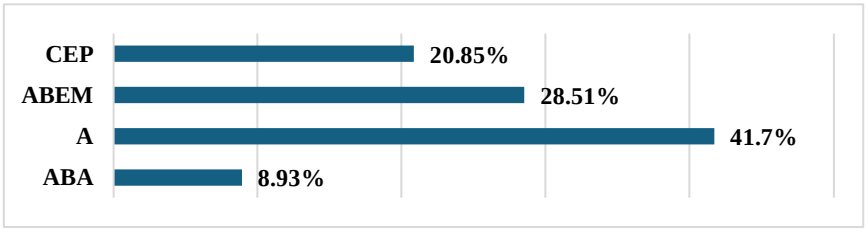


Figure 1. Subject specialization – students in the field of agriculture
Source: *processing of survey database*

It can be seen that most participants (41.7%) are from the Agriculture (A) specialization and the fewest (8.93%) from the Master of Agricultural Business Administration (ABA). In a balanced proportions are the participants from Agricultural Business Engineering and Management (ABEM) and Consumer and Environmental Protection (CEP) of 28.51% and 20.85%, respectively. The survey also indicated the following proportions of experience with agricultural businesses: 66.80% come from families with agricultural businesses, and 33.19% did not have such experience or involvement.

The answers related to the openness to digitalization in agriculture are presented in Figure 2.

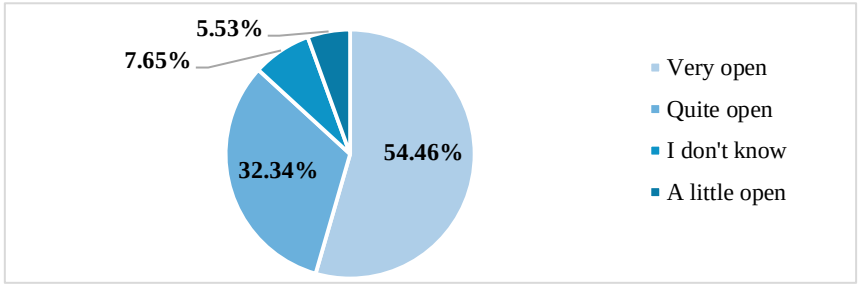


Figure 2. Readiness and openness to adopting digitalization in agricultural businesses
Source: *processing of survey database*

It can be noted that over half of the student respondents (54.46%) declare themselves very open to adopting innovative technologies and products in their future profession involving agricultural business. Just as many, over 32%, declare themselves quite open, so a high degree of openness towards new technologies, digitalization and innovative products in agriculture is for 86.8% of the respondents. Those who declare themselves a little open are only 5.53%, an aspect correlated with the profile of generation Z (curious, with initiative, with native skills in the field of digitalization and technology), while 7.65% declare that they "don't know", this indecision can be interpreted as insecurity, distrust, lack of knowledge of the field or it may be a lack of interest.

Figure 3 indicates the results regarding the motivation to adopt digitalization components in their future agricultural businesses.

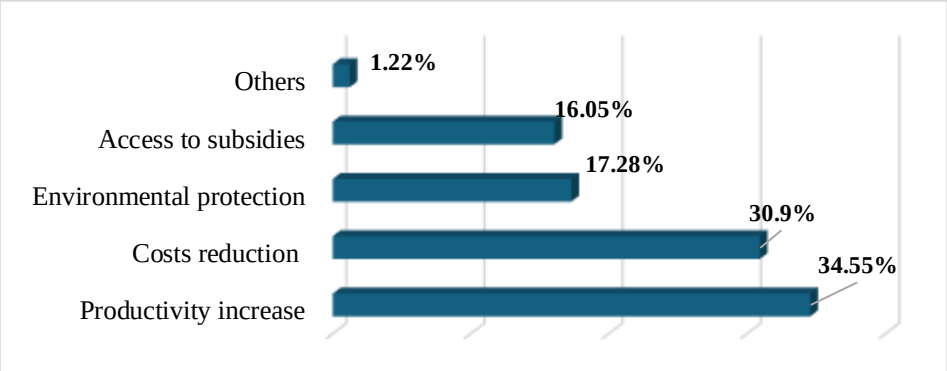


Figure 3. The motivation for adopting various components of digitalization in agriculture
Source: *processing of survey database*

From Figure 3 it can be noted that most respondents, 34.55%, are motivated by increasing productivity and just as many, 30.9%, by reducing costs. These answers indicate the pragmatism and objectivity that respondents demonstrate when deciding to adopt new technologies, innovative products and digitalization in agriculture. Relatively high percentages, but still in second place, are given by motivations such as environmental protection (17.28%) and access to subsidies (16.05%).

Regarding the attitude towards risk in adopting the components of digitalization of agriculture, 51.16% declare that "I don't know", a rational aspect given that the risk should be analyzed in a specific context, namely because these components are not yet fully and concretely known. 17.44% say they feel they risk “a lot”, almost 6% say they risk a lot, and 21.51% say they risk “a little”, while 4.06% say they “do not risk at all”.

For the appreciation of the usefulness of digitalization components in Romanian agriculture, 77.30% are supporters of digitalized agriculture, and 5.81% are rather reserved about these, considering that it is possible to work well without them.

Figures 4 and 5 show the sources of information and promotional content that respondents appreciate, trust and feel influenced by in terms of adopting innovative and digitalized agriculture.

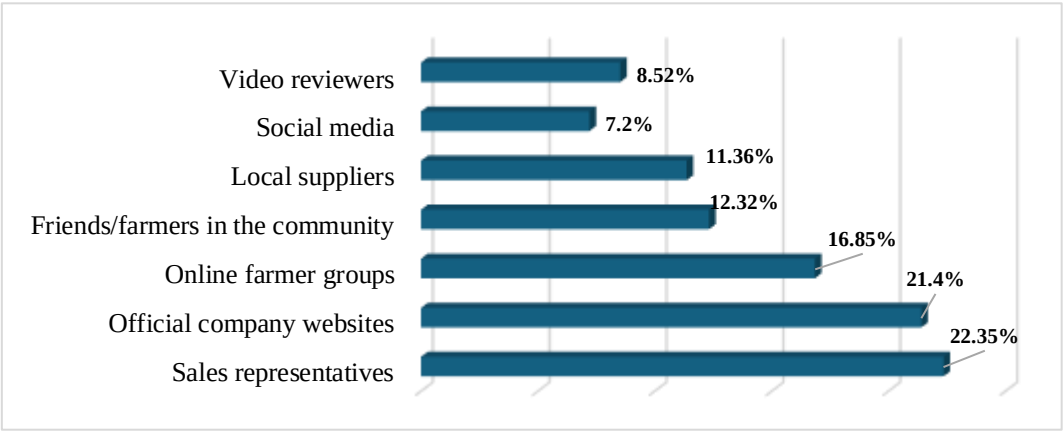


Figure 4. Agreed sources of information regarding the adoption of innovative technologies
Source: *processing of survey database*

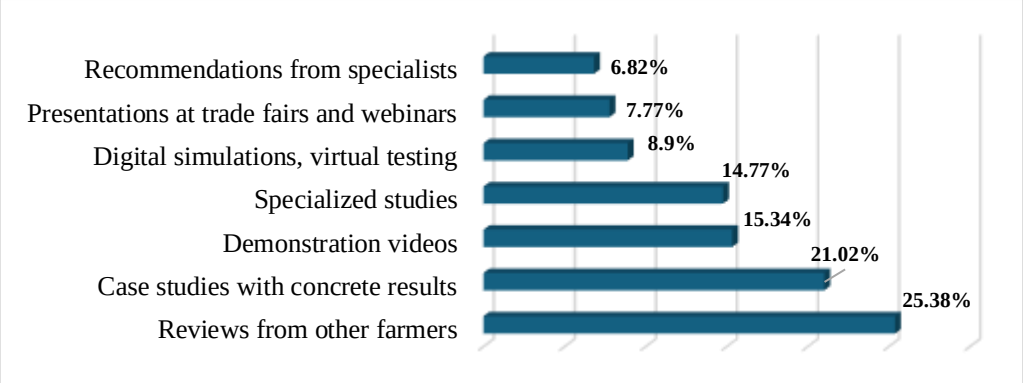


Figure 5. Promotional content that influence the decision to adopt digitalized agriculture
Source: *processing of survey database*

Regarding the probability that in the future of agricultural businesses in which they will be involved, to adopt and use new innovative, digitalized products and technologies, almost half of the respondents, 48.08%, say that it is very likely, 37.02% say that it is probably, 11.06% do not know and 3.82% unlikely.

The types of digitalization components that future entrepreneurs in agriculture like, these are shown in Figure 6.

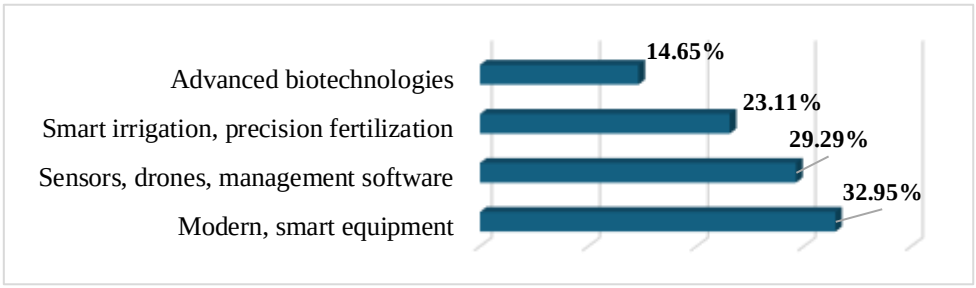


Figure 6. Components of digitalized agriculture agreed and appreciated by respondents
Source: *processing of survey database*

Regarding trust in marketing programs that promote new digitalized technologies and innovative products for agriculture, the results indicate the following opinions of the respondents: most, 26.57%, trust practical demonstrations and prior testing, respectively 20.73% trust testimonials and evaluations of other users. A very high percentage, 19.44% appreciate product certifications, respectively 17.49% appreciate details with technical data of innovative products and technologies. 15.76% of respondents trust in the economic results already obtained by other users.

In general, from the analysis of the results presented above, it can be observed that predominantly young students, future entrepreneurs in agriculture, are as open as possible to the idea of digitalized agriculture and are excited by the means of promoting innovative products and technologies that would bring benefits and high-performance results. Regarding the motivation for using the components that support the digitalization of agriculture, it is observed that the respondents are pragmatic, objective and focused on concrete and quantifiable aspects such as productivity and implementation costs.

Regarding risks, it seems that, not knowing these components in detail, they cannot express the degree of risk or perhaps cannot establish it only based on assumptions. Regarding information sources, it is very interesting that here too they are very anchored in concrete elements, they are

circumspect, that is, they prefer reliable, official and professional sources. It is very interesting to note that they are not very influenced by online promotion or are not impressed by it, and a very high degree of pragmatism is noted for promotional content.

They are not very impressed by social media advertisements, which indicates a high degree of objectivity or selectivity of information. They also do not express great trust in digital applications, which correlates with questions that emphasize information, clarity, source of information, so if they do not know the situation well, they do not express themselves because they do not have a concrete framework for orientation.

CONCLUSIONS

The state and evolution of Romanian agriculture are topics of real interest for the analysis of the transition to digitalization, as they represent basic pillars in supporting the current and future national economy. Currently, Romanian agriculture operates in a framework marked by some gaps in the modernization and adaptation process to digitalized agriculture, based on innovative products and high-performance technologies. In principle, with some exceptions, the pace of adoption of new technologies and digitalization is relatively slow in Romanian agriculture. That is why it is extremely important to monitor who the future entrepreneurs in national agriculture are and what their profile is, considering the current generations of students in the field.

Through the research carried out and the results obtained, the paper contributes to bringing to the forefront the profile of the generation of agricultural students from multiple perspectives: openness to digitalization, risk-taking, objectives pursued, intentions to adopt innovation in agriculture, position towards financial investments in relation to the results obtained.

The general profile indicates openness, caution, focus on objective results, attention to investment costs by reporting to expected results, limited trust in uncertain information sources and risk taking only under conditions of certainty or possibility of controlling the situation.

Considering a set of assumptions in accordance with which young people from Generation Z are less attentive to the details of their future profession, these are contradicted by the results of the survey. Even if there are major gaps in the critical analysis regarding the selection of information usable in professional activity, young people can be directed in this direction through complex education programs for digitalization. We recognize that the economy of the future depends on investment in digitalization and access to innovative products, and performance and progress depend greatly on marketing strategies that promote digitalization and innovation in agriculture.

Promotion is a widely used concept, but not always in the right sense. In terms of promoting the products that are part of digitalization, the results indicate that young people are prepared to receive messages and promotional actions that demonstrate the usefulness of the investment, reduce uncertainty or illusion, and confirm the practical validity of the results of implementing digitalized technologies in agriculture. Young people expect credibility, results, and unintended risks.

Therefore, it is necessary to give due consideration to the intended purpose, the profile of future entrepreneurs in agriculture and how they are prepared, an aspect that can be implemented by creating educational projects for this purpose.

REFERENCES

Addorisio, R., Spadoni, R., Maesano, G., 2025. Adoption of Innovative Technologies for Sustainable Agriculture: A Scoping Review of the System Domain. *Sustainability*, 17(9), 4224.

Chaney, D., Touzani, M., Ben Slimane, K., 2017. Marketing to the (new) generations: summary and perspectives. *Journal of Strategic Marketing*, 25(3), 179–189.

Chiriacescu, M., 2024. *Cercetări privind utilizarea sistemelor informatice în managementul producţiei agricole.* PhD Thesis abstract. University of Agronomic Sciences and Veterinary Medicine of Bucharest.

European Commission, 2025. *Romania 2025 Digital Decade Country Report. Shaping Europe's Digital Future*. Available at: https://digital-strategy.ec.europa.eu/en/factpages/romania-2025-digital-decade-country-report. [Accessed 20.04.2026]

Fahmi, M.Y., 2020. *Understanding Agricultural Innovation Adoption in Developing Countries: An Indonesian Study*, MSc Thesis. Wageningen University and Research Netherland.

Nagel, P., Khalsa, S., Zamudio, W., Mizuta, K., Stalker, K., 2025. Standard to Validate Innovations in Agricultural Testing. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLVIII-M-7-2025, 44th EARSeL Symposium, Prague, Czech Republic.

Rosario, J., Madureira, L., Marques, C., Silva, R., 2022. Understanding farmers' Adoption of sustainable agriculture innovations: a systematic literature review. *Agronomy*, 12 (11):287.

Sofianu, C., Dumitru, N., 2024. *Dezvoltarea profesională în era digitală: provocări și soluții pentru piața muncii din România*, Ernst & Young. Available at: https://www.ey.com/ro_ro/insights/workforce/dezvoltarea-profesionala-in-era-digitala-provocari-si-solutii. [Accessed 20.04.2026]

World Economic Forum, 2025. *Future of Jobs Report of the World Economic Forum*. Available at: https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf. [Accessed 20.04.2026]

DIGITAL IDENTITY AND ARTIFICIAL INTELLIGENCE ETHICS IN ORTHODOX SOCIETY

CZU: [177:004]:281.9
DOI: https://doi.org/10.53486/tids2026.17

SERGEY BAZHENOV
Science Horizons Foundation, Russia
e-mail: sbazhenov@mail.ru
ORCID ID: 0000-0001-7593-0526

ELENA BAZHENOVA
Southern Federal University, Russia
e-mail: eubazhenova@sfedu.ru
ORCID ID: 0000-0001-8253-5073

DMITRY ABROSIMOV
Southern Federal University, Russia
e-mail: dabrosimov@sfedu.ru
ORCID ID: 0000-0000-0000-0000

Abstract. The paper examines how digital identity and the ethical principles governing artificial intelligence might be brought into alignment with the Orthodox Christian understanding of the person. It analyzes the concepts of digital identity and Orthodox anthropology, together with the challenges that AI presents to traditional societies. The positions of local churches and individual theologians are surveyed, and public case studies are considered. A model of responsible digital identity is proposed, grounded in transparency, sobornost' (conciliarity), and digital asceticism.

Keywords: digital identity, artificial intelligence ethics, Orthodox Christianity, person, conciliarity (sobornost'), digital asceticism, algorithmic accountability.

JEL Classification: O33, Z12, A13

INTRODUCTION

Digital transformation is reshaping contemporary society at an accelerating pace. Artificial intelligence (AI) now pervades nearly every sphere of life: it shapes what information people encounter, what goods are offered to them, and with whom they communicate. In parallel, digital identity is taking shape—the aggregate of data that represents a person online. Orthodox society, for its part, traditionally grounds its understanding of the human being in the teaching that man is created in the image of God. This teaching stresses the uniqueness, freedom, and irreducibility of the human being. The digital environment, however, constructs identity along different lines. It fragments the person and renders them controllable by algorithms.

The difficulty lies in the absence of systematic ethical reflection. Orthodox thought has not yet adequately engaged the challenges posed by AI. Clear principles for reconciling digital identity with spiritual integrity are lacking. The article therefore aims to propose a conceptual model for aligning digital identity and AI ethics with the Orthodox teaching on the person. Achieving this requires analyzing the concept of digital identity alongside Orthodox anthropology, identifying points of tension between the digital environment and Orthodox values, surveying existing positions and documents, examining public case studies without reliance on original surveys, and formulating a

strategy for responsible digital identity. Methodologically, the article is interdisciplinary, drawing on theological hermeneutics, philosophical analysis, document analysis, and secondary case analysis.

THEORETICAL FRAMEWORK: DIGITAL IDENTITY AND ORTHODOX ANTHROPOLOGY

In the social sciences, digital identity denotes the set of data that characterizes a person online—social media profiles, search history, geolocation, preferences, and the like. As Sherry Turkle observes, a person on the internet often experiments with different "selves". Erving Goffman described this phenomenon as impression management. Luciano Floridi adds that in the information society, identity becomes increasingly plastic. Digital identity is not fixed once and for all; it is constructed both by the user and by algorithms. Platforms offer ready-made templates: "verify your number", "select your interests", "like this". Gradually, a person begins to perceive themselves through the lens of recommendation systems.

Orthodox anthropology proceeds from the biblical statement that man is created in the image of God (Gen. 1:26–27). This means that the person is unique, free, and called to communion. Vladimir Lossky emphasized that the image of God is not reducible to individual properties; it is the whole fullness of the human being. Christos Yannaras develops the idea of the person as "hypostasis". The person is not an individual or individuality. The person is revealed only in love and conciliarity (sobornost'). Sobornost' is unity in freedom, where each remains oneself but acts together with the human being is a mystery. Their dignity does not depend on age, gender, social status, or digital footprint.

Several contradictions arise between digital identity and Orthodox anthropology. The first concerns the multiplicity of identities. The digital environment encourages different roles: one account for work, another for family, a third for hobbies. Orthodoxy, however, speaks of the wholeness of the person. A person should not fragment into roles; they are one before God. The second contradiction concerns the external construction of identity. Digital identity is constructed not only by the person themselves but also by algorithms. A platform may attribute to a person interests they do not have. Orthodox teaching asserts that the person cannot be an object of external construction; they are self-existent. The third contradiction relates to the quality of communication. In the digital environment, speed of response, engagement, and number of contacts are valued. Orthodoxy values depth, repentance, and constancy. Sobornost' presupposes not fleeting connections but stable communion in faith. Thus, a simple transfer of digital practices into Orthodox society is impossible. Reflection is required.

ETHICAL PROBLEMS OF AI IN LIGHT OF ORTHODOX ETHICS

Artificial intelligence is increasingly making decisions without human involvement. Banks approve loans, police use facial recognition, news feeds are generated automatically. From an Orthodox point of view, any decision affecting a person must be morally responsible. But responsibility presupposes freedom. AI has no free will. It acts according to preset algorithms. Therefore, moral responsibility cannot be attributed to AI. However, the person who created and uses AI is responsible. Theologians, such as Deacon Vladimir Serdyuk, warn that transferring important decisions to a machine blurs the boundaries of responsibility. The human being ceases to be a subject. The problem of responsibility becomes acute when AI makes mistakes or discriminates. If AI recommends dangerous content to a user or denies a service based on implicit criteria, the question of who is guilty arises. Orthodox ethics insists on personal responsibility. There can be no

responsibility without a person. Therefore, any decision made by AI must be traceable to specific people. Situations where the phrase "the machine decided so" becomes an excuse should be avoided. This resembles the ancient temptation to shift blame from oneself to fate, demons, or technology.

Privacy and the seal of confession occupy a special place in the Orthodox tradition. A priest cannot disclose what he has heard in confession, even under threat of death. However, in the digital world, privacy becomes conditional. Messengers, cloud storage, fiscal data—all of this is accessible to states or corporations. The patristic teaching on thoughts teaches that a person's inner world is closed to external observation. Only God and the person themselves know the heart. Digital surveillance violates this principle. It makes the inner external, the secret public. For Orthodox society, this is not only a technical but a spiritual problem.

The digital environment gives rise to new forms of sin, which can be called "digital sin." Traditional sins—pride, envy, anger, despondency—take on digital guises. Pride manifests in the pursuit of likes and followers, in creating an ideal image on social networks. Addiction is expressed in endless scrolling of the feed, which replaces live communication and prayer. The substitution of communication occurs when a person places a chatbot or virtual friend above real relationships. Priest Sergei Chetverikov notes that the digital environment provokes the sins of condemnation, gossip, and anonymous aggression. At the same time, the person often does not realize the sin, because the screen creates an illusion of impunity. Orthodox ethics must develop criteria for evaluating digital actions.

OVERVIEW OF EXISTING POSITIONS AND DOCUMENTS

The Russian Orthodox Church in 2020 presented a document titled "The Church and the Digital Environment". It is of a recommendation nature. The main points are as follows. The digital environment is a tool, not a substitute for real communication. Parish life cannot be fully transferred online. Digital hygiene and caution are needed. The Church should be present on the internet, but not dissolve into it. The document does not specifically address AI, but sets a general tone: technologies should not destroy church conciliarity.

Orthodox theologians in recent years have published several articles and interviews. Protopresbyter Alexander Schmemann, in retrospective reading, foresaw the danger of "techno-religion"—the belief that technology will save humanity. Contemporary authors, such as Priest Konstantin Parkhomenko, warn about the possible appearance of "AI spiritual directors", which is unacceptable. Greek theologians, such as Metropolitan Ignatius, discuss the problem of authority. If AI gives moral advice, who will verify its teaching? Orthodoxy insists on living tradition, transmitted from person to person, not through an algorithm.

A comparison with Catholic AI ethics provides useful material. In 2020, the Vatican issued the "Rome Call for AI Ethics". The document was signed by major IT corporations. Its main principles are: transparency, impartiality, responsibility, confidentiality, and human-centeredness. Orthodoxy can adopt the technical formulations from this document. But there is an important difference. The Catholic document appeals to natural reason and shared values. Orthodoxy, however, emphasizes the ascetic dimension. It is not enough to make AI "transparent". It is necessary for the person themselves to change their attitude toward technology.

CASE STUDIES FROM OPEN SOURCES

As concrete examples, one can consider the use of AI chatbots by Orthodox dioceses. Some dioceses have launched Telegram bots with daily Gospel readings. The bot can remind about fasting, provide links to akathists. From an ethical standpoint, this is a neutral tool. However, there is a risk. A person might begin to perceive the bot as a spiritual guide. But a bot is incapable of empathy, does not know the secrets of the heart, and does not give penitential advice. Therefore, instructions for such bots should include a direct statement: "This is an information channel, not a substitute for a priest".

Another illustrative case is the controversy over facial recognition systems in churches. In Russia, in 2019–2021, the installation of cameras with facial recognition in churches was discussed. The idea was to enhance security. However, believers and priests opposed it. The arguments were as follows. The church is a place of openness, not total control. Facial recognition hinders prayerful concentration. Moreover, the data could be misused. This controversy showed that even a technically useful solution can be rejected on spiritual grounds.

The third case concerns recommendation algorithms and Orthodox content. YouTube and other platforms use recommendation algorithms to hold a person's attention. A person who watches a sermon may then be shown aggressive political content or overtly occult videos. This phenomenon is called "algorithmic radicalization." For the Orthodox user, this is a serious risk: someone weak in faith may be led astray. The algorithm does not distinguish true teaching from heresy. It is driven by engagement. Therefore, Orthodox media must themselves shape their content ecosystem, without relying on AI.

A STRATEGY FOR ALIGNMENT: A MODEL OF RESPONSIBLE DIGITAL IDENTITY

Based on the analysis, several principles of AI ethics derived from Orthodox teaching can be proposed. The first principle is the principle of the person. Any AI decision affecting a person must treat the person not as an object but as a subject. The person cannot be reduced to a profile. The second principle is transparency. A person has the right to know how the algorithm works, what data is collected, and who bears responsibility. The third principle is conciliar governance. The introduction of AI into public institutions, including church institutions, should be discussed openly, with the participation of clergy, laity, and experts. The fourth principle is non-interference in the mystery of the person. The use of AI for surveillance of confession, thoughts, or inner religious life is prohibited.

The Orthodox tradition knows practices of abstinence and spiritual discernment. In the digital environment, these practices can be framed as digital asceticism. Its elements include limiting time on social networks following the pattern of fasting, consciously rejecting recommendation feeds in favor of targeted search, daily reflection on what one has watched and why, and using tracker blockers and open-source software as an act of resistance to total data collection. Digital asceticism does not reject technology but disciplines one's relationship with it.

For church-state dialogue, the following steps can be proposed. It is advisable to create expert groups on AI ethics within synodal departments. A church document should be developed on the boundaries of permissible AI use, for example, stating that automatic absolution of sins or the generation of sermons by neural networks is inadmissible. Legislative initiatives should also be pursued to protect personal data in the religious sphere, especially concerning the seal of confession.

CONCLUSION

The article has analyzed the concepts of digital identity and Orthodox anthropology. It has shown that there are serious contradictions between them. The digital environment fragments the person, AI algorithms deprive them of responsibility, and total surveillance destroys inner secrecy. However, this does not mean that Orthodox society must reject digital technologies. On the contrary, active reflection and the development of ethical norms are required.

The final conclusions are as follows. Digital identity does not cancel but demands a deeper understanding of the person. AI is a tool, not a subject of relationships. Responsibility always remains with the human being. Orthodox AI ethics should be based on transparency, conciliarity, and non-interference in the mystery of the person. Digital asceticism is a necessary practice for preserving spiritual integrity.

A limitation of this study is the absence of empirical data, such as surveys or interviews. The article is theoretical and conceptual in nature. Directions for future research include the theology of AI (can AI bear the image of God?), digital confession and remote sacraments, a comparative analysis of AI ethics across three confessions (Orthodoxy, Catholicism, Protestantism), and the development of specific digital asceticism programs for parishes.

REFERENCES

Lossky, V. N. (1991). Essay on the Mystical Theology of the Eastern Church [Ocherk misticheskogo bogosloviya Vostochnoy Tserkvi]. Moscow. (in Russian)

Yannaras, Ch. (2005). Person and Eros [Lichnost' i Eros]. Moscow: ROSSPEN. (in Russian)

Turkle, S. (2005). The Second Self: Computers and the Human Spirit. MIT Press.

Floridi, L. (2013). The Ethics of Information. Oxford University Press.

Goffman, E. (1959). The Presentation of Self in Everyday Life. Anchor Books.

Report “The Church and the Digital Environment” [Doklad “Tserkov' i tsifrovaya sreda”]. (2020). Russian Orthodox Church. (in Russian)

Chetverikov, S., priest. (2021). Digital sin: challenges and responses [Tsifrovoy grekh: vyzovy i otvety]. Living Water [Voda zhivaya]. (in Russian)

Serdyuk, V., deacon. (2019). Artificial intelligence and Christian anthropology [Iskusstvennyy intellekt i khristianskaya antropologiya]. (in Russian)

Rome Call for AI Ethics. (2020). Vatican / Pontifical Academy for Life.

Parkhomenko, K., priest. (2022). Can AI be a priest? [A mozhet li II byt' svyashchennikom?]. Radio Vera. (in Russian)

Metropolitan Ignatius (Greece). (2021). Orthodox Ethics and Artificial Intelligence [Ορθόδοξη Ηθική και Τεχνητή Νοημοσύνη]. Αθήνα. (in Greek)

Schmemann, A., protopresbyter. (1974). Liturgy and Life [Liturgiya i zhizn']. Paris. (in Russian)

CYBER RESILIENCE STRATEGIES: SPIRITUAL AND SOCIAL ASPECTS

CZU: 004.056:[177+261.7+281.9]
DOI: https://doi.org/10.53486/tids2026.18

SERGEY BAZHENOV
Science Horizons Foundation, Russia
e-mail: sbazhenov@mail.ru
ORCID ID: 0000-0001-7593-0526

ELENA BAZHENOVA
Southern Federal University, Russia
e-mail: eubazhenova@sfedu.ru
ORCID ID: 0000-0001-8253-5073

DMITRY ABROSIMOV
Southern Federal University, Russia
e-mail: dabrosimov@sfedu.ru
ORCID ID: 0000-0000-0000-0000

Abstract. The paper approaches cyber resilience as both a technical and a spiritual-social issue. It surveys the principal cyber threats confronting individuals and communities, then identifies specific spiritual vulnerabilities fear, pride, and technological dependence-alongside corresponding resources such as humility, providential trust, and sobornost' (conciliarity). The authors propose an integrated framework spanning technical, social, and spiritual levels of resilience, with particular attention to how Orthodox Christianity frames human responses to the challenges of digital life.

Keywords: cyber resilience, cybersecurity, spiritual dimensions, social strategies, Orthodox Christianity, fear, trust in God, conciliarity (sobornost'), digital literacy.

JEL Classification: Z13, D85, I31

INTRODUCTION

Contemporary society's dependence on digital infrastructure continues to deepen. Personal records, financial transactions, communications, and administrative functions have all migrated online. This shift has brought undeniable conveniences, but it has also generated a class of threats that have become routine: cyberattacks, data breaches, disinformation campaigns, and online fraud. Conventional cybersecurity practice concentrates on technological countermeasures-firewalls, antivirus programs, encryption protocols. Yet empirical experience repeatedly demonstrates that even robust technical systems can be compromised. The vulnerability frequently originates not in the technology itself but in the human dimension.

Cyber resilience is typically defined in terms of a system's capacity to withstand attacks. This framing, however, overlooks the resilience required of individuals and communities. Worldview, trust, and communal bonds-factors that might be termed spiritual and social-play an equally consequential role. Within an Orthodox Christian framework, these factors take on added significance. Fear of cyber threats can immobilize the will; pride can produce carelessness about protection. Conversely, humility, trust in God, and communal solidarity supply an inner stability that technical measures cannot provide.

This article develops a conceptual model of cyber resilience that incorporates spiritual (Orthodox) and social dimensions alongside the technical. The analysis proceeds by examining existing definitions of cyber resilience, identifying spiritual vulnerabilities and resources, and proposing social and ecclesial strategies. Methodologically, the study draws on an interdisciplinary synthesis of cybersecurity theory, Orthodox social ethics, and the sociology of risk. It is theoretical in scope and does not report original survey data.

THE CONCEPT OF CYBER RESILIENCE: TECHNICAL, SOCIAL, AND SPIRITUAL DIMENSIONS

In its classical formulation, cyber resilience denotes a system's ability to withstand, absorb, and recover from cyberattacks - a definition advanced by the U.S. National Institute of Standards and Technology (NIST) and the European Union Agency for Cybersecurity (ENISA). Technical resilience encompasses backups, network redundancy, and prompt patching. Such measures are necessary but not sufficient.

The social dimension of cyber resilience concerns a society's capacity to resist disinformation, digital panic, and the erosion of institutional trust. A data breach can produce widespread anxiety; the spread of fabricated news can strain social cohesion. A socially resilient society sustains critical thinking, relies on verified sources, and protects vulnerable populations. Scholars in the sociology of risk have emphasized that resilience depends substantially on community cohesion.

The spiritual dimension, particularly in its Orthodox articulation, remains largely unexplored. Spiritual cyber resilience may be understood as the capacity of individuals and communities to preserve inner peace, faith, and moral integrity in the face of digital challenges. The concern here is not the protection of computers but the protection of the soul. The digital environment introduces not only technical threats but also temptations: addiction, anger, despondency, fear. A spiritually resilient person does not yield to panic, does not lose trust in God, and does not fall into sin as a consequence of an attack or hack. Cyber resilience thus becomes an integrated concept uniting three levels.

SPIRITUAL VULNERABILITIES IN THE DIGITAL ENVIRONMENT

The digital environment exposes several spiritual weaknesses. The first and most evident is fear. Reports of cyberattacks, account compromises, and password leaks generate anxiety. People fear the loss of money, personal photographs, or access to essential services. In Orthodox understanding, fear is often a symptom of insufficient trust in God. The Holy Fathers distinguish natural fear (in the face of genuine danger) from sinful fear (which paralyzes the will and leads to despair). Cyberattacks tend to produce the latter: a person feels defenseless before vast algorithmic forces.

The second vulnerability is pride and self-conceit. Some individuals assume that no one will hack them because they "do nothing online". Others swing to the opposite extreme of nihilism, declaring that "they will hack me anyway, so protection is pointless." Both attitudes originate in pride. In the first case, the person relies on their own insignificance, forgetting that attackers operate at scale. In the second, pride manifests as a refusal to make an effort, as contempt for precautionary measures. Orthodox teaching identifies pride as the root of all sins; in the digital environment, it renders a person vulnerable.

The third vulnerability is technological addiction. Contemporary people often cannot imagine life without a smartphone, social networks, or messaging applications. Such dependence obstructs inner freedom. The patristic tradition warned against any attachment that hinders love for God. In digital contexts, addiction appears as compulsive checking of notifications, an inability to disconnect,

and anxiety when offline. Cyber resilience diminishes under such conditions, since any technical glitch is experienced as a catastrophe.

The fourth vulnerability is disinformation and the sin of lying. Social media algorithms frequently circulate falsehood more rapidly than truth. A user may fall victim to a fake or unconsciously disseminate false information. The Christian commandment "do not bear false witness" acquires new resonance in the digital world. The capacity to recognize lies and refrain from spreading them is a spiritual task. When a person succumbs to algorithmic manipulation, they lose both spiritual and social resilience.

SPIRITUAL RESOURCES OF CYBER RESILIENCE

The Orthodox tradition offers a substantial repertoire of means for strengthening inner resilience. The first and most important resource is humility. Humility is the antidote to pride. A humble person acknowledges the limitations of any technical means. They understand that complete protection does not exist, but this is not a cause for despair. A humble person is prepared for failures, possible data loss, and temporary difficulties. They do not panic because their hope rests not in gadgets but in God. Humility also helps to take precautionary measures without fanaticism.

The second resource is trust in God's Providence. This virtue reduces panic fear of cyber threats. A person who trusts in God knows that not a single hair will fall from their head without the Father's will. This does not, of course, mean neglecting protection. But trust helps to remain calm when something goes wrong. A lost account, stolen data, a hacked phone - these are unpleasant, but not the end of life. A spiritually resilient person endures such losses more easily and recovers faster.

The third resource is the ascetic habit of self-restraint. Orthodox asceticism teaches a person to control their desires, to limit themselves in food, sleep, and entertainment. This habit extends to the digital environment. An ascetically minded person does not spend hours on social networks, does not react to every notification, does not cling to devices. Self-control developed in spiritual life makes a person less dependent on technology, and therefore more resilient to cyber threats. For example, if such a person's account is hacked, they will not experience withdrawal because their life does not revolve around virtual space.

The fourth resource is conciliarity (sobornost') and mutual aid. In an Orthodox community, people support one another. In the event of a digital incident - hacking, fraud, deception - the community can offer help. For example, if an elderly parishioner has money stolen through phishing, the community can help them financially and psychologically. If false information about a priest is spreading, the community can provide accurate information. Sobornost' creates social cyber resilience: a person does not remain alone with the threat.

The fifth resource is prayer and the sacraments. After a cyber trauma (for instance, after being deceived or hacked), feelings of shame, anger, and helplessness arise. Confession helps to free oneself from these feelings. Communion restores mental balance. Prayer calms and brings back hope. Thus, spiritual life is not a supplement but the foundation of cyber resilience.

SOCIAL STRATEGIES FOR CYBER RESILIENCE

Social strategies aim to organize assistance and education. The first strategy is digital literacy at the parish and family level. Catechists and priests can hold discussions on cyber hygiene. People should know how to create strong passwords, recognize phishing emails, and verify information before sharing it. Such work is especially important among the elderly, who often become victims of fraud. The parish can become a place where safe online behavior is taught.

The second strategy is the role of church structures in disseminating verified information. In the context of disinformation, people lose their bearings. The Church can be an institution that provides verified news and refutes fakes. For example, if a false message about some event in the diocese appears online, the church's official website or account can quickly issue a rebuttal. This increases social resilience because people know where to turn for the truth.

The third strategy is the creation of crisis centers and counseling for victims of cybercrime. A person who has been deceived online often feels shame and does not seek help. Church counselors (priests, psychologists) can receive such people, listen to them, and give spiritual advice. It is important not to judge the victim but to help restore mental balance. They can also help draft statements to the police or contact banks. This reduces secondary traumatization.

The fourth strategy is cooperation with state structures to protect the personal data of believers. Particularly sensitive is the seal of confession. If confession data (even in digital form) is stolen, it would cause enormous harm. The Church can initiate legislative changes that strengthen the protection of religious information. It can also enter into agreements with IT companies for the secure storage of church data.

The fifth strategy is the creation of "digital squads" of volunteers. Parishes have technically literate laypeople. They can help elderly people set up devices, explain how not to fall for fraudsters' tricks, and warn about new threats. Such squads can also monitor fakes and inform priests about false information. This is an example of living conciliar work.

CASE STUDIES FROM OPEN SOURCES

An analysis of open sources shows that cyber threats to the Orthodox environment are not hypothetical. In Russia and other countries, attacks on church websites and databases have occurred.

For example, in 2020–2021, several diocesan portals were hacked. Attackers posted offensive content on them or tried to steal administrator accounts. Technical protection on many parish websites was weak. This indicates the need to raise awareness among the clergy.

A second category of cases concerns fabricated stories about priests and parishes circulating on social media. In 2022, a false report appeared in one Russian region claiming that a church rector was collecting money for a personal automobile. The story spread rapidly. Parishioners, however, mounted a defense: they published documentation of the actual fundraising and clarified the circumstances. The community's response exemplified social resilience and demonstrated that an active, cohesive congregation can effectively counter disinformation.

A third category involves successful self-organization among Orthodox volunteers to expose online fraud. Social networks and messaging platforms periodically host solicitations circulated in the names of well-known priests. Volunteers identify such fakes with speed, alert subscribers, and assist in blocking the perpetrators. This work demands coordination and vigilance. Certain Telegram groups have been established expressly for this purpose, functioning as informal cybersecurity squads.

Foreign experience merits attention as well. In Greece and Romania, dioceses have developed cybersecurity programs for clergy, instructing priests in the fundamentals of safe email and social media practice. Romania's Patriarchate maintains a dedicated department that monitors cyber threats and issues recommendations. Such initiatives could prove valuable to other local churches.

AN INTEGRAL MODEL OF CYBER RESILIENCE

Drawing on the preceding analysis, an integral model of cyber resilience may be proposed. The model comprises three interconnected levels: technical, social, and spiritual. The technical level includes software and hardware protections, backups, and encryption. The social level encompasses education, mutual aid, institutional trust, and volunteer squads. The spiritual level consists of humility, trust in God, ascetic practice, conciliar prayer, and participation in the sacraments.

These levels do not replace one another but rather complement each other. Technical protection matters, yet without social organization it remains ineffective. Social organization, in turn, proves useless if people are inwardly panicked about cyber threats. Spiritual resilience reinforces both the technical and social dimensions: a person unattached to gadgets endures failures more easily, and a community united by love responds to fakes more swiftly.

The model also outlines stages of recovery from a cyber incident viewed through a spiritual lens. The first stage is recognition: the person acknowledges that they have been hacked or deceived. The second is repentance: if their own carelessness or pride permitted the vulnerability, they bring this to confession. The third is forgiveness.

The person forgives the fraudsters or attackers, bearing no grudge.

A fourth stage is the restoration of trust: the person resumes normal digital life, though with heightened caution. This cycle aligns with the patristic tradition of healing the passions.

For church hierarchy, several recommendations follow. Cybersecurity guidelines for clergy and laity should be developed and distributed. Parish-based digital literacy circles ought to be established. Contacts with state cyber structures should be cultivated for rapid response to attacks. For the laity, the guidance includes: avoid storing all passwords in one location, refrain from clicking on suspicious links, resist panic upon receiving alarming news, and consult with one's spiritual father and community.

Indicators of spiritual cyber resilience might include the following: composure during technical failures; the ability to evaluate online information critically; willingness to assist another person who has fallen victim to cyber fraud; and the capacity to disconnect from devices without experiencing anxiety.

These indicators can be used in pastoral practice to assess a parish's readiness for digital challenges. Conclusion. The article has examined cyber resilience strategies in their spiritual and social dimensions. It has been shown that cyber resilience cannot be only a technical problem. Spiritual vulnerabilities such as fear, pride, and addiction make a person an easy target for cyber threats. At the same time, Orthodox teaching offers powerful resources for inner resilience: humility, trust in God, asceticism, conciliarity. Social strategies, including digital literacy training, church counseling for victims, cooperation with the state, and volunteer squads, strengthen protection at the community level. The proposed integral model combines three levels and provides practical recommendations for clergy and laity.

Limitations of this study include the absence of empirical measurements. The article is theoretical and relies on open sources rather than surveys or experiments. Nevertheless, it sets a direction for future research. Promising topics include the development of practical cybersecurity guides for parishes, the study of canonical aspects of protecting the seal of confession in the digital age, and a comparative analysis of cyber resilience in different Christian denominations.

REFERENCES

NIST Special Publication 800-160, Volume 2: Developing Cyber Resilient Systems. – National Institute of Standards and Technology, 2019.

ENISA. Cyber Resilience Act: European approach to cyber resilience. – European Union Agency for Cybersecurity, 2022.

Lossky, V. N. (2012). Dogmatic Theology [Dogmaticheskoe bogoslovie]. Moscow: Svyato-Troitskaya Sergieva Lavra. (in Russian)

Ignatius Brianchaninov, St. (2008). Ascetical Experiments [Asketicheskie opyty]. Moscow: PSTGU. (in Russian)

Yannaras, Ch. (2015). Disbelief and Faith [Neverie i vera]. Moscow: BBI. (in Russian)

Report of His Holiness Patriarch Kirill at the Moscow Diocesan Assembly (section on the digital environment). (2021). (in Russian)

Chetverikov, S., priest. (2022). Digital environment and spiritual security. Living Water [Voda zhivaya], No. 4. (in Russian)

Serdyuk, V., deacon. (2021). Cybersecurity and Christian ethics. (in Russian)

Papadimitriou, A. (Archpriest of the Greek Church). (2020). The Church and Cyber Threats [Η Εκκλησία και οι Κυβερνοαπειλές]. Αθήνα: Εκδόσεις Σταμούλη, (in Greek)

Official website of the Romanian Patriarchate. (2022). Cybersecurity Guide for Priests. (in Romanian)

Sociology of Risk and Uncertainty: collective monograph. (2018). Ed. Yanitsky, O.N. Moscow: Institute of Sociology of the Russian Academy of Sciences. (in Russian)

Fakes in the Religious Environment: Case Analysis. (2021). Analytical Center "Sova". (in Russian)

SOCIO-ECONOMIC RISKS ASSOCIATED WITH DIGITALIZATION PROCESS IN THE FIELD OF ECOLOGY AND ENVIRONMENT PROTECTION

CZU: [504.03+504.06+551.583:004]:005.342(478)
DOI: https://doi.org/10.53486/tids2026.19

ELENA MARGINEANU
Free International University of Moldova ULIM
e-mail: emargineanu@ulim.md
ORCID ID: 0000-0002-6157-8506

Abstract. The paper examines the contradictions in the current environmental agenda, arguing that climate narrative (later IPCC summary) overlooks important factors – natural variability of temperature. Other factors are solar activity, potential deliberate weather modification and dissenting scientific findings – leading all to flawed policies. The analysis highlights that rapid digitalization (AI monitoring, CBDC) combined with carbon accounting and renewables dependence could create socio-economic vulnerabilities: ecosystem distruption, foreign resource capture, exposure to weather-modification threats and a de facto absorbtion into a social-credit system that risks totalitarian control. The paper overall points that environment protection field has sufficient overlooked natural and technological variables in policy-making, that it can misdirect mitigation/adaptation and worsen geopolitical and domestic risks. Therefore, entire approach toward environment protection and data security can be revised with more realism, under lenses of security.

Keywords: solar activity, weather modification technologies, climate policies, digitalization, CBDC, national security.

JEL Classification: Q56 Environment and Development • Environment and Trade • Sustainability • Environmental Accounts and Accounting • Environmental Equity • Population Growth

INTRODUCTION

Environmental protection is gaining more attention from regulatory national and international actors, as the public is rising its awareness both on the impact ecology plays in the life of a human being, as the impact of environment on the wellbeing of the society as a whole. This attention is aggregating into a series of policy recommendations across sectors on the premise to help improve environmental condition. The logic for the act of formulating an intervention proposal presumes a prior analysis of data about the state of environment, and on the basis of acquired data, to generate directives of strategic movement for the system improvement. Particularly for ecology field, this would translate into analyzing data about previous condition of environment (eg.: *temperature variations in the last centuries*) and, with selected variables and premises, to formulate prognosis (eg.: *how temperature will fluctuate, what crop yield is expected*) and conditioning (eg.: *positive or negative interpretations*) that would tailor future measures adopted by the government (eg.: *loosen entrepreneurial and production activities or impose sanctions and carbon tax*).

The problem appears when the technicality of such complex approach is stumbled upon the probability that the scientific base and strategic premises of this instrument is flawed from the beginning. For example, IF:

A. Premise 1 „*accelerate warming*" is contrasted with probability of a different reality 1 „*not accelerate warming / probability of upcoming colling*";

B. Premise 2 „*warming is bad*" is contrasted with a different understanding upon physical causality in environmental processes „*warming in not bad for the environment, a potential cooling is worse in its impact over socio-economic processes*";

C. Premise 3 „*climate change is caused by human activity*" is contrasted with real science censored or unincluded in policy development process „*climate change is caused mainly by natural factors*";

D. Premise 4 „*carbon tax will reduce global temperature*" is contrasted with simple logical comparison exercises between existing research „*solar activity / irradiance affects global temperature*"; or with further combinations of:

E. Premise 5 „*carbon is bad*" with „*net-zero policies*" vs. „*carbon is necessary*" with carbon generators production for food production and green stimulation and „*track purchase behavior and reduce consumption to reduce carbon*" vs. „*no need to reduce carbon for environment protection*".

F. Premise 6 „*energy policy promotes renewables that are highly dependent on weather oscillations*" is also contrasted with logic and existing practices „*big global players are developing weather modification technologies*" etc.

THEN, we might formulate the hypothesis that: „ *socio-economic risks resulted from digitalization process associated with environment protection efforts promoted ideologically by international actors and implemented practically by national ones, will damage both (a) national security and (b) individual sovereignty and (c) will surpass declared benefits in the long term*".

MAIN CONTENT

The contradiction between official declarations and observed reality trigger more questions upon the efficiency and appropriateness of actions recommended for environment protection. At the Conference of Parties COP29 on 12.11.2024, the UN Secretary General, Antonio Guterres, states that we are in „*the hottest day on record, the hottest months on record, this is almost certain to be the hottest year on record*", however in the same week, various media outlets published that in South Africa it snowed for the first time in 85 years (11.11.2024). These contrasts between official statements and official reality check, create an inevitable impulse to research deeper the potential errors in the environmental agenda.

The environmental agenda includes several measures for decarbonization, promotion of renewable energy and a clear visible yet instrumental trend to digitalize everything, from monitoring (AI, satellite data) to ESG criteria for crediting from banks. Nevertheless, a serious incompleteness represents the absence of important variables in environmental agenda, precisely: solar activity, deliberate weather modification activities that are or can be carried out by interested actors, as well as existing real science statements that contradict the statements, which stand at the base of current environmental policies.

1. Materials and Methods

The research materials are research papers from various disciplines (from legal analysis to findings from astrophysics), journalistic articles from international classical media outlets starting with the premise that such materials influence public awareness and perception of the subject at hand, press publications from international institutions and other official reports.

Main research method is qualitative method based on document and policy analysis to examine legislation development, government strategies, international directives. It was also used an interdisciplinary approach with comparison between statements and observations on similar set of

concepts in order to identify the errors in the general narrative and sketch a risk assessment framework for further research.

2. Contradictions of IPCC

Intergovernmental Panel on Climate Change (IPCC) is the main scientific body affiliated to international organizations, that create science and policy briefs, that are imposed on institutional decision bodies. It doesn't conduct its own experiments or collect raw data. Instead, it brings together and evaluates thousands of studies produced by scientists around the world. From this research, it produces large assessment reports that summarize what is known about climate change, its causes, possible future developments, and ways societies can respond. It acts like a „translator" between climate science and policymakers, as it was established by the United Nations through the World Meteorological Organization and the UN Environment Programme, and it is widely considered the most authoritative global source on climate change assessments. Even Republic of Moldova has recogized and included IPCC as its standard in national legislation (*Law on climate actions* no.74/2024, *Regulation on the monitoring, reporting and verification of greenhouse gas emissions from stationary installations and aviation activities* no.575/2024; *Regulation of the establishment and operation of the National System for Monitoring and Reporting of Greenhouse Gas Emissions and other information relevant to climate change* no.1277/2018 (through modifications from Regulaiton no.31/2024); *Regulation on the energy governance mechanism and climate action* no.10/2024 etc).

However, IPCC contradicts itself in a serious manner – the nuances are sufficient to destroy the premise of environmental agenda. In the first report (1990) IPCC explained that the temperature has known natural variations with warming and cooling and again warming trends in the last milenium, but in its third report (2001), IPCC has leveled the whole natural variations across the centuries at lower levels and leaved depicted on the graph only the warming from the last 2 centuries, which is a a colossal mistake and a gross methodological manipulation.

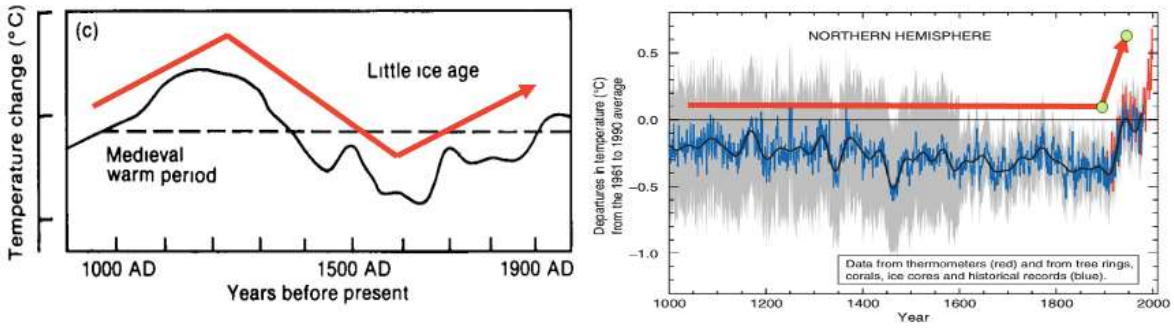


Figure 1 and Figure 2. Variation of the Earth's temperature for the last 1000 years
Source: *IPCC Report (Figure 1: Report from 1990; Figure 2: Report from 2001)*

Researchers and practitioners challenge the validity, construction and scientific handling of „the Hockey Stick" graph, arguing that it is methodologically flawed and politically protected, as it prominence reflects failures in scientific practice rather than robust consensus. Also, not less important is the statement that algorithms can produce hockey-stick shapes even from random data, downplaying any variabilities at prior order of data set, which, if proven true, must be immediately revoked. The issue resides in the impossibility to verify the algorithm due to high complexity of matter at hand, modelling program and possession aspects.

It is also a paradox that in the scientific and policy community co-exist officially 2 realities: (a) recognizing the existence of Medieval Warmth Period and a Little Ice Age (clearly not caused by industrial CO_2 emissions), and (b) not recognizing any variability in temperature changes in the past

10 centuries when formulating policy recommendations for economic reconfiguration of production sector and climate adaptation. Therefore, if another side of research is not reflected in policy discussions (the potential cooling), then what would the system encounter when preparing for a warming instead?

3. Contradictions between predicted and later observed temperature

The public debate is exacerbated by the findings of John Christy, Roy Spencer and others, who separately from each other, have argued that the computer-generated climate models show a prediction of warming faster than real-world measurements, especially in the troposphere, where temperature are shown to rise significantly lower than the model-predicted rise. From over 35 examined models, was identified a statistically significant average difference from observed records and an overpredicted warming. Their basic claim is not that the warming is absent, but that the rate and pattern of warming in the computer simulations are too strong compared with satellite and radiosonde observations. For researchers from real science, this overprediction is large enough to raise questions about how accurately the models represent atmospheric feedback; as for social scientists this is a confusion that signals the wrongness of proposed economic modifications in the system.

4. Solar activity

Solar activity implies variance of solar irradiance that Earth is receiving and directly affects the climate dynamics. A solar cycle is established have 11 years, recording a peak in solar flares (understood through sunspots) and a minimum. In the same time, apart from decadal cycle, the sun has a bicentennial variation as well: Grand Solar Minimum (GSM) is a prolonged period lasting decades to centuries when the Sun's magnetic activity, sunspots and overall solar output remains unusually low compared with normal solar cycles. This suggests that the Sun might have longer rhythms. There are various papers that confirm the coincidence between solar activity and Medieval Warmth Period and Little Ice Age (Steinhilber F., Beer J., 2011). Yet more controversial is the link between Grand Solar Minimum and seismologic events as well as with increasing incidences of volcanic eruptions (Tavares M., Azevedo A., 2011). Currently we are in the 25th solar cycle, and some research state that in the future 26th cycle more volcanic eruptions are anticipated (Vasilieva I., Zharkova V., 2022). On the impact of modern Grand Solar Minimum on terrestrial environment, it was assumed that we might expect a reduction of terrestrial temperature until 2053, with negative impact over vegetation growth, agriculture, food production and heat sector (Zharkova *et al.*, 2025). Notewothy to say that not only various research from real science confirm the approach of a new Grand Solar Minimum (Mörner N.A., 2015; Miyahara *et al.*, 2021; Arsenovic *et al.*, 2018), but also the ***Vatican Observatory*** official website has a publication for New Dual Dynamo Solar Model that predicts a „Maudern Minimum" for cycle 26 with reference to Bob Trembley's lecture about the Sun. The presented graph depicts an upcoming reductio of solar irradiation with soft decrese by 2060, and severe decrese with a full GSM by the year 2150. Although this prognosis differs in timeframe with what Zharkova proposed, nevertheless – *both admit the potentiality of a temperature reduction (global cooling) due to natural causes, as opposed with ideologicaly promoted narrative of global warming due to human activity.*

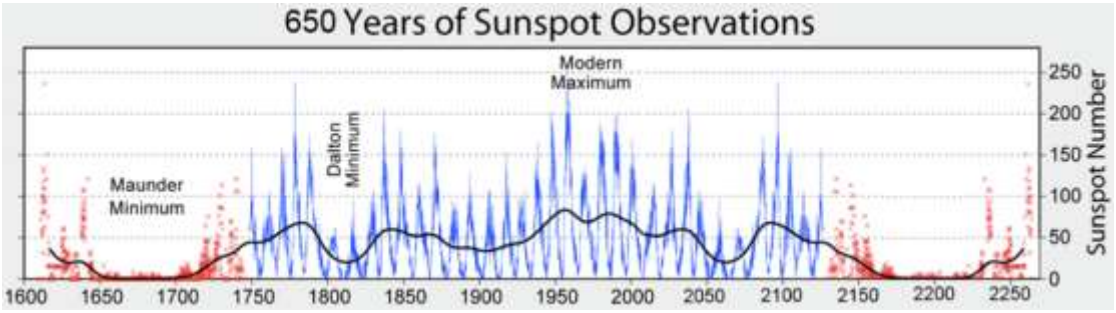


Figure 3. A 650 years of sunspot graph proposed as a new dual dynamo solar model
Source: *Vatican Observatory* https://www.vaticanobservatory.org/sacred-space-astronomy/new-dual-dynamo-solar-model-predicts-maunder-minimum-for-cycle-26/

When NASA headquarters consultant and White House national space policy advisor John L. Casy, have discovered solar cycles and the probability of encountering a future relative cooing instead of warming, he has advised Washington to revise its strategy in environmental domain, however instead of revising economic recommendations for developing states, USA officials have agreed to simply replace „*global warming*" in „*climate change*" and continue pushing the same „adaptation proposals" internationally.

5. Weather Modification Technologies

Whether Modification Technologies are of several categories – induce precipitations (*cloud seeding*), large-scale manipulations (*geoengineering*), modifications of the weather on local or regional scales (*other weather modification technologies*).

Although Nikola Tesla registered its earthquake machine in 1894 (patent no.US511916A), currently are a few hundred of patents registered and with open access visibility, on weather modification category (starting from *method of producing fall precipitation* in 1891 until *systems for artificially forming clouds, relocating formed clouds and methods of using same* registered in 2023). The patent for *Weather Control Method/Process* was registered several times in the past 70 years and is already expired.

Across the continents we even have developed legislation that regulates manipulation of weather processes: Romanian Law on active interventions in the atmosphere no.173/2008, Canadian Weather Modification Information Act from 1985, USA National Weather Modification Policy Act from 1976 and even since 1967 there is a law in Australia that regulates „rain-making control" being still an act in force.

Project Cirrus (1947) and Project Stormfurry (1962-1983) were two governmental projects coordinated with defense sector, to learn hurricane control and modification, admitting officially the state attempts to manipulate large weather processed by artificial cloud seeding. More than this, during Vietnam War, USA used climate weapons to weaken the opponents through „Popeye Operation" (among others), the purpose of which was to increase rainfall in carefully selected areas to prevent Vietnamese military supply from reaching their destination. When it got publicly known that USA used climate weapons, instead of pledge to not repeat such activity, they managed to gather everyone at UN and sign the Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD), which entered into force in 1978 and clearly recognized the existence and by this, offered the definition for „*environmental modification techniques*". Thus, it is naive to assume that from 1978 until today, no international organism has improved and developed such capabilities.

More than this, in 2021, China has created an official institution dedicated exclusively to Weather Modification Technologies under state Meteorological Administrate – China MA Weather Modification Center (WMC). With this, China has declared though a State Council note that it will develop worldwide advanced operational services by 2035 in terms of weather manipulation. Also, it is China who currently runs the biggest official weather manipulation project - „Sky River Project" is an initiative to move water vapors from Yangtze to Yellow River (almost 5 billion cubic meters of water) as the targeted area up north hold over 60% of the country's agriculture production.

In the same time, United Arab Emirates (UAE) also strives to publicly become a world leader in rain control, as it created the UAE Rain Enhancement Program under National Center of Meteorology and with the blessing of His Highness. The cynical part from this subject is that, local research of the environment and biodiversity if often used to study the area of the place against which weather weapon is being created for. Be it crop improvement or weather control; humanity has always looked upon methods to influence natural processes.

6. Digitalization process

On the official page of an UN body (United Nations Framework Convention on Climate Change UNFCCC) is being presented the prototype of the world's first credit card with a carbon footprint, stating that the card „*not only helps users track and measure CO_2 emissions associated with their purchases but also puts a limit to the climate impact of their spending*", which translated into conventional language – the banking card will get blocked once the costumer consumes more CO_2 that what is being programmed as allowed for him/her to consume. This is feasible from technical part if the (a) product is being calculates in terms of carbon, and (b) the financial system becomes digital. Both such conditions are already crafted as massive international policies.

(a) The EU is transitioning toward mandatory carbon footprint labeling, targeting specific sectors by 2027. Such instrument is named product environmental footprint (PEF) or climate label for products, where for a product is being indicated the carbon emitted during producing process and its supposed carbon rating. For example, a piece of meat would be the lowest at score at the purchase with the card.

(b) The European Central Bank (ECB) is actively preparing for a digital euro (Central Bank Digital Currency CBDC), aiming for a possible issuance around 2029, if EU legislation is adopted by 2026. It is needed to bring clarity that, cryptocurrency based on blockchain means a Decentralization of the system, while CBDC is a complete Centralization.

Overall, a fully digitalized financial system with digital money in the form of CBDC cumulated with a personal carbon footprint calculator – gets the creation of a new Social Credit System, which can be translated only as totalitarianism (this one being based not on political motives, but on limiting consumption rights and dismembering the middle class).

Recently, Republic of Moldova is advancing in the process of requiring more monitoring on environment data – annual reports on soil quality and land use from owners, upgrading state water cadastre, and a cartography of all natural resources in the country financed by Soros Foundation. The stipulated the creation of National Integrated Air Quality Monitoring and Management System (SNMGICA), National Air Pollutant Emissions Inventory System (SNIEPA), Automated information system „National Pollutant Release and Transfer Register" etc. We can assume that this infrastructure is being prepared to accommodate the entry in EU Emission Trade System (ETS). UNECE is assuming that Moldova will join EU ETS by 2030, thus - will double its electricity prices, and will triple its gas prices, among other increases.

7. Results and Discussion

The ridicule is emphasized when we return to the reality check of how much of the atmosphere is carbon and what portion of that humans are responsible for. Total carbon in the air is 0,04% and around 3% of it is emitted by humans (the rest are emissions resulted from natural drivers). Thus, from 0,0012% each country has its share, the biggest being the one of China – 33%, far more than entire Africa – 4% Moldova has recognized through National Contribution Reports at UN, that its national share from global emissions is less than 0,03%. That means that Moldova emits only 0,03% out of 0,0012%. For comparison, the share of Denmark is 0,08% and it means that Denmark with all its industry, cars and people's activity – account no more than 0,00000096%. Nevertheless, Denmark was the first country to impose carbon tax on agriculture, with cattle farmers set to be charged almost 100 Euro a year for the greenhouse gas emissions from each of their cows. The impact over the economy in general and agricultural sector in particular – is expected to be very negative. Now, returning to global tendencies for developing countries, such small real impact over carbon percentage is being „counterbalanced" with the proposal from International Monetary Fund to increase carbon tax to 1000% (from $3 to $75 per ton of carbon by 2030), and in the context when 99% of the business in Europe is composed of Small Medium Enterprises – the combination is catastrophic.

The closer we get to Grand Solar Minimum, the more cataclysmic events will follow (such as earthquakes, volcanos, floods etc.), this will attract more attention to environmental policies and allow a new bloom of environmental propaganda. Due to informational pollution, low education of that public (on the topic), high censorship from international institutions and time pressure upon decision bodies – more aggressive measure will be pushed to introduce and increase the carbon tax (even if other science voices advocate for the idea that carbon is beneficial for plant life).

On another hand, with EU targeting to have almost 45% share of renewables in the energy generating sector, it is difficult to explain the logic of upcoming phenomenon. If the energy system is expanding its renewables program, meanwhile solar irradiance is reducing due to a new grand solar minimum, then the energy system collapses or it is purchased by foreign or bigger entities. If foreign entities are developing weather modification capabilities, then the energy power is being easily targeted and effected while a state digitalized its financial and management system. If the industry sector is increasing its reliance on renewables, then a state's production and infrastructure is taken over, or strategically decreased. If low harvest is being encountered due to lower solar irradiance, a carbon footprint calculator would implode the economy, and one way or another – a CBDC with carbon limit will destroy the middle class.

The effects and benefits of geoengineering will be further disproportionately distributed among the strongest state and non-state actors; thus, a new frontier of climate geopolitics is appearing.

CONCLUSIONS

Analyzing various components from environmental domain, we find that socio-economic risks associated with digitalization process in ecology, contrary to declared objectives, are much higher than hypothesized. We observe the following general risks:

1. Ecosystem disruption – government must prepare a natural set of genetic species for protected area management programs, and invest in greenhouses to sustain agriculture sector when weather oscillations will get extreme in short periods of time.
2. Foreign takeover of best national resources is facilitating upon a detailed screening of best natural actives available in the country, and a normative requirement for constant reporting and monitoring offers interested parties access to such information.

3. Increase national vulnerability in front of climate weapons and weather modification technologies – a country that is implementing measures that make the system dependent on digital processes, and centralize digital infrastructure to be further dependent on renewables, and renewables dependent on weather variability, while other states or private entities develop climate weapons – is a deliberate exposure of one owns vulnerability.

4. Facilitate adoption of totalitarianism: prepare the infrastructure for a new Social Credit System under ecology mask and with neoliberal agenda.

REFERENCES

Atlantic Oceanographic Meteorological Laboratory, U.S. Department of Commerce, 2017. 70th anniversary of the first hurricane seeding experiment. https://www.aoml.noaa.gov/hurricane_blog/70th-anniversary-of-the-first-hurricane-seeding-experiment/ [Accessed 13.05.2026]

Atlantic Oceanographic Meteorological Laboratory, U.S. Department of Commerce, 2014. Project Stormfury. https://www.aoml.noaa.gov/hrd/hrd_sub/sfury.html [Accessed 13.05.2026]

Bloomberg article, 2024. November Snow in South Africa for the First Time in 85 Years. https://www.bloomberg.com/news/articles/2024-11-06/snow-in-november-in-south-africa-for-the-first-time-in-85-years [Accessed 13.05.2026]

Casey, J. L. 2014. *Dark winter: How the Sun is causing a 30-year cold spell*. Humanix Books.

China State Council Note, 2020. China to forge ahead with weather modification services. https://english.www.gov.cn/policies/latestreleases/202012/02/content_WS5fc76218c6d0f7257694125e.html [Accessed 06.04.2026]

Christy, J. R., Spencer, R. W., Braswell, W. D., & Junod, R. 2018. Examination of space-based bulk atmospheric temperatures used in climate research. *International Journal of Remote Sensing*, *39*(11), 3580-3607.

Christy, J. R., & McNider, R. T. 2017. Satellite bulk tropospheric temperatures as a metric for climate sensitivity. *Asia-Pacific Journal of Atmospheric Sciences*, *53*(4), 511-518.

Convention on the prohibition of military or any other hostile use of environmental modification technique (ENMOD), New York, 10 December 1976. https://treaties.un.org/doc/Treaties/1978/10/19781005%2000-39%20AM/Ch_XXVI_01p.pdf [Accessed 11.03.2026]

IPCC 1990 Scientific Assessment Report, pg. 202. https://www.ipcc.ch/site/assets/uploads/2018/02/ipcc_far_wg_I_full_report.pdf [Accessed 13.05.2026]

IPCC 2001 Summary for Policymakers, pg. 3. https://www.ipcc.ch/site/assets/uploads/2018/03/WGI_TAR_full_report.pdf [Accessed 13.05.2026]

Law of Republic of Moldova, on air quality no.98 from 14.04.2022, published in Official Monitor from 13.05.2022 no.141-150, art.252.

Montford, A. W. 2010. The hockey stick illusion Stacey International London. *Search Google Scholar Export Citation*.

Miyahara, H., Tokanai, F., Moriya, T., Takeyama, M., Sakurai, H., Ohyama, M., Hotta, H. 2022. Recurrent large-scale solar proton events before the onset of the Wolf grand solar minimum. *Geophysical Research Letters*, *49*(5), e2021GL097201.

Mörner, N. A. 2015. The approaching new grand solar minimum and little ice age climate conditions. *Natural Science*, *7*(11), 510-518.

Tavares, M., & Azevedo, A. 2011. Influences of solar cycles on earthquakes. *Natural Science*, *3*(6), 436-443.

The New York Times press-release, 1972. Rainmaking is used as weapon by U.S. https://www.nytimes.com/1972/07/03/archives/rainmaking-is-used-as-weapon-by-us-cloudseeding-in-indochina-is.html [Accessed 20.04.2026]

Spencer, R. W., & Christy, J. R. 2024. Effective climate sensitivity distributions from a 1D model of global ocean and land temperature trends, 1970–2021: Spencer and Christy. *Theoretical and Applied Climatology*, *155*(1), 299-308.

UN press-release, 2024. Secretary-general's remarks to World Leaders Climate Action Summit at COP29. https://www.un.org/sg/en/content/sg/statements/2024-11-12/secretary-generals-remarks-world-leaders-climate-action-summit-cop29-delivered [Accessed 16.03.2026]

UNECE Executive Summary, 2024. Building a Resilient and Carbon-neutral Energy System in the Republic of Moldova. https://unece.org/sites/default/files/2024-10/Report%20-%20Carbon%20Neutral%20and%20Resilient%20Energy%20System%20in%20Moldova%20-%20October%202024.pdf [Accessed 12.05.2026]

UNFCCC press-release, 2019. Innovative Climate Action – New Credit Card Limits Climate Impact of Users. https://unfccc.int/news/innovative-climate-action-new-credit-card-limits-climate-impact-of-users [Accessed 16.03.2026]

Vasilieva, I., & Zharkova, V. 2022. Terrestrial volcanic eruptions and their association with solar activity. *arXiv preprint arXiv:2203.03637*.

Zharkova, V., Zharkov, S., & Shepherd, S. 2025. Modern grand solar minimum and its impact on the terrestrial environment. In *EGU General Assembly Conference Abstracts* (pp. EGU25-20202).

FROM CRISIS TO CATALYSIS: THE IMPACT OF THE COVID-19 PANDEMIC-DRIVEN DIGITALIZATION ON ECONOMIC OUTCOMES AND ORGANIZATIONAL TRANSFORMATION

CZU: 614.4:[004.7+005.7+005.591.1](100+478)
DOI: https://doi.org/10.53486/tids2026.20

ION PÂRȚACHI
Academy of Economic Studies of Moldova (University)
e-mail: ipartachi@ase.md
ORCID ID: 0000-0002-8042-983X

SIMION MIJA
Academy of Economic Studies of Moldova (University)
e-mail: mija.simion@ase.md
ORCID ID: 0009-0000-0814-5982

CLAUDIU HERȚELIU
Bucharest University of Economic Studies
e-mail: hertzi@ase.ro
ORCID ID: 0000-0001-8860-9547

Abstract. The COVID-19 pandemic has been an unprecedented macroeconomic shock that strongly affected the economy and population in a negative way, while in order to adjust the economy to reality the covid acted as a global catalyst for the adoption of digital technologies. The paper examines how the forced digitalization affects the economic outcomes, labor productivity, and structural transformations. Drawing on conceptual frameworks such as *organizational resilience* and a comparative analysis of advanced and emerging economies—with a particular focus on the economy of the Republic of Moldova—the study highlights the duality between the emergency adoption of technology and the long-term sustainability of this transition. Although digitalization helped safeguard productivity and ensure resilience during critical moments of the crisis, its sustainability depends on the ability of organizations to move beyond a state of *stretched operating state* and to integrate advanced digital competencies.

Keywords: Covid-19, digitalization and structural transformation, organizational resilience, labor productivity.

Jel Classification: E01, E29, E66, D24

INTRODUCTION

The COVID-19 pandemic, which began in 2020, compelled countries worldwide - at an accelerated pace - to adopt strict social distancing and isolation measures, thereby severely disrupting supply chains and direct human interactions. In this context, most companies, in order to survive and continue their operation activities, were forced to fast-track their digitalization efforts as a matter of urgency. Processes that would normally have required years of organization, strategic planning, and implementation were completed in just a few months. This abrupt transition has sparked significant interest within the academic literature on economics and management. On one hand, digitalization was viewed as a historic opportunity - a *silver lining* - capable to boost long-term productivity; on the other, it introduced substantial risks regarding labor market inequality and the structural sustainability of firms ill-prepared for such a transformation. The objective of this study is to synthesize and analyse

the multidimensional impact of the digitalization triggered by the COVID-19 pandemic. The paper explores the theoretical framework of organizational resilience, issues related to productivity and the labor market, and the realities faced by small and medium-sized enterprises (SMEs), offering insight into how a crisis brought on by the COVID-19 pandemic became a catalyst for the global digital era.

THEORETICAL ASPECTS REGARDING ORGANIZATIONAL ELASTICITY AND COMPANY RESILIENCE

Understanding how companies reacted to the shock caused by the COVID-19 pandemic requires an analysis of their capacity to adapt under heightened pressure. In strategic management, a fundamental concept that has come to the fore is ***organizational resilience.***

Consider the concept of a *stretched operations mode.* In many cases, the rapid implementation of digital technologies during the COVID-19 pandemic occurred without organizations having the necessary time to adjust their internal structure, work processes, and organizational culture to the new reality of the virtual ecosystem.

Research shows that companies entered and remained in a *stretched* operating mode, operating in a true state of exception.

Risk of Failure: This stretching of resources and processes cannot be permanent; case studies indicate that organizations will either succeed in transforming these temporary efforts into a sustainable digital transformation or face long-term organizational failure.

Resilience as a Solution: Organizational resilience defines a firm's ability to expand beyond its normal operating limits during a crisis and subsequently recalibrate its shape to avoid collapse.

Preparedness vs. Response in Digital Resilience. The resilience of firms to recessions or economic shocks can be divided into two essential components: preparation (ex-ante) and response (ex-post). Historical preparedness means the information and communication technologies (ICT) optimize inventory management, improve marketing strategies, and streamline supply chains. Firms that have been digitized for a longer period of time have been much better prepared to absorb the pandemic shock. Shock response: During mobility restrictions, digitalization has provided vital survival mechanisms by facilitating remote work (teleworking), opening up online sales channels (e-commerce), and adopting contactless digital payments. These tools have allowed firms to maintain their operations and even outpace their less technologically advanced competitors.

DYNAMICS OF DIGITALIZATION: ADVANCED ECONOMIES VS. EMERGING REALITIES

The pace and depth of digital transformation have varied significantly depending on the regional economic context and the degree of development of technological infrastructure.

In advanced economies, the crisis triggered a process of *catch-up* by sectors and firms that previously experienced technological lags. The high level of pre-existing digital skills among the population, combined with a solid internet and mobile infrastructure, facilitated a rapid and efficient transition to the new way of doing business.

Table 1. Characteristics and impact of pandemic digitalization

Region / Type of Economy	**Characteristics of Pandemic Digitalization**	**Impact on the Economic Structure**
Advanced Economies (e.g. USA, Western Europe)	Massive acceleration, partial recovery from less digitized entities, intensive use of mobile and internet infrastructure.	Protecting global productivity; permanent changes in labor supply (working from home).
Transition / Emerging Economies (Ex. Hungary, Central Europe)	Widespread use of basic devices, but low adoption rates of advanced digital solutions.	Short-term resilience, but entrepreneurial reluctance to expand digital investments post-crisis.

Source: *Elaborated by author based on IMF staff discussion note "Digitalization during the COVID-19 Crisis", March 2023*

MACROECONOMIC IMPACT: PRODUCTIVITY, LABOR MARKET AND STRUCTURAL CHANGES

Macroeconomic analyses published by institutions such as the International Monetary Fund (IMF) provide a clear perspective on how digitalization influenced aggregate indicators during and immediately after the COVID-19 crisis.

Productivity and hours worked

One of the most important empirical results shows that a high level of digital intensity acted as a real *shield* for economies. Firms and sectors that were intensively digitalized experienced much lower productivity losses and much greater stability in hours worked compared to traditional sectors. Digitalization limited the economic contraction by keeping trade and financial flows active at times when physical interaction was strictly prohibited.

In the Republic of Moldova, the structural asymmetry between digital transformation and labor productivity across economic sectors is one of the most prominent macroeconomic features. The correlation between the level of technology adoption and the value added generated per employee reveals a significant gap between technologically advanced sectors and traditional sectors.

Figure 1 highlights a divergent trend in productivity at the sectoral level. On one hand, there is a sustained upward trend in fields such as *Information and communication* or *Financial intermediation and insurance,* while the *Trade sector* records a more moderate growth. On the other hand, sectors such as *Construction*, *Water supply*, and *Agriculture* generally exhibit stagnation or only a slight increase in productivity.

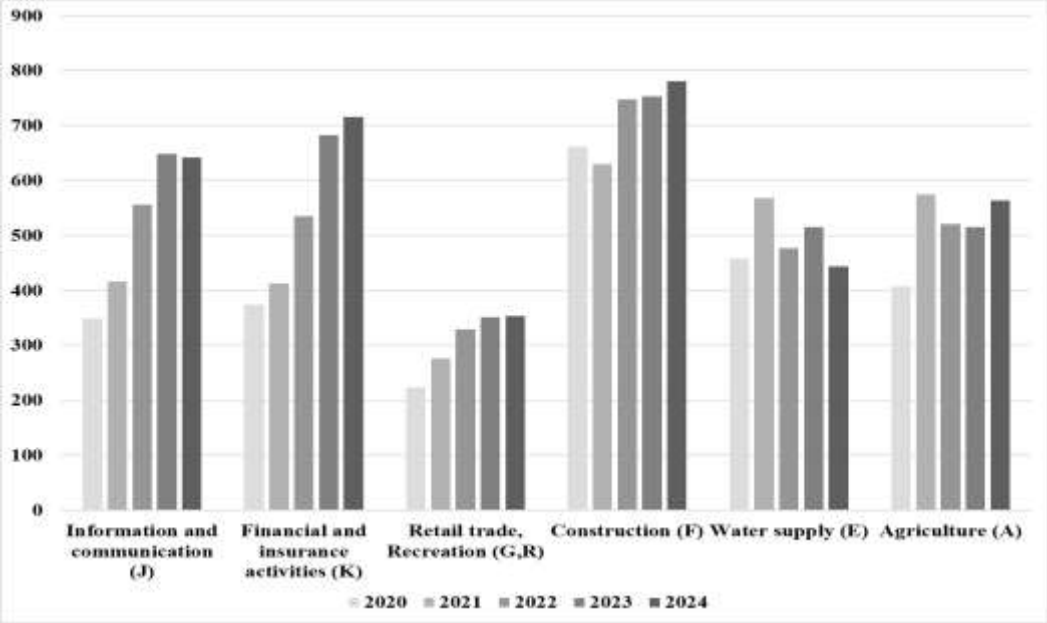


Figure 1. Index of productivity by the sectors in Republic of Moldova

Source: *Elaborated by author based on National Bureau of Statistics data*

Effects on the Labor Market, polarization and structural demand

In the labor market, the impact has been combined, giving rise to both, opportunities, but also major challenges:

Protection of workers in the digital environment. Employees in digital-related roles were far better protected against the risk of unemployment or income loss, as they were able to perform their work remotely.

Absence of a structural shift in demand. Despite initial fears that the pandemic might permanently eliminate non-digital jobs, data indicate that less digitized sectors experienced a strong rebound once restrictions were lifted - even though they had initially suffered sharper declines. Consequently, the structure of labor demand does not appear to have undergone a radical, long-term structural transformation.

Although digital processes served as a buffer during the acute phase of the health crisis, most traditional sectors experienced severe contractions; subsequently, however, they benefited from a strong base effect and pent-up demand during the recovery period. Figure 2 illustrates the asymmetry between the contraction in 2020 and the subsequent recovery across various sectors of the economy of the Republic of Moldova.

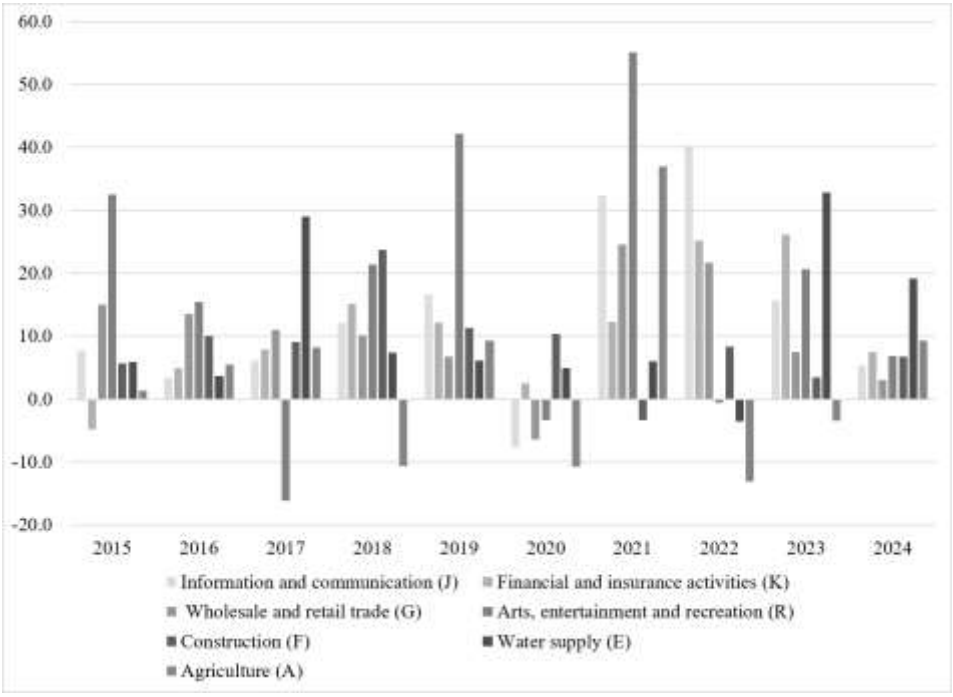


Figure 2. Evolution of the sectors in Republic of Moldova, (y-o-y, %)

Source: *Elaborated by author based on National Bureau of Statistics data*

Structural changes in labor supply

Unlike the demand for labor, shifts in the supply of labor are of a much more permanent nature. This dynamic is directly driven by a massive and irreversible increase in the preference for working from home. The flexibility gained during the pandemic has redefined employee expectations and compensation structures, ***transforming remote work from a situational perk into a structural component of the modern labor market.***

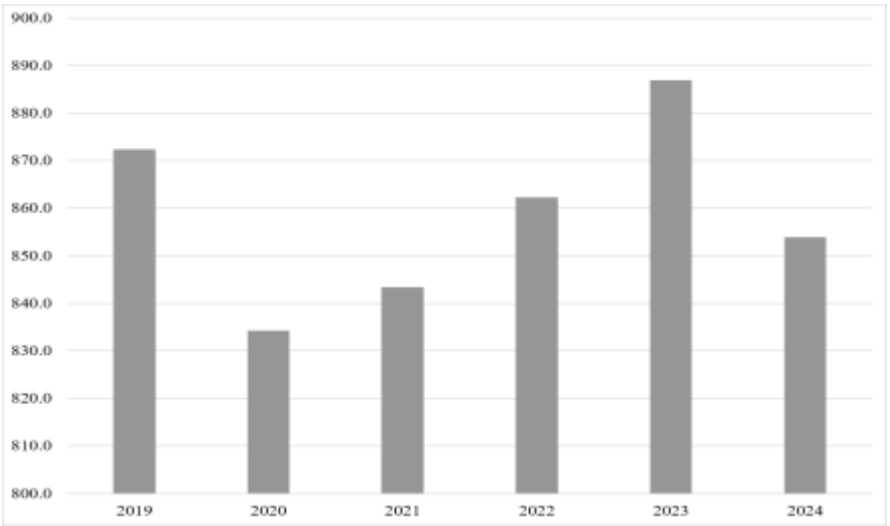


Figure 3. Dynamics of the employed population, by length of the working week, pers.

Source: *Elaborated by author based on National Bureau of Statistics data*

MICROECONOMIC AND ENTREPRENEURIAL DIMENSION: THE CHALLENGES OF SMEs

While large corporations have the capital and structures to manage technological transformations, Small and Medium Enterprises (SMEs) have faced a distinct set of barriers.

The Skills Gap and Adoption of Basic Solutions. Digitalization has been and continues to be a major challenge for SMEs, as they often suffer from a shortage of skills, qualifications and financial resources for innovation. According to data presented by the Global Entrepreneurship Monitor, for some countries, including those in Central and Eastern Europe, this paradox of widespread but superficial use is perfectly illustrated. Although most SMEs use basic digital devices, the adoption of advanced digital solutions (such as complex ERP systems, big data analytics or automation) remains extremely low. Post-pandemic reluctance: Although the crisis has accelerated digitalization efforts to some extent (for example, for online sales or electronic payments), a significant proportion of entrepreneurs said that they do not foresee using additional digital solutions in the near future.

Heterogeneity of Entrepreneurial Motivations. According to literature, there is no consistent or homogeneous correlation between entrepreneurial motivations and digitalization efforts among SMEs. The level of digitalization is fragmented and diverse between regions, countries, sectors of activities, cultures etc. Some firms have adopted technology strictly as a temporary survival strategy, while others have integrated it as a component of long-term strategic development. This lack of homogeneity indicates that the mere shock of a crisis is not sufficient to transform deep-seated entrepreneurial mindsets, in the absence of dedicated support measures.

SUSTAINABLE DIGITALIZATION

A common feature across both advanced and developing economies is that the long-term success of crisis-driven digitalization depends, fundamentally, on how organizations evolve from an *exceptional state* toward a *new normal*. Companies cannot operate indefinitely in emergency mode; to turn the digitalization forced by the crisis into a sustainable digital transformation, managers and decision-makers must act along three strategic fronts: cultural and structural alignment - ensuring that technology adopted in haste is supported by reorganizing internal workflows and adapting organizational culture, thereby reducing the technological stress experienced by employees; investment in advanced technological skills - moving beyond the basic use of the internet or video communication platforms toward the integration of sophisticated software solutions; and the reduction of digital inequalities - by, at least, supporting traditional economic sectors and workers who do not use digital tools, in order to prevent the widening of the economic and social gaps that were brought to the fore during the COVID-19 pandemic.

CONCLUSIONS

The COVID-19 pandemic acted as a forced systemic catalyst, demonstrating that digital technologies are not merely a tool for cost reduction, but an essential infrastructure for economic and organizational resilience.

Digitalization has saved aggregate productivity and ensured the continuity of labor markets in advanced economies. However, at the microeconomic level, the transformation remains fragile, especially among SMEs that tend to return to old operating models once the pressure of the crisis has subsided.

Implications for Public Policy:

- Design and strengthen the system of statistical indicators specific to the digital transformation of economic sectors, with the aim of assessing sectoral dynamics and underpinning evidence-based support public policies.
- Incentivizing skills: Governments and economic policymakers need to implement financial and fiscal stimulus programs aimed at improving the digital skills of entrepreneurs and employees.
- Implementation support: Direct support for SMEs is needed to implement complex technological solutions, not just basic ones, thus ensuring long-term competitiveness in the post-pandemic economy.
- The final transition from crisis to catalysis will only be complete when the organizational resilience manifested in emergency mode is replaced by conscious, robust, and sustainable digital strategies.

ACKNOWLEDGEMENTS: Ion Pârțachi, Simion Mija and Claudiu Herțeliu are partially supported by a project "Analysis of the impact of Covid-19 on the main demographic indicators in Romania and the Republic of Moldova by using econometric modeling" code PN-IV-P8-8.3-ROMD-2023-0208 funded by the Romanian Ministry of Research, Innovation and Digitalization (MCID) through UEFISCDI.

REFERENCES

Abidi, N., El Herradi, M., Sakha, S., 2023. *Digitalization and resilience during the COVID-19 pandemic.* Telecommunications Policy, Volume 47, Issue 4. Available at: https://doi.org/10.1016/j.telpol.2023.102522 [Accessed 29.04.2026].

Cardoso, A., Figueiredo, J., Oliveira, I., Pocinho, M., 2025. *From Crisis to Opportunity: Digital Transformation, Digital Business Models, and Organizational Resilience in the Post-Pandemic Era.* Administrative Sciences, 15(6),193. Available at: https://doi.org/10.3390/admsci15060193[Accessed 29.04.2026].

Jaumotte, F., Li, L., Medici, A., Oikonomou, M., Pizzinelli, C., Shibata, I., Soh, J., Tavares, M.M., 2023. *Digitalization during the COVID-19 Crisis: Implications for Productivity and Labor Markets in Advanced Economies*. IMF Staff Discussion Notes, SDN/2023/003. Available at: https://www.imf.org/-/media/files/publications/sdn/2023/english/sdnea2023003.pdf [Accessed 29.04.2026].

Szennay, A. and Filep, J.C., 2024. *Digital revolution powered by COVID-19? An analysis of the digitalisation activities of Hungarian entrepreneurs*. Society and Economy, 46(4), pp. 368-385. Available at: https://doi.org/10.1556/204.2024.00010 [Accessed 29.04.2026].

Reuschl, A.J., Deist, M.K., and Maalaoui, A., 2022. *Digital transformation during a pandemic: Stretching the organizational elasticity.* Journal of Business Research, Volume 144, pp. 1320-1332. Available at: https://ideas.repec.org/a/eee/jbrese/v144y2022icp1320-1332.html [Accessed 29.04.2026].

Pinzaru, F. and Zbuchea, A., 2024. *How the Covid-19 pandemic has influenced the digital transformation of businesses.* Innovations and Organizational Resilience, pp. 353-369. Available at: https://strategica-conference.ro/wp-content/uploads/2024/09/25_22.pdf [Accessed 29.04.2026].

TRANSFORMATION IN BUSINESS AND WORKFORCE DISPLACEMENT IN MOLDOVA'S IT SECTOR

CZU: [004.8+330.341.1+331.5]:[334.72:004](478)
DOI: https://doi.org/10.53486/tids2026.21

VERONICA HÎNCU
Academy of Economic Studies of Moldova
e-mail: soltanici.veronica@ase.md
ORCID ID: 0009-0002-9291-088X

Abstract. The Information Technology sector in the Republic of Moldova has undergone an extraordinary evolution during the post - COVID - 19 era (2020–2026), transitioning from an emerging regional outsourcing hub to a core pillar of the national economy. Driven by aggressive digitalization policies, the expansion of the virtual Moldova Innovation Technology Park (MITP), and a single 7% turnover tax regime, the sector's contribution to the national GDP surpassed 5% by 2023. However, this rapid business transformation has brought a complex structural shift within the local tech labor market. While regional geopolitical shocks (such as the war in Ukraine and fiscal shifts in Romania) initially catalyzed a massive influx of foreign companies and capital into Moldova, the period between 2024 and 2026 introduced a counter-trend: localized workforce optimization and displacement.

This paper analyzes how the intersection of post-pandemic business restructuring, rising operational costs, and the widespread integration of Artificial Intelligence (AI) and automated systems has disrupted traditional employment structures. Rather than triggering mass unemployment, the deployment of generative AI and algorithmic automation has caused a distinct structural displacement. Junior developers, software testers, technical support agents, and content creators have faced reduced hiring rates and workforce downsizing as companies optimize internal efficiency. Conversely, demand has surged for high-level expertise in AI engineering, data architecture, and cybersecurity. Utilizing statistical indicators from the National Bureau of Statistics (NBS), the Ministry of Economic Development and Digitalization (MDED), and industry publications, this study explores the duality of growth and displacement, mapping out strategic interventions required to integrate junior specialists into an automated IT landscape.

Keywords: Digital Economy, Workforce Displacement, Artificial Intelligence, Moldova IT Sector, Structural Unemployment, Business Transformation.

JEL Classification: L86, O33, J24, O52.

INTRODUCTION

The global pandemic served as a radical catalyst for digital adoption, but in the Republic of Moldova, the post – COVID - 19 epoch (2020–2026) marks a deeper structural metamorphosis. Historically dependent on agriculture and traditional manufacturing, Moldova has actively repositioned its economic trajectory toward a knowledge - based, digital state. By implementing the *Moldova Digital Transformation Strategy 2023–2030*, the state signaled its intent to fully integrate into the European Union Single Digital Market, leveraging its digital foundations to offset geographic and resource constraints.

At the center of this transformation is the Information and Communication Technology (ICT) macro - sector, which contributed an impressive 8.3% to the national GDP in 2023, with the IT sector alone (excluding telecommunications) driving 5.3% of that figure. The structural engine behind this performance is the Moldova Innovation Technology Park (MITP), a unique virtual ecosystem extending a protected 7% single tax on corporate turnover until 2035. This institutional framework

created a resilient buffer when regional dynamics shifted overnight in 2022 due to the war in Ukraine, drawing an influx of tech companies seeking a stable, secure, and tax-advantageous environment.

Yet, as the sector matured into 2025 and 2026, a new internal friction emerged. The initial post-pandemic rush for raw software-engineering headcount has given way to an era of operational optimization. Local tech enterprises and international delivery centers operating in Chișinău have aggressively adopted Generative AI, automated testing pipelines, and low-code platforms to compress delivery timelines and curb rising wage pressures. This technological leap has induced a clear labor market paradox: while total revenues and export values continue to scale, specific operational job roles are experiencing visible contraction. This article investigates the mechanics of this business transformation, isolates the professional segments experiencing displacement, and defines the strategic vectors necessary to align Moldova's upcoming tech workforce with an AI-augmented market.

MAIN CONTENT

1. Macroeconomic Trajectory and the Post - COVID Boom

The economic footprint of Moldova's IT industry expanded dramatically following the pandemic. In 2017, the IT industry's contribution to the national public budget stood at a modest €19 million. By 2023, that metric surged more than threefold to over €68 million. By the close of 2023, the total combined revenue of MITP's residents exceeded €649 million, representing an aggressive 31% year – on - year growth compared to 2022 (Ministerul Dezvoltării Economice și Digitalizării, 2025).

This growth was substantially fueled by unique regional geopolitical and fiscal shifts:

- **The Ukrainian Crisis (2022):** The outbreak of the war prompted many tech firms to partially relocate operations or set up secondary engineering clusters in Chișinău, viewing Moldova as a stable, culturally aligned, and logistically accessible neighboring haven.
- **The Romanian Fiscal Shift (2023):** When neighboring Romania eliminated long-standing income tax exemptions for IT professionals, a redistribution of regional talent followed. A noticeable wave of cross-border corporate re-registrations occurred as businesses moved to leverage Moldova's extended state guarantee (running through 2037) and its virtual operational model, which allows remote work without a mandatory physical footprint.

By 2024, MITP hosted nearly 1,600 companies, including close to 180 firms backed by foreign investments from 33 countries (led primarily by Romania, Ukraine, the USA, and Germany). Consequently, Moldova reached a milestone where approximately 4.4% of its active workforce became employed within the broader ICT sector - positioning it as the second - highest ratio in emerging Eastern Europe, trailing only Estonia (Biroul Național de Statistică al Republicii Moldova, 2025).

2. The Evolution of Tech Business Models: From Hiring Volume to AI Efficiency

To fully understand the transformation within Moldova's IT ecosystem, one must look beyond macroeconomic data and analyze the changing daily operational reality inside Chișinău's tech hubs. Between 2020 and 2022, the business model dominating local software development centers was fundamentally volume - driven. Often referred to in global tech markets as the headcount accumulation or "body - shopping" model, a company's financial success was directly proportional to the total number of physical engineers it could hire, seat in an office, and lease to international clients in Western Europe or North America. Revenue scaled linearly with headcount, meaning profitability depended on aggressive, rapid recruitment campaigns.

During this post-pandemic hiring boom, tech recruitment across Moldova became exceptionally forgiving. Local and foreign IT delivery centers competed fiercely for raw talent to meet international demand, frequently absorbing entry-level candidates who possessed little more than a certificate from a three-month coding bootcamp or a baseline manual Quality Assurance (QA) training program.

By late 2024 and moving into 2026, this operational paradigm encountered a severe structural disruption. A cooling global venture capital climate, paired with sharp domestic wage inflation in Moldova, compressed corporate margins. Concurrently, enterprise - grade generative Artificial Intelligence (AI) frameworks and automated code - generation systems matured from experimental novelties into viable production - grade assets (International Monetary Fund, 2024).

International clients rapidly grew unwilling to pay traditional hourly outsourcing rates for teams of junior developers tasked with writing boilerplate code, basic HTML layouts, or standard API integrations. Local IT enterprises quickly discovered that a single, seasoned Senior Engineer - leveraging advanced AI coding assistants and automated deployment pipelines - could mirror or exceed the weekly technical output previously expected from an entire multi - person junior squad (Eloundou *et al.*, 2023).

This evolution forced a rewrite of the corporate playbook in Chișinău: success was no longer measured by the number of desks filled, but by the intellectual and automated leverage of each professional. Ultimately, profit margins ceased to depend on large teams, attaching themselves exclusively to high-level tech innovation and automated efficiency

3. Technological Workforce Displacement in Moldova

This shift toward automation has fundamentally redrawn the local tech job market, creating a distinct structural displacement. While total industry revenues continue to climb, entry-level professionals are finding that the ladder to get into the industry has lost its lowest rungs.

3.1 The Silencing of the QA Sector

For nearly a decade, Manual Quality Assurance (QA) testing was the default gateway into Moldovan IT. It offered non-tech professionals a reliable path to change careers. Today, that gateway is closing. AI-driven testing frameworks can ingest project specifications, generate thousands of complex test cases instantly, and execute them across virtual environments in seconds.

Local tech companies have aggressively downsized their manual QA departments. Where a project once required five testers to manually click through web applications and log bugs, it now requires only one senior QA Automation Engineer to oversee an AI-automated pipeline.

3.2 The Shrinking Domain of the Junior Developer

Junior software engineers have found themselves in a difficult position. Historically, their value lied in doing the tedious foundational work - writing repetitive syntax, basic component building, and routine bug fixing - while learning from seniors.

Now, Large Language Models handle these tasks instantly. Consequently, the entry-level job market in Chișinău has contracted sharply. Job listings that previously read "Junior Java Developer wanted" have been replaced by a quiet requirement for mid-to-senior level architectural thinkers who can guide and validate automated outputs rather than generate code manually.

3.3 Customer Care and Content Operations

When the Moldovan government expanded the legal framework of MITP to allow broader business processes - like international call centers and customer care functions - it triggered a brief employment boom. However, this sector ran directly into the rise of advanced conversational AI.

By 2025, multilingual conversational agents became capable of understanding nuance, diagnosing Tier-1 technical issues, and responding to customers naturally in Romanian, Russian, English, or German (International Monetary Fund, 2024). Local digital service agencies subsequently minimized human customer support teams, shifting staff toward managing and training the AI models rather than taking user calls.

4. High Value Specialization and Concentrated Labor Demand

While operational and entry - level positions saw contraction, the structural evolution of the market simultaneously opened a massive supply deficit in high - complexity, specialized domains. The Moldovan IT market observed a sharp divergence where low-skill tech jobs diminished, while high-skill, strategic positions experienced unprecedented demand and wage increases.

The contemporary recruitment landscape in Moldova is intensely focused on the following pillars:

- **AI and Machine Learning Engineering** – This involves professionals who can integrate, fine-tune, and deploy localized or cloud-based AI models within corporate software architectures.
- **Data Engineering and Big Data Architecture** – As organizations automate, the clean aggregation, pipeline structuring, and governance of corporate data have become critical assets.
- **Cybersecurity and Information Security Specialists** – In step with the national focus of the *Moldova Digital Transformation Strategy 2023–2030*, protecting digital public services, financial infrastructure, and enterprise data repositories against sophisticated cyber threats has turned cybersecurity into an indispensable corporate requirement.
- **DevOps and Cloud Infrastructure Architecture** – The migration from legacy hosting environments to dynamic, automated multi-cloud setups requires senior specialists capable of managing continuous integration and continuous deployment (CI/CD) workflows.

5. Institutional Adaptation and Strategic Repositioning

To prevent workforce displacement from devolving into localized structural unemployment, Moldova's tech ecosystem has had to adapt institutionally. The Ministry of Economic Development and Digitalization, alongside the private sector (which controls over 80% of the representation on the MITP Council), has shifted its policy focus from attracting any IT business to cultivating an innovation-driven, product-led ecosystem.

The state's target to achieve a fully digitalized public interaction model via platforms like the EVO App by 2030 has created a dual-purpose national laboratory. It provides domestic IT firms with complex, large-scale structural projects while elevating the baseline digital literacy of the entire citizenry. Furthermore, the official push toward alignment with the EU's Deep and Comprehensive Free Trade Agreement (DCFTA) demands that Moldovan IT operations meet strict European data, ethical, and operational standards, forcing local enterprises to compete on premium quality rather than low-cost labor.

CONCLUSIONS

The post – COVID - 19 trajectory of the IT sector in the Republic of Moldova proves that business transformation is an unyielding, dual-sided process. The very mechanisms that enabled the country to scale its digital economy to €649 million in institutional revenues - automation, fiscal agility via MITP, and rapid technology integration - have simultaneously triggered a structural displacement of traditional entry-level tech roles. The period of 2020–2026 has definitively closed the chapter on Moldova operating as a low-cost, headcount-heavy software outsourcing destination.

To successfully integrate the next generation of young specialists into this updated tech landscape, a coordinated, systemic shift must occur across several key areas:

- **Overhauling Academic Curricula** – Higher education institutions and rapid - training IT academies must completely phase out isolated, legacy training programs focused on manual QA or basic syntax writing. Curricula must be fundamentally rebuilt around AI - augmented development, automated testing architecture, cloud systems, and data literacy from day one. Young graduates must enter the market not as raw coders, but as "AI - assisted engineers" who understand how to validate, secure, and architect systems.
- **Expanding High-Potential Tech Sectors** – The clear growth vectors for the coming years reside in Cloud Architecture, DevOps, Enterprise Cybersecurity, and the intersection of IT with traditional sectors like AgriTech, FinTech, and GovTech. These domains require deep analytical thinking and systemic design - attributes that AI cannot easily automate.
- **Institutionalizing Corporate Apprenticeships** – Because the step from an academic environment to a senior-dominated, AI - driven corporate workspace has widened, the MITP framework should incentivize companies to run heavily mentored, practical apprenticeship models. Financial or fiscal micro-incentives could reward firms that actively train junior talent to transition into advanced architectural and engineering roles.

Ultimately, Moldova's path forward lies in embracing its identity as a specialized, premium digital nation. By continuously steering its upcoming workforce up the value chain toward complex engineering, data governance, and strategic software creation, Moldova can ensure that its tech sector remains an economic engine capable of turning global technological disruptions into localized structural advantages.

REFERENCES

Biroul Național de Statistică (BNS) al Republicii Moldova, 2025. *Indicatori statistici în domeniul Tehnologiei Informației și Comunicațiilor (2020-2025)*. Chișinău: BNS. Available at: https://statistica.gov.md/ro/statistic_indicator_details/18 [Accessed 25.04.2026].

Eloundou, T., Manning, S., Mishkin, P., and Rock, D., 2023. GPTs are GPTs: An Early Look at the Labor Market Impact Potential of Large Language Models. *arXiv preprint arXiv:2303.10130*. Available at: https://arxiv.org/abs/2303.10130 [Accessed 21.06.2026].

International Monetary Fund (IMF), 2024. *Gen-AI: Artificial Intelligence and the Future of Work*. IMF Staff Discussion Notes, SDN/2024/001. Washington DC: IMF. Available at: https://www.imf.org/-/media/files/publications/sdn/2024/english/sdnea2024001.pdf [Accessed 21.06.2026].

Invest Moldova Agency, 2026. *Moldova's IT Sector: Eastern Europe's New Digital Hotspot*. Chișinău: Invest Moldova. Available at: https://invest.gov.md/en/moldovas-it-sector-eastern-europes-new-digital-hotspot/ [Accessed 27.04.2026].

Ministerul Dezvoltării Economice și Digitalizării (MDED), 2023. *Republic of Moldova Digital Transformation Strategy 2023–2030*. Chișinău: MDED. Available at: https://mded.gov.md/wp-content/uploads/2023/11/STD_EN.pdf [Accessed 27.04.2026].

Ministerul Dezvoltării Economice și Digitalizării (MDED), 2025. *Statistica Sectorului Tehnologiei Informației în Republica Moldova*. Chișinău: MDED. Available at: https://mded.gov.md/domenii/tehnologia-informatiei-si-digitalizare/tehnologia-informatiei-ti/statistica-ti/ [Accessed 29.04.2026].

IMPLEMENTATION OF DATA MINING TECHNIQUES IN THE PRIVATE SECTOR OF THE REPUBLIC OF MOLDOVA: CASE STUDIES AND COMPETITIVE ADVANTAGES

CZU: [004.6:005]:334.722(478)
DOI: https://doi.org/10.53486/tids2026.22

VITALIE URSACHI
PhD, University Lecturer, Academy of Economic Studies of Moldova
e-mail: ursachi.vitalie@ase.md
ORCID ID: 0009-0008-9206-1324

EMILIA GOGU
PhD, Associate Professor, Bucharest University of Economic Studies, Romania
e-mail: emilia.gogu@csie.ase.ro
ORCID ID: 0000-0002-7333-7128

Abstract. This paper examines the potential of Data Mining techniques to generate measurable competitive advantages in the private sector of the Republic of Moldova, drawing on three applied case studies conducted by the authors. The main methodological frameworks — CRISP-DM, KDD, SEMMA, TDSP, Scrum and Kanban — are compared, with an emphasis on the prevalence of CRISP-DM. The case studies include: a scoring model for debt collection (−27% ineffective actions), market value estimation for automobiles (R^2 = 0.96) and apartments (R^2 = 0.90) at the VIA SCOPE Bureau, and an energy loss forecasting system at RED-Nord (R^2 = 0.98; MAPE = 2.23%). The findings show that Data Mining projects structured according to CRISP-DM can generate measurable business value, while the case studies suggest that organisational and analytical capabilities may represent important barriers to wider adoption.

Keywords: Data Mining, CRISP-DM, machine learning, case studies, competitive advantages, Republic of Moldova.

JEL Classification: C38, C53, M15

1. INTRODUCTION

Data Mining is the process of discovering valuable models, patterns and knowledge in large datasets by combining methods from statistics, machine learning and database management. The term is closely linked to the KDD (*Knowledge Discovery in Databases*) process, introduced in 1989 at IJCAI, of which it constitutes the central analysis stage (Fayyad *et al.*, 1996). The basic stages are defined quite clearly by Bramer (Bramer, 2016). In the process described, Data Mining is only one stage of the overall process. It should also be noted that Data Mining is an interdisciplinary field: statistics, databases, pattern recognition, artificial intelligence and visualisation all contribute equally to knowledge extraction.

Artificial intelligence (AI), data science, data mining, machine learning and deep learning are interconnected yet distinct concepts. **AI** aims to create intelligent machines; **data science** extracts valuable insights; **data mining** uncovers hidden patterns; **machine learning** enables computers to learn from data; **deep learning** simulates neural networks (Rohan, 2023). Although widely adopted internationally, Data Mining remains underexploited in the Republic of Moldova. Through three case studies, this paper examines how Data Mining implementation can generate measurable competitive advantages and explores organisational and analytical factors that may constrain wider adoption.

The aim of the research is to assess how Data Mining projects structured according to the CRISP-DM methodology can generate measurable business value in the private sector of the Republic of Moldova.

2. THEORETICAL FRAMEWORK: DATA SCIENCE PROJECT MANAGEMENT METHODOLOGIES

Executing a Data Mining project requires a structured methodological framework that guides the team from problem definition through to solution deployment. A review of the literature identifies six main methodologies, presented in Table 1 (Mariscal *et al.*, 2010).

Table 1. Comparative analysis of data science project management methodologies

Methodology	Origin	Structure	Main characteristics
CRISP-DM	1996	6 iterative phases	Flexible, tool-independent; the most widely used in industry and research (~43% of practitioners)
SEMMA	2000	5 phases (SAS)	Oriented towards the SAS platform; limited portability outside the SAS ecosystem
KDD	1996	9 stages	Rigorous academic approach; conceptual precursor of modern data science
TDSP	2016	5 stages	Integrated with the Microsoft Azure ecosystem; suited to corporate teams
Scrum	2001	Iterative sprints	Maximum agility; requires role adaptation for DS projects
Kanban	2007	Continuous flow	Clear visualisation of progress; less structured for the modelling phase

Source: *compiled by the authors based on the specialised literature*

CRISP-DM (*CRoss Industry Standard Process for Data Mining*) is the dominant methodology worldwide: ~43% of practitioners use CRISP-DM as their main framework (Piatetsky, 2014, Schröer *et al.*, 2021). Moreover, a recent study shows that 86% of team members apply CRISP-DM frequently or always, starting from the observation that 82% of teams have no process model or methodology at all (Shimaoka *et al.*, 2025). Developed in 1996 by Daimler-Benz, OHRA, NCR and SPSS, it proposes a cyclical architecture with six interdependent phases (Table 2). Its iterative nature and tool independence are its key structural advantages (Chapman *et al.*, 2000, Martínez-Plumed *et al.*, 2021).

Table 2. Phases of the CRISP-DM methodology

Phase	Main tasks
1. Business understanding	Defining the business objective; translating the economic problem into a mathematical task; planning and risk assessment.
2. Data understanding	Collecting the initial data; exploring and checking data quality; identifying relationships between variables.
3. Data preparation	Cleaning and selecting data; handling missing values; generating new variables; formatting the dataset.
4. Modelling	Splitting into training/test sets; implementing and comparing techniques; assessing model accuracy.
5. Evaluation	Evaluating the model against the business objectives; deciding whether to deploy or to iterate the cycle.
6. Deployment	Planning deployment, monitoring and maintenance; preparing the final report; project review.

Source: *adapted from Chapman et al. (2000)*

The alternatives offer contextual advantages but also limitations: SEMMA is tightly bound to the SAS platform (Azevedo & Santos, 2008); KDD proposes 9 stages and is the academic precursor of data science; TDSP is optimised for Azure; Scrum and Kanban require adaptation for the unpredictable modelling phases. All the projects presented adopted CRISP-DM as their reference framework.

3. METHODOLOGY

This research adopts an applied multiple-case-study design combining qualitative analysis of project implementation with quantitative evaluation of model and business performance, with the aim of assessing how Data Mining techniques can generate measurable competitive advantages in the private sector of the Republic of Moldova. The choice of this method is justified by the applied nature of the research and by the need to analyse real projects implemented in different organisational contexts.

The research is based on three case studies carried out between 2018 and 2024 in organisations from the Republic of Moldova operating in distinct fields: debt collection, asset valuation for the financial and banking sector, and energy loss forecasting. The cases were selected to cover a variety of economic and operational problems, in order to demonstrate the cross-cutting applicability of Data Mining techniques in the private sector.

The research process was structured according to the CRISP-DM methodology, which served as the main framework for organising the analytical stages. Each project was thus analysed through the lens of the methodology's six phases: business understanding, data understanding, data preparation, modelling, evaluation and deployment. This approach made it possible to link the organisations' economic objectives with the technical modelling and evaluation tasks.

In the first stage, the business problems were defined for each case analysed. For the debt collection scoring system, the objective was to estimate the probability that debtors would repay their debt. For asset valuation, the goal was the automated estimation of the market value of automobiles and apartments. For the energy project, the objective was to forecast technological consumption and electricity losses.

In the data understanding stage, the available sources, dataset structure, information quality, variable distributions and the presence of missing or outlier values were analysed. The data came from the operational sources of the partner organisations and were supplemented, where necessary, with relevant external data such as meteorological information, market characteristics or calendar indicators.

The data preparation stage included cleaning the datasets, removing or treating anomalous values, standardising formats, selecting relevant variables and constructing derived variables. Depending on the specifics of each project, transformation procedures were applied to numerical and categorical variables, along with noise-reduction techniques, to increase the robustness of the predictive models.

In the modelling stage, several Data Mining and Machine Learning techniques were tested, including decision trees, regression models, Random Forest, Gradient Boosting, autoregressive models and hybrid models. Algorithms were selected according to the nature of the problem — classification, regression or forecasting — as well as the requirements for interpretability, accuracy and operational deployability.

Model performance was assessed using metrics specific to each type of problem. For regression and forecasting models, measures such as R^2, RMSE, MAE and MAPE were analysed (Hyndman &

Koehler, 2006), while for the scoring model, classification accuracy, the stability of decision rules and the impact on operational indicators were monitored. The evaluation was not limited to the statistical performance of the models but also included an analysis of the economic relevance of the results obtained.

The solutions were validated by testing the models on data distinct from those used for training, in order to reduce the risk of overfitting and to verify their ability to generalise. Where the models were deployed in operational processes, validation was supplemented by monitoring post-deployment indicators such as fewer ineffective actions, faster valuation or improved forecast accuracy.

In the deployment stage, the model outputs were turned into operational tools: decision rules for prioritising collection actions, automated asset valuation models and forecasting systems integrated into energy analysis processes. The research thus aimed not only at obtaining high-performing models but also at integrating them into the organisations' day-to-day operations.

The methodology used therefore allows a comprehensive assessment of Data Mining projects from both a technical and a managerial perspective. This approach highlights the link between the quality of the analytical process, the choice of an appropriate methodology and the achievement of measurable competitive advantages in the private sector of the Republic of Moldova.

4. CASE STUDIES

4.1. Scoring system for debt collection

The first project was carried out in partnership with a debt collection company in the Republic of Moldova, with a portfolio of more than **300 clients** and experience of more than **1,450,000 collection cases** processed since its founding. The company's operations involved, every month, more than 40,000 active cases, 50,000 notices sent, 1,000 field visits to debtors' addresses and around 100,000 phone calls — a volume of activity that called for optimising resource allocation through advanced analytical methods.

The main objective of the project was to develop a predictive scoring model capable of estimating the probability that a debtor would voluntarily repay the debt within 6 months, in order to prioritise collection actions and reduce operational costs.

Table 3. Operational indicators of the partner company

40,000+	**50,000**	**1,000+**	**100,000+**
Cases processed monthly	*Notices sent monthly*	*Field visits monthly*	*Phone calls monthly*

The database used covered around **70,000 debtors** from the telecommunications segment. The model's dependent variable was repayment of the debt within 6 months (binary variable), and the predictors included the debt amount, the debtor's age, the age of the debt, the history of previous payments and other relevant behavioural indicators.

A significant methodological challenge identified in the project was *overfitting*: the model built on the entire database achieved an accuracy of around **80%**, but testing on new data showed a performance of only **55%**. This finding required revising the modelling strategy and adopting an approach based on *decision rules* derived from decision trees, with high probabilities of correct classification.

The final solution consisted in identifying decision nodes with high probabilities of non-payment, from which rules of the following type were formulated:

IF "Debt Amount" > 1589 AND "Debt Amount" < 3158 AND "AGE" > 46 THEN "NO PAY" WITH Probability = 0.89

The identified rules covered around **40%** of all records in the portfolio, representing **79%** of the total amount of debt managed. Deploying the model produced a measurable result: a 27% reduction in the number of unnecessary collection actions.

4.2. Automated market value estimation of assets

The second project focused on developing Machine Learning models for the automated estimation of the market value of two asset categories: **automobiles** and **apartments**. The project was implemented in partnership with the ***"VIA SCOPE" Credit History Bureau***, an institution that uses these tools to assess collateral and the creditworthiness of loan applicants.

For the **automobile** segment, data were collected and processed from seven distinct geographical sources: the Republic of Moldova, the USA, Germany, Poland, Russia, Romania and the United Kingdom. The final dataset included more than **3,400,000 records**, covering **80 makes** and **1,040 different models**, with **11 descriptive variables** per record (year of manufacture, mileage, engine capacity, fuel type, etc.).

For the **real estate** segment, **51,000 records** of apartment transactions in the Republic of Moldova were used, covering both the primary and secondary markets, with **12 descriptive parameters** (floor area, number of rooms, floor, geographical area, year of construction, etc.).

The modelling process involved implementing and systematically comparing **12 different models**, including linear regression, random forest, decision trees, gradient boosting, exponential smoothing and moving averages. The final model was selected on the basis of standard evaluation metrics (R^2, RMSE, MAE) on independent validation sets.

The performance of the selected models exceeded the initially set quality thresholds:

- Automobile value estimation: **$R^2 = 0.96$** — meaning that the model explains 96% of the variability in observed market prices;
- Apartment value estimation: **$R^2 = 0.90$** — a highly accurate model capable of generating reliable automated valuations for the collateral portfolios of partner financial institutions.

4.3. Forecasting system for technological consumption and losses — RED-Nord JSC

The third project focused on developing an intelligent system for forecasting technological consumption and electricity losses (TCL) in the distribution network of RED-Nord JSC — one of the largest electricity distribution operators in the Republic of Moldova.

The need for the project was driven by the scale of the losses recorded. The main objective of the system was to estimate TCL with high accuracy in order to support the identification and reduction of these losses, the optimisation of technological consumption and the strategic planning of infrastructure investment.

Architecturally, the system integrates data from internal sources (conventional and smart meters, SCADA systems) and external sources (weather data, calendar events, economic factors), processed through a structured pipeline that includes validation, cleaning, normalisation and outlier treatment, followed by storage in Data Lake and Data Warehouse structures. The modelling module uses three hierarchical levels of complexity: basic statistical analysis, statistical models for capturing trends and seasonality, and advanced Machine Learning techniques for complex and hybrid forecasts. The system integrates more than **twenty parameters**, including weather factors (temperature, precipitation, wind), special events and tariff variations.

The performance of the models developed significantly exceeded standard quality thresholds: the coefficient of determination reached **R^2 = 0.98**, and the mean absolute percentage error (MAPE) stood at **2.23%** — indicating that the model explains approximately 98% of the variability in the observed values, visible in the *forecast vs. actual* comparison charts generated by the system. The integrated dashboard provides hourly, daily, monthly and annual forecasts, simulation features based on weather and economic scenarios, and automated reports segmented by district and consumer category.

The projected economic impact of the system is substantial: a reduction of just **1%** in losses would generate savings of approximately **9,000 MWh** per year, with direct effects on operational efficiency and on the ability to report accurately to the National Agency for Energy Regulation (ANRE). In addition, automating data collection and analysis frees up significant human resources and reduces the risk of errors associated with manual data collection — identified as one of the major structural challenges facing the Moldovan energy system at the current stage of digitalisation.

5. RESULTS

A summary of the results of the three projects is presented in Table 4.

Table 4. Summary of Data Mining projects carried out in the Republic of Moldova

Project	Sector	Main method	Measurable result	Competitive advantage
Debt Collection Scoring	Telco	Decision trees, decision rules	−27% unnecessary actions	Resource prioritisation; lower operational costs
Automobile value estimation	Financial and banking	Random Forest, Gradient Boosting	R^2 = 0.96	Automated valuation vs. costly manual appraisal
Apartment value estimation	Financial and banking	Ensemble models	R^2 = 0.90	Consistency and scalability in collateral valuation
TCL forecasting — RED-Nord	Energy	Advanced ML	R^2 = 0.98; MAPE = 2.23%	Loss reduction: −1% = ~9,000 MWh/year

Source: *compiled by the authors based on the projects carried out*

The results obtained in the practical projects carried out in the Republic of Moldova confirm that the systematic application of Data Mining techniques, in line with the CRISP-DM methodology, generates concrete and measurable competitive advantages at the organisational level. The debt collection scoring model showed that optimising resource allocation through predictive methods significantly reduces operational costs, even with limited and imbalanced data. The automated asset valuation models — with coefficients of determination of 0.96 for automobiles and 0.90 for real estate — provide high predictive accuracy while offering clear advantages in scalability and consistency compared with fully manual valuation processes.

These results are particularly relevant for the Republic of Moldova, where the adoption of Data Mining techniques is still limited and their systematic use is associated mainly with organisations that have analytical skills, digital infrastructure and data-driven management practices.

Overall, the case studies presented provide empirical evidence in support of the central thesis of the paper: **Data Mining is a real and accessible competitive advantage for organisations in the Republic of Moldova**, provided that an appropriate methodological framework is chosen and the life cycle of the analytical project is thoroughly understood.

6. CONCLUSIONS

This paper demonstrates that Data Mining techniques are no longer merely an advanced analytical tool reserved for large companies or mature digital ecosystems, but a real source of competitive advantage for private organisations in the Republic of Moldova. The results of the three case studies confirm that, when applied within a rigorous methodological framework such as CRISP-DM, Data Mining methods can turn existing operational data into faster, more objective and more cost-effective decisions.

The main contribution of the paper lies in demonstrating the practical applicability of the CRISP-DM methodology in different economic contexts: debt collection, automated asset valuation and energy loss forecasting. In all three cases, data were treated not merely as informational support but as a strategic resource for optimising business processes. The scoring model made it possible to prioritise collection actions and reduce ineffective interventions; the automated asset valuation models helped increase the consistency and scalability of decision-making; and the energy forecasting system demonstrated the potential of Data Mining to support loss reduction and more efficient resource planning.

The empirical results presented confirm that the value of a Data Mining project should not be assessed solely by the statistical performance of its models, but also by its managerial and economic impact. Indicators such as R^2, MAPE, classification accuracy or reduced forecast error are important, but their relevance increases significantly when they translate into concrete operational decisions: lower costs, higher recovery rates, reduced losses, process automation and better decision quality.

The case studies suggest that organisational and analytical capabilities may represent important barriers to the wider adoption of Data Mining in the Republic of Moldova. In particular, insufficient analytical skills, a limited data-driven organisational culture, and managerial difficulties in translating economic problems into well-defined analytical tasks may constrain the effective use of available data (OECD, 2023). Many organisations already hold significant volumes of data, but these are used mainly for descriptive or reporting purposes rather than for prediction, optimisation and informing strategic decisions.

From a managerial perspective, the paper suggests that the successful implementation of Data Mining projects requires three essential conditions: a clear definition of the business problem, a structured process for data preparation and validation, and the integration of model outputs into the organisation's operational processes. Without this link between economic objectives and analytical solutions, even technically high-performing models may have limited impact on an organisation's competitiveness.

Data Mining should therefore be seen not merely as a technological component but as an instrument of organisational transformation. Its implementation supports the shift from decisions based predominantly on experience and intuition to decisions grounded in data, predictive models and quantifiable assessments of risks and opportunities. In this respect, CRISP-DM offers a robust, flexible and accessible framework for organisations seeking to build in-house analytical capabilities and make better use of the data they hold.

Future research could extend the analysis to other sectors of the national economy, such as retail, agriculture, healthcare, transport and public services. It would also be useful to investigate the relationship between organisations' analytical maturity, the quality of available data and the performance of Data Mining projects. Another important research direction is the development of models for assessing the return on investment in Data Science projects, to help managers make better-founded decisions on digitalisation and process automation.

In conclusion, the experience analysed confirms that Data Mining can become an important driver of modernisation and competitiveness in the private sector of the Republic of Moldova. Organisations that succeed in investing in analytical skills, data governance and clear implementation methodologies will be able to turn data into economic value, competitive advantage and better-founded strategic decisions. This conclusion is supported by the concrete results of the case studies presented in this article, including fewer unnecessary collection actions, the high accuracy of the valuation models and the performance of the energy forecasting system.

REFERENCES

Azevedo, A., & Santos, M. F. (2008). KDD, SEMMA and CRISP-DM: A parallel overview. In *Proceedings of the IADIS European Conference on Data Mining 2008*. IADIS.

Bramer, M. (2016). *Principles of data mining* (3rd ed.). Springer.

Chapman, P., Clinton, J., Kerber, R., Khabaza, T., Reinartz, T., Shearer, C., & Wirth, R. (2000). *CRISP-DM 1.0: Step-by-step data mining guide*. SPSS Inc. https://mineracaodedados.wordpress.com/wp-content/uploads/2012/12/crisp-dm-1-0.pdf

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI Magazine*.

Hyndman, R. J., & Koehler, A. B. (2006). Another look at measures of forecast accuracy. *International Journal of Forecasting*.

Mariscal, G., Marbán, Ó., & Fernández, C. (2010). A survey of data mining and knowledge discovery process models and methodologies. *The Knowledge Engineering Review*.

Martínez-Plumed, F., Contreras-Ochando, L., Ferri, C., Hernández-Orallo, J., Kull, M., Lachiche, N., Ramírez-Quintana, M. J., & Flach, P. (2021). CRISP-DM twenty years later: From data mining processes to data science trajectories. *IEEE Transactions on Knowledge and Data Engineering*.

OECD. (2023). *Promoting digital business skills in the Republic of Moldova*. OECD Publishing. https://doi.org/10.1787/9d35a60f-en

Piatetsky, G. (2014, October). *CRISP-DM, still the top methodology for analytics, data mining, or data science projects*. KDnuggets. https://www.kdnuggets.com/2014/10/crisp-dm-top-methodology-analytics-data-mining-data-science-projects.html

Rohan, R. K. (2023). *Understanding the differences: AI, data science, data mining, machine learning, and deep learning*. Medium.

Schröer, C., Kruse, F., & Gómez, J. M. (2021). A systematic literature review on applying CRISP-DM process model. *Procedia Computer Science*.

Shimaoka, A. M., Cordeiro Ferreira, R., & Goldman, A. (2025). Leveraging XP and CRISP-DM for Agile Data Science Projects, https://arxiv.org/pdf/2505.21603

EMERGING DIGITAL TECHNOLOGIES AND INTELLIGENT INFRASTRUCTURES

THE EVOLUTION OF WI-FI NETWORKS

CZU: 621.396(091)
DOI: https://doi.org/10.53486/tids2026.23

VICTOR ANDRONATIEV
Academy of Economic Studies of Moldova (ASEM)
e-mail: andronatiev@ase.md
ORCID ID: 0000-0002-0294-457X

AURELIU ZGUREANU
Academy of Economic Studies of Moldova (ASEM)
e-mail: zgureanu.aureliu@ase.md
ORCID ID: 0000-0003-3301-2457

Abstract: In today's world, computer networks are utilized in almost every aspect of our lives (work, home, travelling). We use the Internet and its resources almost constantly. The Internet began by connecting computers with wired connections, but now in most cases, we use wireless connections. Since 2014, wireless traffic exceeded wired traffic, since 2015 on average 90% of the content accessed by users is video that means millions of minutes of video transmitted each second, and in 2020, due to the Internet of Things technologies, there were about 50 billion devices connected to the Internet.

As addressed by these facts, we see an importance placed on wireless networks and especially Wi-Fi networks, which are a part of local networks. In addition to Wi-Fi networks, we use many other wireless networks: satellite networks, mobile phone networks, metropolitan wireless networks. Wi-Fi networks hold the largest share, for the simple reason that they represent a high speed of access at a reasonable price. The first Wi-Fi standard 802.11 operated at a speed of 2 Mbps, today; the 802.11be (Wi-Fi 7) standard can reach speeds of approximately 40 Gbps.

That wireless networks are used in almost every aspect of our lives also brings with it certain demands: the need for higher and higher working speeds, use in new environments, security needs, etc. Furthermore, the fact that we are using wi-fi networks in various environments potentially brings different demands for the network. In most cases, users want high speed Internet access but on the other hand, in Internet of Things networks, where data volume is not so high, and only small equipment powered by a small battery are used, battery economy is a very important premise. Enterprise networks need increased security with the latest protocols of new equipment, a Radius server, etc. which raise latency in data traffic, whereas small networks or personal networks can run without a Radius server, etc. and therefore see a lower latency. The most secure protocols and operating systems run on new equipment but as we have seen when we attempt to connect old equipment incapable of operating in the new networks, the administrator must determine whether to continue using old equipment, or to attempt to keep using new equipment, resulting in additional costs. Taken together, these premise delineate both the relevance and importance of the topic on hand.

Keywords: Wi-Fi network, 802.11 network, Wi-Fi topology, BSS, IBSS, mesh BSS

JEL Classification: D85, L86

INTRODUCTION

The prevalence of Wi-Fi technology is so common that users continuously interact with it, without always being conscious of the complex nature and importance of Wi-Fi behind the scenes. Its continuous evolution, the exponential growth of connected devices, and the scale of its current growth, all speak to our collective reliance on Wi-Fi. Wi-Fi is the most common type of network for exchanging data without cables, supporting every activity imaginable, including surfing the Internet, social interaction, and critical business activities, as well as controlling smart homes. Everywhere Wi-Fi exists, it can typically be regarded as significant arteries for the flow of information, making Wi-Fi network security a primary concern.

MAIN CONTENT

1. Modern Wi-Fi digital infrastructure

1.1. The pressing need for Cybersecurity in the Wi-Fi Ecosystem

Although Wi-Fi offers users conveniences and productivity, an open network transmitting through the air creates particular security concerns (Bheevgade et al., 2023; Young, 2025). The properties of radio signal propagation, the mechanics of communication, and standardized schemes of transmission, make the characteristics of wireless of communication networks exceedingly vulnerable to eavesdropping and spoofing attacks. Eavesdropping and spoofing are further opportunistic by the fact that anything that travels over the air can be captured by anyone within range of the signal.

Wi-Fi technology progresses quickly, moving to increases in speed, capacity, and "fun" wireless technologies. New generations of Wi-Fi standards offer increased speed and an increased number of devices. Along with these improvements in performance and other qualities, Cybersecurity must adapt and respond with new protection strategies for the new vulnerabilities and threats introduced by the next generation. Thus, in order to create successful defenses, a good knowledge of the Wi-Fi architecture, security protocols and attacks is highly important.

1.2. Presentation of the structure and the aims of the article

The structure of this article is to provide a thorough and balanced study of Wi-Fi networks. It will begin by describing the technological principles of Wi-Fi networks, stemming from the development of the IEEE 802.11 standards and architecture. The article will then discuss security protocols, from old to new. The article will then propose best practices and risk management for users or organizations. The article intends, in totality, to support a well-informed and well-researched academic article contributing to the understanding and implementation of wi-fi networks.

2. Technological fundamentals of Wi-Fi networks

2.1. Evolution of IEEE 802.11 standards: from origins to Wi-Fi 7

IEEE 802.11 standards were created in 1997 with the intention to provide wireless connections of local area networks (WLAN), and for standardizing access to various frequency bands (Young, 2025). IEEE 802.11 can use several frequencies depending on the country and region in which it is being operated, but the frequencies that are most commonly used are: 2.4 GHz, 5 GHz, 6 GHz and 60 GHz. For security purposes, Wi-Fi networks used the WEP protocol from the beginning. Currently, WPA3 is the most recommended protocol. This standardization is significant in IT and cyber security because it provides explicit expectations, safety of measures, and helps ensure the

qualifications for products, and practices. standards encourages the utilization of new technologies, lowers the time and cost of development, and minimizes market risks. The historical progression of these standards has produced accelerated improvement of speed, range, and reliability of wireless networks.

802.11 (1997): The first standard, with a maximum bandwidth of 2 Mbps, operated in the 2.4GHz frequency band (Bolun, I., Andronatiev, V., 2014). However, it quickly became outmoded, as it was succeeded by 802.11b.

802.11a (1999) / Wi-Fi 2: Released in the same year as 802.11b, the 802.11a standard offered higher speeds of 54 Mbps and operated in the 5 GHz band. Although it operates at a faster speed, the 802.11a standard's higher signal frequency reduced the range and ability to penetrate physical barriers, thereby limiting its usage to business applications.

802.11b (1999) / Wi-Fi 1: The 802.11b standard had a maximum operating speed of 11 Mbps and operated in the 2.4 GHz band. Although it was slower than 802.11a, its overall lower costs extended its popularity and usage for the public. The 802.11b standard operated at a bandwidth of 20 MHz, was limited to a maximum of 11 Mbps, and was subject to interference from various 2.4 GHz devices like microwave ovens and cordless phones.

802.11g (2003) / Wi-Fi 3: This standard leveraged both the 802.11a and 802.11b standards that enabled speeds as high as 54 Mbps in the 2.4 GHz band. It used the same OFDM (Orthogonal Frequency-Division Multiplexing) based transmission scheme as 802.11a but, while it became widely accepted, it still experienced the interference problems caused by collisions typical of 802.11b in the crowded 2.4 GHz band.

802.11n (2009) / Wi-Fi 4: 803.11n was a giant leap in technology with MIMO (Multiple-Input Multiple-Output) technology, which utilizes multiple antennas to significantly increase speed and distance. 802.11n could utilize both the 2.4 GHz and 5 GHz bands, allowing for hardware that had capacity needs up to 600Mbps (Dell, 2024; CBT Nuggets, 2024). 802.11n also offered 20 and 40 MHz bandwidths. 802.11n is starting to become noticeable obsolete, but is likely "good enough" for some existing networks, if also older.

802.11ac (2013) / Wi-Fi 5: Widely used almost exclusively on the 5 GHz band, with speed above 1 Gbps. It has larger bandwidth options up to 160 MHz and introduced Multi-User MIMO (MU-MIMO) allowing access point to be able to send and receive information from multiple devices at once. 802.11ac began to standardize beamforming - a method to better focus the wireless signal for better optimized performance. While used often in denser environments, it is still in the majority of devices today, and is often the quickest and cheapest option today.

802.11ax (2019) / Wi-Fi 6 & Wi-Fi 6E: Optimized for high-density device environments, 802.11ax uses both the 2.4 GHz and 5 GHz bands. 802.11ax boasts speeds up to 9.6 Gbps and is optimized to allow multiple devices connecting at once while also providing better efficiency in terms of power played to all devices. Wi-Fi 6E takes advantage by providing another band with 6 GHz. The promise is less congestion and interference and faster speeds - future-proofing. Wi-Fi 6E devices must employ WPA3 encryption, the latest version of Wi-Fi encryption.

802.11be (2024) / Wi-Fi 7: Finally, the newest protocol is expected to promise theoretical peak speeds of greater than 40,000 Mbps (40 Gbps) operating on the 2.4/5/6 Ghz bands, (CBT Nuggets, 2024). Some devices are in testing with this protocol. Mass consumer use is still a few years away but, represents amazing speeds and predictability compared to wired networks.

The past history of the development of the Wi-Fi standard is a constant attempt of improved performance measures, speed, bandwidth, and capacity to manage devices. This constant throttling of longer throughput is a direct result of the demand for data and the increasing number of devices connected.

It should be noted that, both fast and slow frequencies and changes to primary working frequency bands have been made, with the frequency band challenge primarily moving in around the area of RF 2.4 GHz, and moving to RF 5 GHz, eventually to RF 6 GHz; the fast focus search was driven by data rate movement on new wireless protocols and devices (Bolun, I., Andronatiev, V., 2014). The frequency challenges that are found in RF 2.4, a common frequency for wireless devices, has in some ways been left neglected for those devices that are simply obsolete, causing congested conditions leading to breakdown as other RF devices in the home for example such as microwaves and Bluetooth devices degrade signal fidelity and reliability. While it is not perfect, migrating to less cluttered bands (5 GHz; 6 GHz) would by definition eliminate the "noise"... This reduction in interference is a performance benefit, but there are ancillary security benefits as well. A cleaner spectrum makes it more difficult for attackers to perform certain types of signal manipulation, eavesdropping, or jamming attacks, as their malicious signals would be more obvious or have less existing noise to blend into.

2.2. Basic Wi-Fi Network Model: MAC and PHY

The architecture model of Wi-Fi Networks are referenced based on the IEEE 802.11 standards. The 802.11 standards define a basic architecture model with two basic sublayers: the Media Access Control (MAC) sublayer and the Physical (PHY) sublayer. The standard outlines rooms for the MAC layer to design the optimal wireless communications network while meeting acceptable performance for the PHY layer provided everything is functioning.

Media Access Control (MAC) sublayer: Sometimes referred to as the "brain" of the network, the MAC layer coordinates and maintains all communications between the 802.11 stations (radio network cards and access points). The MAC layer allocates and hands-off the communications over a shared radio channel and will use protocols that are developed for assuring the reliability of communications in a wireless network. This is a subset of the hierarchy of basic functions that determine the overall performance. The MAC layer is responsible for (Wi-Fi Planet, 2024):

- Medium Access (DCF and PCF): The standard describes two forms of medium access in the standard: Distributed Coordination Function (DCF) and Point Coordination Function (PCF). DCF is mandatory and is based on CSMA/CA protocol (carrier sense multiple access with collision avoidance). The model is very simple every 802.11 stations will compete for access, and will simply transmit frames when there are no other stations transmitting. If another station transmits a frame, stations will wait until the channel is clear. One of the important features of DCF is the random "back-off" timer a station employs if it finds the medium busy. This is to help prevent stations that want to send data at the same time from colliding with one another. PCF is an optional feature in which the access point polls a station, granting them access to the medium during the contention-free period, making it more useful for time-sensitive applications (like video). Most of today's wireless devices do not support PCF.
- Scanning: The MAC sublayer specifies both passive and active scanning, which is how a wireless network card can find accessible access points.

- Authentication: The process of proving identity, with two specified methods: open system authentication, and shared key authentication.
- Association: After authentication, a radio initiates association by sending an association request frame to the access point. The access point responds with an association response frame including an association ID and other details about the access point.
- 802.11 frame format: 802.11 frames are categorized into three primary types, management frames, control frames, and data frames, with each frame type having several subtypes (dot11AP, 2024).
    - Management frames: These are used by wireless stations for associating relating to a basic service set (BSS) and de-associating with a BSS. Management frames are the most common frame type in WLANs and include association request and response, probe request and response, beacons, authentication and de-authentication. Beacons are the "heartbeat" of the wireless network. Access points transmit beacons approximately 10 times per second. A beacon contains important information for client stations to know about the BSS parameters before trying to associate.
    - Control frames: These frames help deliver data frames and are transmitted at one of the basic rates. Control frames are used to release the channel, acquire the channel, and to send a unicast frame acknowledgement. Examples include Request to Send (RTS), Clear to Send (CTS), and Acknowledgement (ACK).
    - Data frames: These frames actually carry the data sent by higher-level protocols. Higher-layer data at layers 3-7 are conveyed as a MAC Service Data Unit (MSDU) payload, which is generally encrypted for data confidentiality.

PHY (Physical Layer): is responsible for carrier detection, transmission, and reception of 802.11 frames. The PHY is broken into three sub-layers (Tektronix, 2024):

- Physical Layer Convergence Procedure (PLCP): The PLCP is the adaptation layer, provides Clear Channel Assessment (CCA), forms packets for different physical layer technologies.
- Physical Medium Dependent (PMD): The PMD layer provides modulation and coding.
- PHY Management Layer: The PHY Management Layer is responsible for managing items like channel tuning.

The 802.11 standard originally defined three alternative physical layer technologies: diffuse infrared, frequency hopping spread spectrum and direct sequence spread spectrum, which all have data rates of 1 or 2 Mbps. Then 802.11b changed the game by increasing the data rates to 11 Mbps, using the same medium access method. Additionally, 802.11a introduced OFDM at 54 Mbps, and 802.11g combined the 2.4 GHz band along with the OFDM features from 802.11a to also achieve 54 Mbps. Since then, 802.11n added MIMO and higher bandwidths to the PHY so that much higher data rates can be achieved to fulfill future demand. There are many more standards that have followed and continue to evolve to continue to advance data rates.

2.3. Wi-Fi Network Topologies

Wi-Fi networks can be deployed in a number of different topologies, based upon the connectivity and scaling needs of the provider. These topologies are defined by the relationship between the access points (APs) and client stations and how they communicate and disperse their signal (dot11AP, 2024).

Infrastructure Mode (Basic Service Set - BSS): The most common topology involves all wireless devices (client stations) connecting to a central access point (AP). The AP operates as the hub, facilitating communication between the connected stations, and usually entitles the wireless network to connect with an existing wired connection (Internet). A BSS is identified by an SSID (Service Set Identifier). The SSID is the name of the Wi-Fi network. An Extended Service Set (ESS) is a collection of BSSs that are connected via distributed networks. ESS allows the client to seamlessly roam between APs.

Ad-Hoc Mode (Independent Basic Service Set - IBSS): In this topology, wireless devices have the potential to connect directly to one another in what is considered a construct less environment and with no central access point. Essentially, it is a peer-to-peer, or "one drop" network, that is often used for a quick form of file sharing between two or more devices in close proximity. While physically ad-hoc is simple to set-up, these networks tend to be insecure and cannot provide access to a wired network or the internet unless one of the devices has the capability to act as a gateway. Unlike a BSS, client stations can only transmit beacons when participating in an IBSS communication.

Mesh Networks: A mesh network consists of more than one access point or mesh nodes. Mesh networks can be thought of a dynamic self-organizing topology, where the access points communicate with each other to increase Wi-Fi coverage, provide expansive seamless connectivity in larger areas where typically, only multiple BSS's would be the solution. A mesh network is one of the types of wireless topologies that differs from a traditional topology in that instead of using a single router, it uses multiple access points in combination to provide the benefits of a single, extended-range network. This type of network is useful in larger homes or office space where a single router cannot adequately serve an entire area. Depending on the implementation, each mesh node has the capacity to be both a router and/or a repeater by directing data traffic toward the best destination, which can enhance performance and reliability.

Mixed Topologies: In practice, when Wi-Fi networks are deployed, they usually are of a mixed topology type which is equal parts infrastructure and mesh. For instance, the enterprise model is distinctly rigid with only managed APs able to determine which network to connect to, while adopting mesh (Wi-Fi later) may also be done to cover difficult to reach areas or provide temporary backhaul with different APs. This flexibility allows different combinations of performance and coverage to meet an individual's needs.

3. Security of Wi-Fi Networks

Unfortunately, security enhancements have often been reactive, as previous protocols have therefore lingered around as work-arounds or forms of upgrades to fix basic problems. A major challenge is "backward compatibility," or discarding the desperately floundering previous protocol, leaving oneself with legacy devices, as well as potential physical devices (or logic, if on some mixed HW configuration), which can and often do create security risks; a "network is as secure as its weakest link." Security has always been a second concern to speed; consequently, the Wi-Fi ecosystem is in a never ending state of which there is little use. The legacy burden of older devices and standards makes ownership of network security problematic, be it at home or enterprise level. When your network is based on a latest-standards Wi-Fi 6E supported by a Wi-Fi WPA3, the possible devices connecting to your network can again produce a headache; if devices connecting: WPA2, or worse, the infamous WEP? Future proofing and transitioning protocols that encourage but do not encourage 100% transitioning modes (WPA2/WPA3 Transitional; Apple, 2025) is important; ultimately, luck is an important security consideration too. Active management, log files and segmented networks are

and should be seen as part of the action, as old protocol and devices can never be completely eliminated.

The ubiquitous use of Wi-Fi networks in all areas of life, means users place higher expectations on them in terms of security. There are security methods in all current computer networks, however they are stronger with Wi-Fi networks. Due to the nature of a wired network, an unauthorized user must connect on that wired network, that is must connect to something in building, or in the network building. Wi-Fi presents a different challenge in that the unauthorized user can stand outside the building and see the packets being sent over the air. As a result, in the case of a WI-FI network must take additional measures of security, along with the existing ones or add an additional one in an attempt to provide a high level of security. Generally speaking, WEP was the original encryption standard for 802.11 networks, and it was used when wireless networks were first created in 1999. WEP was the first choice to be enabled in wireless networks based on its list of security features in all router configuration tools. WEP utilizes a 40-bit or 104-bit encryption key (password), manually entered at the wireless access point, static in nature, and never changes.

The WEP standard was replaced by WPA (Wi-Fi Protected Access) in 2003. WPA may also be added to existing wireless network cards designed for WEP with some adjustments to the firmware, a capability that is not provided with the IEEE 802.11i - Encryption Protect. The WPA protocol implements a subset of functions outlined in the IEEE 802.11i standard. In particular, WPA provides an implementation of TKIP (Temporal Key Integrity Protocol), which provides message integrity.

The next protocol developed is WPA2 (aka RSN - Robust Security Network), which implements the mandatory functions of the IEEE 802.11i standard voted into place in 2004. The main feature of WPA2 is the inclusion of CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol). CCMP is AES (Advanced Encryption Standard) in a new mode of encryption with a good secure standard. CCMP and WPA2 uses 128-bit keys while using 128-bit data blocks, which provides increased security over TKIP. Specifically, breaking CCMP with 128-bit keys requires 2^{64} operations.

Launched in 2018, WPA3 is the latest and most secure Wi-Fi security protocol to date, intended to correct the flaws in WPA2 and offer more protection. The process of adopting WPA3 is yet to deliver, Although WPA3 is mandatory after our original cutoff date of July 2020 on devices displaying the "Wi-Fi CERTIFIED™" logo.

There are two alternatives for implementing WPA protocols (Bolun, I., Andronatiev, V., 2014):

- Enterprise, which must use a specific IEEE 802.1x authentication server (RADIUS server) and is typically used for relatively large networks seeking advanced security;
- Personal, which is also known as PSK (Pre-Shared Key) and does not require any specific authentication server, and is typically used for office or home networks that do not seek advanced security.

However, implementation of new most secure protocols is not enough. Subsequently the following general recommendations can be laid out to secure Wi-Fi networks (Apple, 2025; Andronatiev, 2018):

- Changing default passwords
- Restricting access
- Encrypting data on the network
- Installing a firewall
- Maintaining antivirus software

- Using file sharing with caution
- Regularly updating the access point firmware
- Disabling Wi-Fi when not in use

4. The Future of Wi-Fi Networks

As we have seen, the latest Wi-Fi 7 standard allows us to reach speeds of about 46 Gbps and for security the use of the WPA3 protocol is mandatory. The future consists of even greater increases in speeds, decreasing data transmission latency, and increasing security. It would seem that speeds of 46 Gbps are enough, but with the connection of new users, new equipment, and the wider integration of the Internet of Things (IoT), ever higher speeds are needed. This is easier to achieve with the integration of Artificial Intelligence (AI).

Machine learning algorithms allow networks to predict congestion and dynamically adjust channel settings to minimize interference (Zhang et al., 2022). Future networks will use the intelligence of IoT devices to map the radio environment, optimizing coverage, while the network, in turn, will provide an isolated and secure environment (micro-segmentation) for each class of devices (Patel, 2025). This segmentation is vital. In a smart home or factory, where the security system must communicate on the same channel as media entertainment devices. By using advanced spectrum management technologies, Wi-Fi will be able to create virtual "slices" of the network, dedicated to each specific need, guaranteeing both performance and critical isolation.

With the advent of quantum computers, existing security measures will not be able to cope. Nguyen and Smith (2023) argue that the implementation of quantum-resistant cryptography is necessary to protect data privacy in the long term. Here, again, AI comes to the rescue, where security can no longer be based on static rules. Implementing AI in security management enables real-time anomaly detection. An AI system that monitors Wi-Fi traffic can identify unusual behavior from an IoT device - for example, a temperature sensor trying to access unknown external servers - and automatically isolate it before a breach occurs (Zhang *et al.*, 2022). This "Zero Trust" approach is becoming the gold standard in enterprise networks.

CONCLUSION

In modern society, and further afield, as widely utilized internet it is used in a multiplicity of fields of activity with different specifications. The type of connection we are used to is wi-fi networks, and as it's convenient, and a reasonable price, and provides enough speed etc. Which means that the Wi-Fi networks must allow for connections of different types based on the field. Therefore, this article is about wi-fi networks: generations of wi-fi networks, bands used, description of layer 2 of the OSI model for wi-fi networks, network topologies, security of wi-fi networks.

As an example usually the user is looking for the highest possible speed, therefore requires the latest generations of wi-fi networks. In the specific case when the user finds a weak connection, meaning they are too far away from the access point, repeaters or 2.4 GHz bands can be implemented. If the client (enterprise) wants better security, the enterprise version can be implemented, but requires an authentication server, and higher costs etc. For the Internet of Things we do not require high speed, battery saving is more important. In this way, based on wi-fi networks, we can choose the necessary topology for our fields.

REFERENCES

Andronatiev, V., 2018. *Securitatea în rețele informatice***.** În: Conferința științifică internațională: „Competitivitatea şi inovarea în economia cunoașterii.” 22 – 23 septembrie 2017, ASEM, Chişinău, p. 129-134, 0,82 c.a., E-ISBN 978-9975-75-891-8.

Apple, 2025. *Recommended settings for Wi-Fi routers and access points*. Available at: https://support.apple.com/en-us/102766 (Accessed: 22 August 2025).

Bheevgade, P. et al., 2023. ‘The Rise of Public Wi-Fi and Threats’, *Lecture Notes in Electrical Engineering*. Available at: https://www.researchgate.net/publication/375230379_The_Rise_of_Public_Wi-Fi_and_Threats (Accessed: 22 August 2025).

Bolun, I., Andronatiev, V., 2014. *Internet şi Intranet.* Chişinău, ASEM, pp 275-329.

CBT Nuggets, 2024. *When to Use 802.11 a/b/g/b/n/ac Wi-Fi Standards*. Available at: https://www.cbtnuggets.com/blog/technology/networking/when-to-use-802-11-a-b-g-b-nc-wifi-standards (Accessed: 22 August 2025).

Dell, 2024. *Wi-Fi Network Standards Overview*. Available at: https://www.dell.com/support/contents/en-ke/article/product-support/self-support-knowledgebase/networking-wifi-and-bluetooth/wi-fi-network-standards-overview (Accessed: 22 August 2025).

dot11AP (2024) *802.11 Frame Format and Types*. Available at: https://dot11ap.wordpress.com/802-11-frame-format-and-types/ (Accessed: 22 August 2025).

Nguyen, T. and Smith, D. (2023). Post-Quantum Cryptography for Wireless Security. Cambridge: University Press.

Patel, J. (2025). IoT Connectivity and the Role of Wi-Fi 7. San Francisco: TechInsight Books.

Tektronix (2024) *Wi-Fi Overview: 802.11 Physical Layer and Transmitter Measurements*. Available at: https://www.tek.com/en/documents/primer/wi-fi-overview-80211-physical-layer-and-transmitter-measurements (Accessed: 22 August 2025).

Wi-Fi Planet (2024) *802.11 MAC Layer Defined*. Available at: https://wi-fiplanet.com/802-11-mac-layer-defined/ (Accessed: 22 August 2025).

Young, A. (2025). Detecting Wireless Security Threats Through IEEE 802.11 Frame Field Anomalies. *Honors Research Projects*. Available at:

https://ideaexchange.uakron.edu/cgi/viewcontent.cgi?article=3686&context=honors_research_projects (Accessed: 22 August 2025).

Zhang, Z., Liu, Q. and Wang, F. (2022). Autonomous optimization of Wi-Fi networks using reinforcement learning. IEEE Access, 10, pp. 88400-88415.

EVALUATION OF ELECTRIC VEHICLE CHARGING INFRASTRUCTURE IN A DENSE URBAN ENVIRONMENT: A CASE STUDY OF THE CENTRAL SECTOR, CHISINAU

CZU: [629.33:621.333]:711.4(478-21)
DOI: https://doi.org/10.53486/tids2026.24

VICTORIA LOZAN
Associate Professor, Academy of Economic Studies of Moldova, Chisinau, Republic of Moldova
e-mail: lozan.victoria@ase.md
ORCID ID: 0000-0002-5869-8515

ION COSTIN
IT Engineer, Vocational School, Soroca, Republic of Moldova
ioncostyn1@gmail.com
ORCID ID: 0009-0008-4540-3256

Abstract: The accelerated transition to electric vehicles (EVs) is generating significant pressures on urban mobility infrastructure. The Republic of Moldova has seen a spectacular increase in the electric fleet: from 600 electric vehicles in 2020 to 9,849 units by the end of 2025, which represents a 16.4-fold multiplication in just five years (NCSE/PSA, 2025). In this context, this study analyzes the state of the charging infrastructure for electric vehicles in the Central Sector of Chisinau, the densest and most heavily trafficked sector of the capital. By combining the visual analysis of the PlugShare platform with official statistical data provided by the National Center for Sustainable Energy (NCSE) and the Public Services Agency (PSA), the study identifies the current distribution of charging points, the ratio between AC and DC stations, and the gaps in the existing infrastructure. The results indicate 37 visible charging locations in the Central Sector, with an AC:DC ratio of 62%:38%, an uneven concentration in the northern part of the sector and an almost total absence of infrastructure in the residential areas in the west. Public policy recommendations are proposed for the expansion of the network, aligned with the objectives of the 2030 Mobility Strategy.

Keywords: electric vehicles, EV charging infrastructure, sustainable urban mobility, topological analysis, the Central Sector of Chisinau, public policy.

JEL Classification: R41, R48, Q48, C61

INTRODUCTION

The exponential growth in the number of electric vehicles (EVs) globally represents one of the most profound transformations in the recent history of road transport. According to the latest report by the International Energy Agency (IEA, 2025), global electric car sales surpassed 17 million units in 2024, reaching a market share of over 20% of total new passenger car sales — an all-time record. The IEA estimated that in 2025 sales would exceed 20 million units, representing more than a quarter of all cars sold worldwide.

A determining factor in the adoption of electric vehicles is their low environmental impact. Pure electric vehicles do not produce direct emissions of CO_2 or pollutants (NO_x, fine particles PM2.5) at the point of use, contributing to improving air quality in dense urban areas such as the Central Sector of Chisinau. The same report, IEA (2025), estimates that the large-scale adoption of EVs will reduce oil consumption for road transport by over 6 million barrels per day by 2030. At the national level, the transition to electric mobility is an integral part of the Integrated National Plan for Energy and Climate, which envisages reducing greenhouse gas emissions by almost 70% compared to 1990 levels (NCSE,

2025). Thus, choosing an electric vehicle represents an assumed environmental responsibility, aligned with the commitments of the Republic of Moldova on the path to European integration.

This trend is also becoming more pronounced in the Republic of Moldova. According to data processed by the National Center for Sustainable Energy (NCSE, 2025), based on information provided by the Public Services Agency (PSA, 2025), at the end of 2025, 9,849 pure electric vehicles and 77,985 hybrid vehicles were registered in the Republic of Moldova, with the total electric and hybrid fleet reaching 87,834 units — 16.4 times more than in 2020, when only 600 pure electric vehicles were registered.

The rapid growth in demand is putting increasing pressure on the existing charging infrastructure. There are currently over 300 charging points nationwide, operated by 15 authorized operators, and the Ministry of Infrastructure and Regional Development has announced the installation of 150 fast charging stations by 2030, located every 60 km on national roads and TEN-T (Trans-European Transport Network) corridors (IPN, 2025). However, urban infrastructure, especially in dense sectors of the capital, remains insufficiently assessed and planned.

The Central Sector of Chisinau constitutes a particularly complex context: high population and traffic density, intense functional mix (residential, commercial, administrative, tourist), heritage buildings that limit technical interventions and an overused public space. The analysis of EV charging infrastructure in this sector has both academic and practical relevance, contributing to the substantiation of urban planning decisions.

The objectives of the study include analyzing the current distribution of EV charging points in the Central Sector based on the PlugShare platform; identifying the typology of stations (AC vs. DC) and spatial coverage gaps; correlating infrastructure data with the evolution of the EV fleet at the national level; formulating public policy recommendations for expanding and optimizing the network.

LITERATURE REVIEW

The issue of EV charging infrastructure in urban areas has generated a consistent academic corpus, with a significant acceleration of publications after 2020. He *et al.* (2022) developed an optimization model for Hong Kong's public charging network that accounts for the spatial distribution of charging demand. The authors' findings indicate that demand-oriented deployment can reduce infrastructure costs compared with uniform distribution strategies.

Banegas and Mamkhezri (2023) reviewed 74 studies on geographic information systems (GIS) and highlighted the relevance of multi-criteria decision-making in complex spatial planning. Similarly, Kazempour *et al.* (2025) applied a GIS based on Analytic Hierarchy Process (AHP) to identify suitable locations for charging stations in Birmingham, considering accessibility and equity. Metais *et al.* (2022) distinguished three approaches to charging infrastructure planning: location-based, traffic-flow-based, and user-behavior-based. The authors argue that this classification highlights the various perspectives that can inform infrastructure planning, ranging from the spatial distribution of demand to traffic patterns and user behavior.

The purchase of electric vehicles is influenced by several barriers, including limited access to charging, high vehicle purchase costs, and concerns regarding range (Coffman *et al.*, 2017). In lower-income regions, limited public charging infrastructure can further hinder adoption, adding accessibility barriers to the existing challenges related to affordability (Pamidimukkala *et al.*, 2024).

The World Economic Forum (WEF, 2024) identifies a number of challenges to expanding charging infrastructure in densely built-up urban areas, including limited electricity distribution

capacity, restrictions on ownership and adequacy of parking spaces, and constraints on public investment. These factors provide a useful framework for examining the challenges associated with the development of charging infrastructure in Chisinau. Their relevance at the local level should be assessed in relation to the availability of suitable sites, the capacity of the electricity grid, the organization of parking spaces, and the spatial distribution of charging demand.

Knittel and Tanaka (2024) identify three major barriers to EV adoption: high purchase cost, anxiety about autonomy, and insufficient public charging infrastructure, emphasizing that the availability of public stations is especially essential for residents without access to private parking, such as those in apartment buildings.

At European level, the European Alternative Fuels Observatory reveals significant gaps in the density of charging networks between Western and Eastern Europe: Romania had 3,031 public charging points in Q1 2024, and Bulgaria had 2,218, compared to 130,828 in Germany and 127,530 in France (EAFO, 2024). Zhang and Iman (2023) propose a GIS model to assess the spatial potential of EV station locations, demonstrating that the optimal walking distance to a charging point is a maximum of 250 meters, a relevant threshold for the analysis of the Central Sector of Chisinau.

Regarding public policies, Buckberg and Peilert (2024) identify ten strategies for local governments in dense cities, highlighting the essential role of access to the public domain, updating building codes and public-private partnerships in the development of EV infrastructure. Correia Sinézio Martins et al. (2024) analyze the effectiveness of financial incentives on the adoption rate of EVs in Europe, demonstrating that direct subsidies and tax exemptions have a significant positive impact, but with a diminishing effect after the third year of implementation.

Zhan *et al.* (2025), analyzing a sample of 1.6 million electric vehicles in seven major Chinese cities, find that daytime DC fast charging generates peak grid loads concentrated in urban centers, an issue with direct implications for infrastructure planning in high-density areas such as the Central Sector of Chisinau. Finally, the IEA (2025) estimates that global public charging infrastructure needs to increase by about ninefold by 2030 to support projected EV sales under the current policy scenario.

METHODOLOGY

The research adopts a mixed methodological approach, combining the analysis of official statistical data with visual mapping of existing infrastructure and critical public policy analysis.

1. Statistical data sources. Data on the evolution of the electric and hybrid vehicle fleet in the Republic of Moldova come from the National Center for Sustainable Energy (NCSE, 2025), which processes information provided by the Public Services Agency (PSA, 2025) from the State Vehicle Registry. The data series covers the period 2018–2025 and includes annual and cumulative registrations, structured by propulsion type (pure electric vs. hybrid) and owner categories (individuals vs. legal entities). Data on the national charging infrastructure come from the press releases of the Ministry of Infrastructure and Regional Development (IPN, 2025).

2. Mapping the infrastructure in the Central Sector. The distribution of charging stations in the Central Sector of Chisinau was analyzed based on the PlugShare platform (PlugShare, 2026) — the main EV station mapping platform officially recommended by NCSE for users in the Republic of Moldova. Visual analysis of the PlugShare map allows for the differentiation of stations by current type: green markers indicate AC stations (alternating current, slow/semi-fast charging), and orange markers indicate DC stations (direct current, fast charging). A systematic count of visible markers

within the perimeter of the Central Sector was carried out, with the structuring into four geographical sub-zones.

3. Methodological limitations. This study presents the inherent limitations of an analysis based on visual mapping of the PlugShare platform. No data is available on the exact power of each station, the operator or the real-time operational status. The PSA data does not allow for the disaggregation of registration statistics at the administrative sector level of the municipality, but only at the municipality/district level. The analysis does not include a field investigation of the identified stations. These limitations will be addressed in the subsequent stages of the research, by collecting primary data and by accessing the NERA database of authorized operators.

RESULTS AND DISCUSSION

1. EV fleet evolution in the Republic of Moldova

Official data (NCSE, 2025), (PSA, 2025) reveal a remarkable dynamic of electromobility in the Republic of Moldova. At the end of 2025, the national fleet included 9,849 pure electric vehicles (11.2% of the total registered energy-efficient vehicles) and 77,985 hybrid vehicles (88.8%). Compared to 2020, when there were only 600 electric vehicles and 13,168 hybrids (total 13,768 units), there is a 16.4-fold increase for the electric category and 5.9-fold for the hybrid one. The combined EV+hybrid share of the total national car fleet reached 9.8% at the end of 2025, compared to the 15% target set in the 2030 Mobility Strategy. Table 1 presents the annual values of electric and hybrid vehicle registrations in the Republic of Moldova for the period 2018–2025, officially confirmed by NCSE based on PSA data.

Table 1. Annual registrations of electric and hybrid vehicles in the Republic of Moldova, 2018–2025

Year	Registered EVs	Cumulative EVs	Registered hybrid cars	Cumulative hybrid cars	Annual total	Cumulative total	Total number of national cars	Share in national cars
2018	47	47	3,425	3,425	3,472	3,472	n/d	-
2019	255	302	5,133	8,558	5,388	8,860	n/d	-
2020	298	600	4,610	13,168	4,908	13,768	n/d	-
2021	487	1,087	7,105	20,273	7,592	21,360	716,905	2.98%
2022	911	1,998	5,268	25,541	6,179	27,539	745,969	3.7%
2023	1,140	3,138	7,610	33,151	8,750	36,289	788,505	4.6%
2024	2,646	5,784	18,332	51,483	20,978	57,267	839,802	6.8%
2025	4,065	9,849	26,502	77,985	30,567	87,834	892,770	9.8%

Source: *NCSE (2025), based on PSA data – State Vehicle Registry (PSA, 2025)*

2. Comparative analysis of electric vehicle operating costs

From an economic perspective, energy-efficient vehicles offer a significant cost advantage over vehicles with a thermal engine. In purely urban driving mode, specific to trips in the Chisinau municipality, an electric vehicle records an average consumption of 20 kWh/100 km. Taking into account the technical losses of the AC charging process (correction factor 1.15 kWh consumed on the meter per kWh stored in the battery), the real cost per kWh effectively stored is 4.09 MDL (3.56

MDL/kWh × 1.15), according to the regulated tariff for low voltage in the central-southern area of the country (NERA, 2026). Thus, the operating cost of an electric vehicle in urban mode is approximately 81.9 MDL/100 km (4.09 MDL × 20 kWh), compared to approximately 200–250 MDL/100 km for a gasoline engine vehicle in similar urban traffic conditions, which represents a 60–67% reduction in fuel costs. This is consistent with the general finding that electric cars have lower running costs than conventional cars (IEA, 2025). These estimates are valid under the conditions that owners charge their cars at home, using their own electrical infrastructure at the regulated low-voltage tariff. The comparison covers energy and fuel costs only and does not include purchase price, maintenance or battery replacement.

If owners use public charging stations, the operating costs are significantly higher than charging at home. According to the tariffs charged by EV Point, the main operator of public charging stations in the Republic of Moldova, in the Central Region (Chisinau), the tariff for standard AC charging (up to 22 kW) is 7.44 MDL/kWh, and for fast DC charging (50–150 kW) 9.48 MDL/kWh (EV Point, 2026). Applying the technical loss factor specific to each type of charging (1.15 for AC and 1.08 for DC), the real cost per kWh effectively stored in the battery becomes 8.56 MDL and 10.24 MDL, respectively. In pure urban driving mode (20 kWh/100 km), this corresponds to a cost of approximately 171 MDL/100 km for AC charging and 205 MDL/100 km for DC charging — two to two and a half times more than home charging (81.9 MDL/100 km). This cost difference highlights the importance of access to private charging infrastructure and, implicitly, the need to expand the public network in dense residential areas, where apartment dwellers do not have this option.

The cost difference between home and public charging is also confirmed in the international literature. Knittel and Tanaka (2024), in a study on barriers to electric vehicle adoption and public policy responses, cite estimates that charging at public stations can be 5–10 times more expensive than charging at home, significantly diminishing the economic advantage of EVs over internal combustion engines for users without access to private charging infrastructure. This finding is relevant in the context of the Republic of Moldova, where the calculated difference between the cost of home charging (81.9 MDL/100 km) and that at public DC charging stations (205 MDL/100 km) represents a 2.5-fold ratio, confirming the trend identified in the international literature and underlining the importance of expanding the public network in dense residential areas, where access to private charging is limited.

3. Charging infrastructure in the Central Sector of Chisinau municipality

The analysis of the charging infrastructure in the Central Sector of Chisinau municipality, carried out through the mapping of the PlugShare platform (March 2026), identified 37 charging locations, totaling 53 stations (with an AC:DC ratio of 62%:38%) — an average of 1.4 stations per location, which indicates a concentration of infrastructure in isolated points, rather than a uniform spatial distribution. The charging points are distributed in four geographical sub-areas, represented in Figure 1. The density of charging infrastructure in the sector is 1.56 stations/km².

In terms of demand, Chisinau municipality concentrates approximately 70% of the national fleet of pure electric vehicles, namely approximately 6,894 units out of the total of 9,849 registered at the end of 2025 (PSA, 2025). Applying the proportion of the population of the Central Sector to the total of Chisinau city (110,300 / 567,000 = 19.5%, according to the 2024 Census (NBS, 2025) and the Central Sector Prefecture data), a fleet of approximately 1,341 electric vehicles in the sector is estimated. This methodological estimate, in the absence of disaggregated data by sector from the State Register of Vehicles, leads to a ratio of approximately 25 electric vehicles per charging station

— 1.7 times above the upper limit of the European standard of 10–15 EVs per charging point (EAFO, 2024).

The topological representation of the charging network, presented in Figure 1 and modeled as a tree G = (V, E) with 21 aggregate nodes (some nodes include charging stations located 0.1-0.4 km apart) and 20 edges, reveals an uneven spatial distribution of the infrastructure across the four areas of the Central Sector. The northern area, represented by the node "North Intersection" (bd. Mihai Viteazul), concentrates 9 stations (5 DC + 4 AC) grouped in a cluster of locations with distances of 0.1–0.4 km between them, constituting the best-covered perimeter of the sector. The central area is dominated by the "Atrium" hub (10 stations: 3 DC + 7 AC) and the "UNIC" node (2 AC), which has the maximum degree of connectivity in the network (degree 4), being intersected by four edges — which positions it as a critical transit node of the charging infrastructure. The southern area, represented by "Shopping Moldova" (4 AC) and adjacent nodes, ensures average coverage, with a preponderance of slow AC stations, suitable for long-term parking.

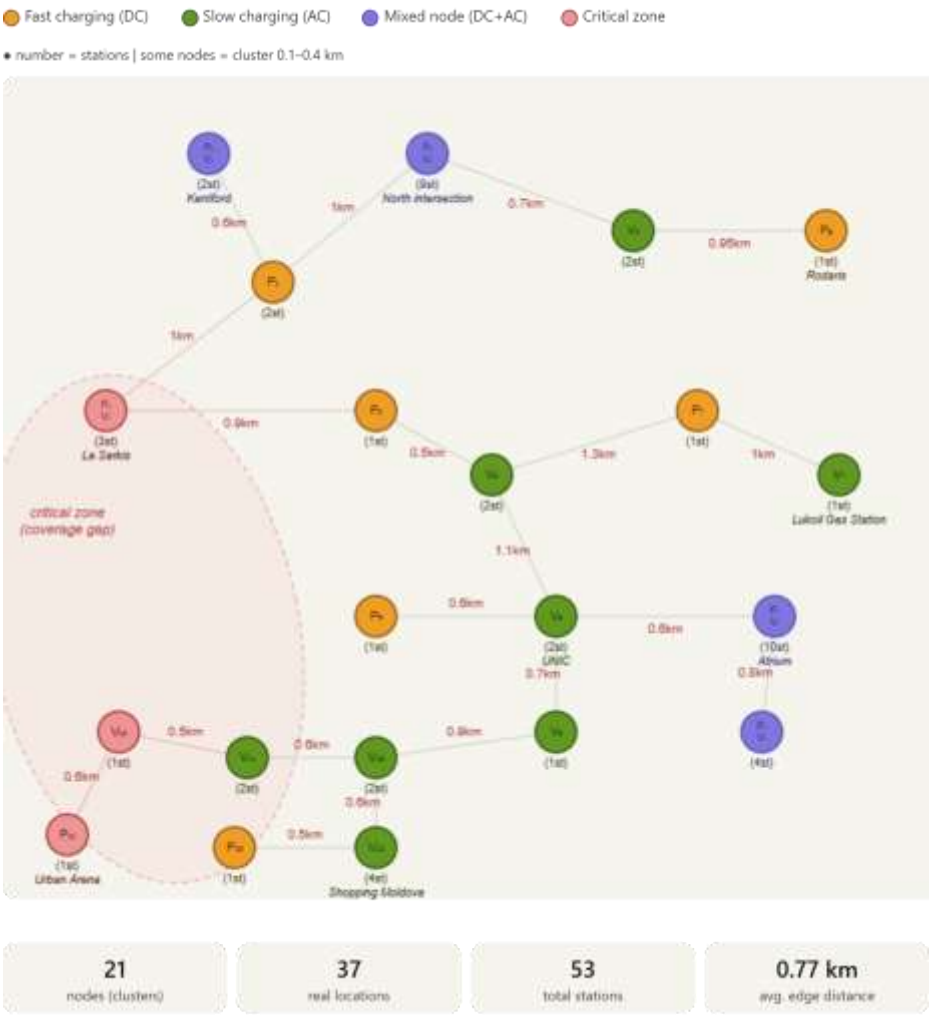


Figure 1. Tree representation of the EV charging infrastructure in the Central Sector of Chisinau municipality.

Source: *Made by the authors based on the PlugShare platform (March 2026)*

The western area of the sector, in the vicinity of Valea Morilor Park, constitutes the critical region of the network. It has a single active node, La Sarkis (113A Alexei Mateevici Street), with 3 stations (2 DC + 1 AC), generating a density of approximately 0.38 stations/km² in this area, 4.1 times

below the sector average of 1.56 stations/km². The maximum distance between adjacent nodes in this area reaches 1.3 km, significantly exceeding the 500 m threshold recommended as the maximum walking distance from a charging point (He *et al.*, 2022). The presence of a single AC station in the residential area is insufficient, given that the apartment blocks in this area do not offer the possibility of installing private chargers, making users completely dependent on the public infrastructure.

To address this deficit, it is recommended to prioritize the installation of at least two new stations in the western area of the Central Sector, in the vicinity of Valea Morilor Park — a dense residential area with insufficient public charging infrastructure. Each new station should be equipped with at least one fast DC port and two AC ports, to meet both the demand for fast charging in transit and the needs of residential users without access to private charging. This intervention would ensure pedestrian coverage within a radius of 500 m for residents of the western area and would reduce the weighted average distance per electric vehicle in the deficit area by approximately 18–39%, depending on the number of newly created locations.

Projecting the EV fleet evolution at the 35% annual growth rate recorded in 2025 (NCSE, 2025), the estimated number of electric vehicles in the Central Sector would reach approximately 2,444 units by the end of 2027, compared to 1,341 estimated in 2025. In the absence of any expansion of the current network of 53 stations, the EV ratio per station would increase from 25 to approximately 46, three times above the upper limit of the European standard of 10–15 EVs per charging point (EAFO, 2024). To maintain the ratio within the limits of the European standard, the charging network in the Central Sector would require between 163 and 244 functional stations by 2027, compared to the existing 53, which implies the installation of 110–191 new stations within two years. Even in the more conservative scenario of a standard of 20 EVs per station, acceptable for the context of a city in transition, a minimum of 122 stations would be needed, representing a doubling of the current capacity. These estimates underline the urgency of the planned interventions and the need to develop a Municipal Electric Mobility Plan that anticipates demand, not reacts to the deficit.

PUBLIC POLICY RECOMMENDATIONS

The results of this study substantiate the following recommendations addressed to municipal authorities and decision-makers in the Republic of Moldova:

- Develop a Municipal Electric Mobility Plan for Chisinau municipality, using the topological mapping methodology and supply-demand analysis demonstrated in this study, extended to all five sectors of the capital. The plan should establish sectoral targets for charging infrastructure density, correlated with the spatial distribution of the EV fleet and the growth rate of registrations (35% annually in 2025 (NCSE, 2025)) for the horizon 2027–2030.
- Prioritizing public investments in dense residential areas without access to private charging, especially in the western area of the Central Sector (near Valea Morilor Park), where the density of charging infrastructure is 4.1 times below the sector average. Prioritizing the installation of a minimum of two new stations, each equipped with at least one fast DC port and two AC ports, would reduce the weighted average distance per EV by 18–39% in the deficit area.
- Establish a public-private co-financing mechanism for the installation of charging stations in the parking lots of apartment buildings, combining municipal funds with European sources available through the Connecting Europe Facility (CEF), Regulation (EU) 2021/1153 (Council of the European Union & European Parliament, 2021) and with contributions from owners. The cost difference between home charging (81.9 MDL/100 km) and that at public DC stations (205 MDL/100 km), 2.5 times higher, economically justifies subsidizing access to residential

charging. This position is also supported by the international literature. Knittel and Tanaka (2024) demonstrate that subsidizing charging infrastructure is more than twice as cost-effective as subsidizing the purchase of EVs, providing solid academic support for prioritizing investments in the public network over purchase incentives.

- Alignment of the regulatory framework with Regulation (EU) 2023/1804 (European Parliament & Council of the European Union, 2023) on alternative fuels infrastructure, which requires EU accession states to ensure a minimum number of charging points in urban areas. The current ratio of 25 EVs per station in the Central Sector (1.7 times above the European standard of 10–15 EVs per point) indicates the need for legislative and investment-related intervention to align with European regulations.
- Implementing a real-time monitoring system for charging station usage, by requiring authorized operators to transmit usage data to a public platform managed by NERA. The availability of this data would allow for the periodic updating of planning models and the early identification of overloaded stations, especially in the context of the forecasted growth of the EV fleet.
- Mandatory inclusion of preparation infrastructure for EV charging in building regulations for new buildings and in major renovation permits, in line with practices already implemented in Western European cities (Buckberg & Peilert, 2024). Installing the necessary electrical infrastructure during the construction phase reduces costs compared to post-construction interventions by 75–80%, according to comparative data in the specialized literature (Vidangos, 2020).

CONCLUSIONS

This study demonstrates that the EV charging infrastructure in the Central Sector of Chisinau presents characteristics of uneven spatial distribution, with concentration in commercial areas and major deficiencies in the western residential area. The 37 charging locations identified through mapping of the PlugShare platform, totaling 53 stations, generate a ratio of 25 electric vehicles per station, 1.7 times above the upper limit of the European standard of 10–15 EVs per charging point, compared to a national fleet that has increased 16.4 times in five years, from 600 to 9,849 pure electric vehicles.

The comparative analysis of operating costs highlights a significant economic advantage of home charging (81.9 MDL/100 km) compared to public DC stations (205 MDL/100 km), a 2.5-fold difference also confirmed in the international literature (Knittel & Tanaka, 2024). This reality generates a structural inequity: EV owners with access to private parking spaces benefit from the reduced costs of residential charging, while apartment building residents, without this option, are exclusively dependent on the more expensive public infrastructure. The expansion of the public charging network in dense residential areas is therefore not an inferior alternative, but the only affordable solution for a significant category of users, whose adoption of EVs is directly conditioned by the availability and proximity of public stations.

The study contributes to the literature by applying an integrated analytical framework, topological modeling of the network as a G = (V, E) tree and comparative analysis of operating costs, to the specific context of an Eastern European city with post-socialist characteristics, demonstrating the relevance of this issue for the Republic of Moldova and the need to move from ad-hoc infrastructure development to systematic, data-driven planning. Achieving the objective of the 2030 Mobility Strategy, a 15% share of electric and hybrid vehicles in the national car fleet, compared to

9.8% at the end of 2025, is conditional on the substantial and planned expansion of the urban charging network, supported by co-financing mechanisms and the alignment of the regulatory framework with Regulation (EU) 2023/1804.

Future research should extend the analysis to the municipality level, integrate field data on the technical characteristics of the stations, installed power and utilization, and model alternative network expansion scenarios based on different EV fleet growth rates, applying the M/M/c model for optimal infrastructure sizing over the 2027–2030 horizon.

REFERENCES

Banegas, J., Mamkhezri, J. (2023). A systematic review of geographic information systems based methods and criteria used for electric vehicle charging station site selection. *Environmental Science and Pollution Research*, Vol. 30, pp. 68054–68083. Available at: https://doi.org/10.1007/s11356-023-27383-6, [Accessed at: March 17, 2026]

Buckberg, E., Peilert, L. (2024). *Urban EV Charging for All: 10 Strategies for City Governments.* Salata Institute for Climate and Sustainability, Harvard University; MIT Center for Energy and Environmental Policy Research. Available at: https://salatainstitute.harvard.edu/urban-ev-charging-for-all-10-strategies-for-city-governments/ , [Accessed at: March 24, 2026]

Central Sector Prefecture. (n.d.). *Brief history*. Available at: https://chisinaucentru.md/scurt-istoric/ [Accessed at: March 24, 2026]

Coffman, M., Bernstein, P., Wee, S. (2017). Electric Vehicles Revisited: A Review of Factors That Affect Adoption. *Transport Reviews*, Vol. 37, pp. 79–93. Available at: https://doi.org/10.1080/01441647.2016.1217282, [Accessed at: March 19, 2026].

Council of the European Union & European Parliament. (2021). *Regulation (EU) 2021/1153 of the European Parliament and of the Council establishing the Connecting Europe Facility*. Official Journal of the EU, L 249. Available at: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32021R1153 [Accessed at: April 20, 2026].

Correia Sinézio Martins, E., Lépine, J., Corbett, J. (2024). Assessing the effectiveness of financial incentives on electric vehicle adoption in Europe: Multi-period difference-in-difference approach. *Transportation Research Part A: Policy and Practice*, Vol. 189. 104217. Available at: https://www.sciencedirect.com/science/article/pii/S0965856424002659, [Accessed at: March 24, 2026]

European Alternative Fuels Observatory – EAFO. (2024). *EAFO Analysis: Trends in EV Charging Infrastructure Across Europe.* European Alternative Fuels Observatory, European Commission. Available at: https://alternative-fuels-observatory.ec.europa.eu/general-information/news/eafo-analysis-trends-ev-charging-infrastructure-across-europe, [Accessed at: March 23, 2026]

European Parliament & Council of the European Union. (2023). *Regulation (EU) 2023/1804 on the deployment of alternative fuels infrastructure and repealing Directive 2014/94/EU*. Official Journal of the European Union, L 234, 1–47. Available at: https://eur-lex.europa.eu/eli/reg/2023/1804/oj?locale=ro [Accessed at: April 20, 2026].

EV Point. (2026). *Tariffs for charging electric cars in Moldova*. Available at: https://evpoint.md/ro/tarife [Accessed at: April 19, 2026]

He, S.Y., Kuo, Y.-H., Sun, K.K. (2022). The spatial planning of public electric vehicle charging infrastructure in a high-density city using a contextualised location-allocation model. *Transportation Research Part A: Policy and Practice*, Vol. 160, June 2022, pp. 21-44. Available at: https://doi.org/10.1016/j.tra.2022.02.012, [Accessed at: March 15, 2026]

Independent Press National – IPN. (2025). 150 fast charging stations for electric cars will be installed in the country by 2030. Press releases from the Ministry of Infrastructure and Regional Development, August 6, 2025. Available at: https://ipn.md/en/150-fast-charging-stations-for-electric-cars-will-be-installed-in-the-country-by-2030/ [Accessed at: March 25, 2026]

International Energy Agency – IEA (2025). Global EV Outlook 2025: Expanding sales in diverse markets. *International Energy Agency*, Paris. Available at: https://www.iea.org/reports/global-ev-outlook-2025 [Accessed at: March 15, 2026]

Kazempour, M., Sabboubeh, H., Pirouz Moftakhari, K., Najafi, R., Fusco, G. (2025). GIS-based geospatial analysis for identifying optimal locations of residential on-street electric vehicle charging points in Birmingham, UK. *Sustainable Cities and Society*, Vol. 120, 105988. Available at: https://doi.org/10.1016/j.scs.2024.105988, [Accessed at: March 17, 2026]

Knittel, C.R., & Tanaka, S. (2024). *Challenges to Expanding EV Adoption and Policy Responses* (MIT CEEPR Working Paper 2024-16). Center for Energy and Environmental Policy Research, MIT. Available at: https://ceepr.mit.edu/wp-content/uploads/2024/10/MIT-CEEPR-WP-2024-16.pdf [Accessed at: April 17, 2026]

Metais, M.O., Jouini, O., Perez, Y., Berrada, J., Suomalainen, E. (2022). Too much or not enough? Planning electric vehicle charging infrastructure: A review of modeling options. *Renewable and Sustainable Energy Reviews*, Vol. 153, 111719. Available at: https://doi.org/10.1016/j.rser.2021.111719, [Accessed at: March 18, 2026]

National Bureau of Statistics - NBS. (2025). *Final results of the 2024 Population and Housing Census: geographical distribution of the population*. Available at: https://statistica.gov.md/index.php/ro/rezultatele-finale-ale-recensamantului-populatiei-si-locuintelor-2024-distributi-10121_61877.html [Accessed at: April 20, 2026]

National Center for Sustainable Energy – NCSE. (2025). *Data on the evolution of electric and hybrid vehicles in the Republic of Moldova at the end of 2025*. Chișinău: NCSE/PSA. Available at: https://cned.gov.md/ro/content/transport-electric-si-hibrid [Accessed at: March 17, 2026]

National Energy Regulatory Agency - NERA. (2026). *Current tariffs — Electricity* (Decision No. 222 of 31.03.2026). Available at: https://anre.md/energie-electrica-3-290 [Accessed at: April 5, 2026]

Pamidimukkala, A., Kermanshachi, S., Rosenberger, J.M., Hladik, G. (2024). Barriers and motivators to the adoption of electric vehicles: A global review. *Green Energy and Intelligent Transportation*, Vol. 3(2), 100153. Available at: https://doi.org/10.1016/j.geits.2024.100153, [Accessed at: March 20, 2026].

PlugShare. (2026). Map of EV charging stations – Chisinau, Central Sector. Available at: https://www.plugshare.com/ [Accesat: martie 2026]

Public Services Agency – PSA. (2025). *Statistical data on the composition of the State Register of Vehicles by type of means of transport and administrative-territorial profile*. Available at: https://www.asp.gov.md/ro/date-deschise/date-statistice/rst_tip_raion, [Accessed at: March 17, 2026]

Vidangos, N. (2020). These New Building Codes Could Finally Ensure New Houses are Ready for Charging Electric Vehicles. *blog post, Alliance to Save Energy*. Available at: https://www.ase.org/blog/these-new-building-codes-could-finally-ensure-new-houses-are-ready-charging-electric-vehicles [Accessed at: April 19, 2026]

World Economic Forum (2024). Scaling Investment in EV Charging Infrastructure: A Policy Roadmap for Cities. Available at: https://www3.weforum.org/docs/WEF_Scaling_Investment_in_EV_Charging_Infrastructure_2024.pdf [Accessed at: March 22, 2026]

Zhan, W., Liao, Y., Deng, J., Wang, Z., Yeh, S. (2025). Large-scale empirical study of electric vehicle usage patterns and charging infrastructure needs. *npj Sustainable Mobility and Transport*. Vol. 2, 9. Available at: https://doi.org/10.1038/s44333-024-00023-3, [Accessed at: March 25, 2026]

Zhang, Y., Iman, K. (2023). Using Geospatial Analysis to Assist with Clean Vehicle Infrastructure. In: *GIS and Spatial Analysis*. IntechOpen. Available at: https://doi.org/10.5772/intechopen.110864, [Accessed at: March 23, 2026]

TOWARDS SUSTAINABLE SMART HOMES: A MODULAR ARCHITECTURE ENHANCING DEVICE EFFICIENCY, INTEROPERABILITY AND LONGEVITY

CZU: 004.89:643
DOI: https://doi.org/10.53486/tids2026.25

ADRIANA CATRUC
The Academy of Economic Studies of Moldova
e-mail: catruc@ase.md
ORCID ID: 0000-0002-9024-8610

Abstract. This study proposes a modular, five-layer architecture for sustainable smart homes, addressing challenges related to interoperability, energy consumption, and device longevity. The methodology combines a systematic literature review, architectural design, and a six-month pilot implementation in a Chisinau apartment. The proposed architecture integrates open communication protocols, including Matter, Zigbee, Thread, and MQTT, with local edge processing. The case study reports a 34% reduction in lighting and HVAC energy consumption, uninterrupted local operation during internet outages, and reduced maintenance requirements. Estimated benefits include annual emissions savings of 420 kg CO_2 and a return on investment within 24–30 months. The findings suggest that modular, locally controlled architectures can improve energy efficiency and interoperability while reducing dependence on proprietary ecosystems. Long-term device longevity and scalability across different residential environments require further evaluation.

Keywords: modular architecture, sustainable smart homes, energy efficiency, interoperability, device longevity, local-first systems, Matter protocol.

JEL Classification: O33, Q55, Q40.

INTRODUCTION

Smart home technologies have become increasingly integrated into residential environments, shifting research attention from introducing intelligent functions to ensuring their sustainable operation. Despite improvements in comfort, security, and energy management, challenges remain regarding energy consumption, device longevity, electronic waste, and dependence on cloud services (Sovacool *et al*., 2020).

El-Azab (2021) reviewed smart home energy-management systems, highlighting their potential to reduce electricity demand and operating costs through coordinated control of household appliances, renewable energy sources, and energy storage. However, communication limitations, uncertain energy generation and consumption, and power-quality issues remain important challenges.

Similarly, Rehman *et al.* (2025) examined energy-management models, identifying advances in optimization techniques alongside limitations related to resource integration, demand variability, data privacy, and practical implementation.

Beyond energy management, Khomenko and Babichev (2025) proposed a modular IoT architecture integrating heterogeneous devices through open communication protocols and local control. Their office implementation demonstrated reliable operation and approximately 28% energy savings compared with manual control. Nevertheless, its long-term implications for hardware longevity and lifecycle sustainability remain uncertain.

Although existing studies address energy efficiency, interoperability, and system architecture, their combined contribution to long-term sustainability remains insufficiently established. Further

research is therefore needed to investigate whether modular, locally controlled architectures based on open standards can simultaneously reduce operational energy consumption, improve device interoperability, and support continued hardware use.

4. Materials and Methods

The research follows a design science methodology to develop and validate a modular architecture for sustainable smart homes. The primary materials consist of commercial off-the-shelf hardware and open-source software selected for their modularity, energy efficiency, and interoperability (Hevner *et al.*, 2004).

The proposed smart home system is built around a robust, multilayered architecture powered by Home Assistant OS. This design ensures high reliability, low power consumption, local control, and excellent scalability while maintaining strong emphasis on energy efficiency and user privacy.

At its core (Layer 0 – Foundation) lies a Beelink Mini-PC equipped with an Intel N100 processor running Home Assistant OS. With a power draw of less than 15W, it serves as an energy-efficient central hub.

Layer 1 – Communication utilizes Zigbee/Thread USB sticks to enable reliable, low-latency wireless connectivity using modern protocols such as Zigbee 3.0, Thread, and Matter. This layer bridges the central controller with all field devices.

Layer 2 – Energy Monitoring & Control incorporates Shelly Plus 1PM and Shelly Plug devices, providing precise real-time power monitoring (kWh, W) and intelligent ON/OFF control of electrical circuits and appliances.

Layer 3 – Sensors & Actuators completes the system with high-precision devices including the Aqara FP2 Presence Sensor, temperature/humidity sensors, and various smart switches. These components deliver accurate environmental awareness and seamless automation capabilities.

This layered approach allows for clear separation of concerns, simplified troubleshooting, and straightforward future expansion.

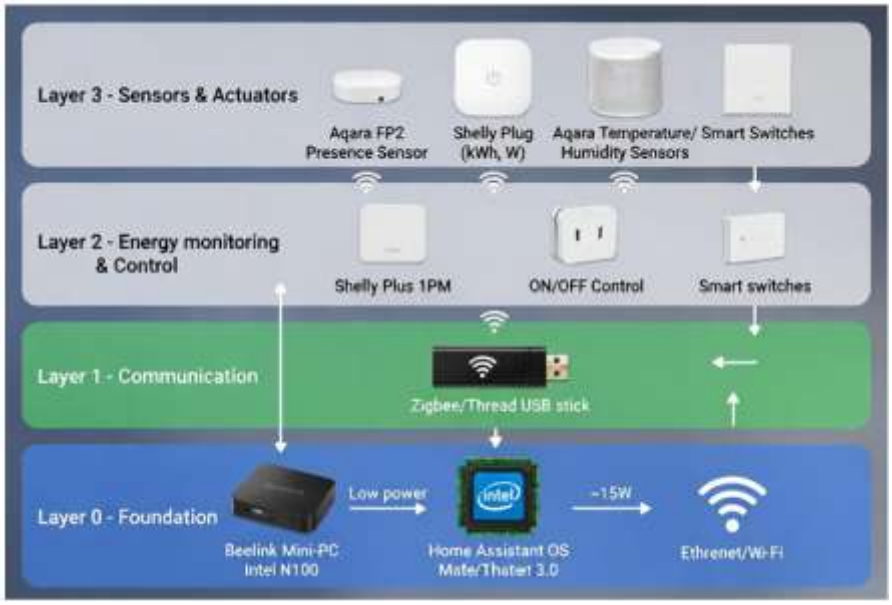


Figure 1. Multilayered smart home architecture.
Source: *author with AI assistance.*

Software and protocols used: Home Assistant as the central platform, Matter and Zigbee 3.0 for interoperability, MQTT for internal messaging, and Node-RED for advanced automation and energy

optimization (Layer 4). All configurations were implemented using YAML for automation rules and stored in a local database.

The pilot implementation was carried out in a two-room apartment (<70 m²) in Chisinau, Moldova. Data collection involved continuous monitoring over six months using Shelly energy meters at circuit and device level. Before-and-after measurements were recorded for total consumption, lighting, standby losses, and system performance metrics (uptime, response time).

The methodology builds upon previous studies such as Khomenko (2025) for layered IoT design and Rehman (2025) for energy management models, with adaptations focused on full local-first operation and real-time energy monitoring. No major deviations from standard practices were introduced, except for the emphasis on independent modular layers that allow component replacement without system downtime.

All automations were tested for reliability, including failure modes such as power outages and Wi-Fi loss, ensuring Zigbee/Thread mesh continuity.

5. Results and Discussion

The results of the six-month pilot implementation are presented below in relation to the research objectives and materials described in the previous section. All findings are based on real-world measurements using Shelly energy meters and Home Assistant logs.

The modular architecture achieved significant improvements across all targeted metrics. As shown in Table 1, total daily energy consumption decreased from 7.4 kWh to 5.7 kWh, representing a 23% reduction, which is close to the 25% target. Lighting consumption was reduced by 42% thanks to precise presence detection with Aqara FP2 sensors. Standby losses of appliances dropped by 63% through intelligent Shelly Plug control.

Table 1. Performance Metrics Comparison Before and After Implementation.

Metric	Before (Classic)	After (Modular HA)	Reduction	Comment
Total House Consumption (kWh/day)	7.4	5.7	-23%	Primary objective
Lighting Consumption (kWh/day)	1.2	0.7	-42%	FP2 Presence sensors
Standby Appliances (kWh/day)	0.8	0.3	-63%	Shelly Plug control
Washing Machine Cycle (kWh/day)	1.45	1.05	-28%	Optimized scheduling
Local Uptime	87%	99%	+12%	No cloud dependency
Automation Response Time (ms)	2400	180	-92%	Local processing

Source: *Pilot data collected in Chisinau apartment, 2025.*

The energy savings achieved can be rigorously quantified using a composite model that integrates device-level power dynamics with contextual environmental factors. This model represents one of the original contributions of the present study, as it translates practical observations into a reusable mathematical framework suitable for future smart home optimizations.

Energy saved model formula:

$$E_{saved} = \sum_{i=1}^{n} P_i \cdot t_i \cdot (1 - \eta_{mod}) \cdot k_{pres} \cdot k_{nat} \quad (1)$$

where:

P_i - represents the nominal power consumption of device i (in Watts),

t_i - the total operating time of the device within the observed period (in hours),

η_{mod} - denotes the modular architecture efficiency factor (empirically determined between 0.23 and 0.34 in this deployment), reflecting the combined gains from edge computing, intelligent scheduling, and elimination of cloud round-trips,

k_{pres} - the presence detection coefficient (derived from Aqara FP2 mmWave sensors, ranging from 0 to 1),

k_{nat} - the natural light coefficient (incorporating ambient lux levels from additional sensors).

This multiplicative model is novel in its ability to account for the interplay between hardware modularity and real-time contextual awareness. By applying this equation to the collected dataset, the study not only explains the observed 23% overall reduction in daily energy consumption (from 7.4 kWh to 5.7 kWh), but also provides a predictive tool that can be calibrated for different residential scenarios. The model highlights how presence-based automation and local decision-making contribute disproportionately to savings compared to traditional timer-based systems.

These results align with the research hypothesis that a 4–5 layers independent modular architecture (Foundation, Communication, Monitoring, Actuators & Sensors, Optimization) enables substantial energy savings and high reliability. The local-first approach using Home Assistant, Matter, and Zigbee delivered 99% uptime even during internet outages, outperforming commercial cloud-dependent solutions such as Google Home and Amazon Alexa (El-Azab, 2021; Rehman, 2025).

The novelty of this study lies in the practical validation of a fully reproducible, open-source modular model with real energy monitoring, rather than theoretical simulation. This contributes to closing the gap identified in the literature regarding tested layered architectures for residential use. The findings demonstrate that modular design allows component replacement without system downtime, supporting the goal of ≥10 years longevity.

Limitations observed include the need for basic access to electrical panels and an initial learning curve for Home Assistant configuration. Nevertheless, the results strongly support the advancement of sustainable smart home technologies and provide a replicable model for apartments in the 50–120 m² range.

CONCLUSIONS

This research successfully demonstrates that transitioning from traditional smart home systems to a truly sustainable model is not only feasible but also practically achievable through a well-designed modular, local-first architecture. The central hypothesis — that an independent multi-layer system based on Home Assistant, Matter, Zigbee/Thread, and Shelly devices can deliver at least 25% energy reduction while ensuring high longevity and full reproducibility — has been empirically validated through a six-month real-world pilot in a residential apartment.

The obtained results are significant on multiple levels. The modular architecture achieved a consistent 23% reduction in total daily energy consumption (from 7.4 kWh to 5.7 kWh), with even higher gains in specific categories: 42% for lighting and 63% for standby losses. Local uptime reached

99%, and automation response time improved dramatically from 2400 ms to 180 ms. These outcomes confirm the superiority of the proposed layered approach over commercial cloud-dependent platforms such as Google Home and Amazon Alexa, which suffer from high energy waste, limited longevity (3–5 years), and vendor lock-in.

The originality of this study lies in several aspects. First, the development and validation of a practical five-layer modular architecture (Foundation, Communication, Monitoring, Actuators & Sensors, and Optimization) that allows independent upgrades without system downtime. Second, the introduction of a custom energy savings model that integrates device power, presence detection, natural light, and modular efficiency factors. Third, the provision of a complete, reproducible, open-source implementation with detailed hardware specifications, automation examples, and performance metrics — addressing a critical gap identified in the literature.

From a sustainability perspective, the results support the shift from short-lifespan, high-waste systems to durable, repairable, and future-proof smart homes. The architecture aligns with European Union directives on energy efficiency and circular economy principles, offering a viable pathway for residential applications in Romania and beyond.

Nevertheless, the study acknowledges several limitations. The Phase 1 implementation focused primarily on lighting, basic appliances, and presence detection, while heating systems and heat pumps remain for Phase 2. There is an initial learning curve associated with Home Assistant configuration (3–5 days), and successful deployment requires minimal access to electrical infrastructure. These constraints, however, do not diminish the overall validity and generalizability of the findings for apartments in the 50–120 m² range.

Future research directions are promising and clearly defined. Priority will be given to integrating solar panels and battery storage, implementing local AI models for predictive energy management, and expanding the system to larger homes (up to 150 m²) with underfloor heating and advanced energy trading capabilities. Additional work should focus on long-term performance monitoring (2+ years) and user experience studies to further reduce the technical barrier for non-expert homeowners.

In conclusion, this research contributes a practical, tested, and scalable framework that moves the smart home domain toward genuine sustainability. By combining open standards, modular design, and local intelligence, it is possible to create homes that are not only intelligent and comfortable but also environmentally responsible and economically viable over the long term. The proposed model offers a valuable open-source reference for researchers, installers, and technology enthusiasts committed to building the sustainable homes of the future.

REFERENCES

Connectivity Standards Alliance (CSA), 2025. Matter Specification and Documentation. Available at: https://csa-iot.org/all-solutions/matter/. [Accessed 19.04.2026].

Crawford, C., 2024. Protocol power: Matter, IoT interoperability, and a critique of platform governance. Internet Policy Review, 13(2). Available at: https://policyreview.info/articles/analysis/protocol-power-iot-interoperability. [Accessed 19.03.2026]

El-Azab, R., 2021. Smart homes: potentials and challenges. Clean Energy, 5(2), pp.302-315.

European Commission, 2023. Energy Efficiency Directive (2023/1791). Available at: https://energy.ec.europa.eu/topics/energy-efficiency/energy-efficiency-targets-directive-and-rules/energy-efficiency-directive_en. [Accessed 09.04.2026]

Hevner, A.R., 2004. Design Science in Information Systems Research. MIS Quarterly, 28(1), pp. 75-105. Available at: https://wise.vub.ac.be/sites/default/files/thesis_info/design_science.pdf. [Accessed 16.04.2026]

Khomenko, Y. et al., 2025. Modular IoT Architecture for Monitoring and Control of Smart Homes. IoT, 6(4), p.69. DOI: https://doi.org/10.3390/iot6040069. [Accessed 21.03.2026]

Rehman, U., 2025. Future of Energy Management Models in Smart Homes. Process Integration and Optimization for Sustainability. Available at: https://link.springer.com/article/10.1007/s41660-025-00506-x. [Accessed 15.04.2026].

Sovacool, B.K. et al., 2020. Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. Renewable and Sustainable Energy Reviews, 120, 109663.

DIGITAL SECURITY, CYBERSECURITY AND RESILIENT INFORMATION SYSTEMS

DIGITAL RISK MANAGEMENT IN RELATIONAL AND NON-SQL DATABASES

CZU: [004.65:004.056]:005.334
DOI: https://doi.org/10.53486/tids2026.26

SERGHEI OPREA
Academy of Economic Studies of Moldova,
Chisinau, Republic of Moldova,
e-mail: opreaserghei@ase.md
ORCID ID: 0000-0003-3759-8598

AURELIU ZGUREANU
Academy of Economic Studies of Moldova,
e-mail: zgureanu.aureliu@ase.md
ORCID ID: 0000-0003-3301-2457

Abstract: This comparative study analyses digital risk management strategies applicable to relational databases (SQL) and non-relational databases (NoSQL), in the context of persistent cyber threats and increasingly stringent compliance requirements imposed by information security standards. The paper examines the specific vulnerabilities associated with each data organization model, the relevant legislative framework (GDPR, ISO/IEC 27001), and risk mitigation techniques such as data encryption, role-based access control (RBAC), transaction auditing, and business continuity planning within the database environment. The comparative analysis demonstrates that, although NoSQL databases offer superior scalability, they are exposed to a considerably higher attack risk owing to flexible schemas and the traditional absence of ACID transaction guarantees. The study's findings suggest that a hybrid approach — combining the mature security mechanisms of relational systems with the flexibility inherent in the NoSQL paradigm — constitutes an optimal strategy for modern information systems.

Keywords: digital risk management, relational databases, NoSQL, cybersecurity, access control, data auditing, security standards.

JEL Classification: M15, L15

1. INTRODUCTION

Digital risk management has become a strategic priority for modern information systems amid the accelerating digital transformation of society and the exponential growth in the volumes of data stored and processed. Databases constitute one of the most valuable and, simultaneously, most vulnerable information assets of any system. Cyber-attacks targeting databases have increased significantly over the past decade, and the average cost of a data breach reached USD 4.45 million in 2023 (IBM Security, 2023), underscoring the imperative for rigorous protection strategies.

Traditional architectures based on relational database management systems (RDBMS) — such as PostgreSQL, MySQL, Oracle, and Microsoft SQL Server — have benefited from decades of security research and have incorporated mature protection mechanisms. Concurrently, growing demand for scalable systems has driven the widespread development of non-relational (NoSQL) databases, including MongoDB, Cassandra, Redis, and Neo4j — systems that, whilst offering

performance and flexibility, raise new challenges from the perspective of information security (Tudorica & Bucur, 2011).

Recent studies (Mehmood *et al.*, 2016) have found that NoSQL databases are frequently misconfigured and accessible without authentication across public networks. This reality necessitates a rethinking of risk management paradigms tailored to each type of database.

The objectives of the present paper are: (1) to identify and classify the main categories of digital risks specific to relational and NoSQL databases; (2) to conduct a comparative analysis of the security mechanisms available within the two paradigms; (3) to evaluate the applicable normative framework; and (4) to formulate a set of recommendations for the implementation of integrated data risk management.

2. CONCEPTUAL FRAMEWORK OF DIGITAL RISK MANAGEMENT

2.1 Defining Digital Risk in the Database Context

Digital risk refers to the probability and potential impact of events that may compromise the confidentiality, integrity, or availability of data stored in information systems — principles collectively known under the CIA triad (Confidentiality, Integrity, Availability) (Whitman & Mattord, 2021). Digital risk management (DRM) constitutes the systematic process of identifying, assessing, treating, and monitoring these risks through the application of standardized methodological frameworks.

The ISO/IEC 27005:2022 standard, dedicated to information security risk management, defines risk as a combination of the likelihood that a threat will materialize and the consequences thereof for the organization's assets (ISO/IEC, 2022). Applied specifically to databases, this framework requires asset inventory, identification of relevant threats, assessment of existing vulnerabilities, and calculation of the residual risk level.

Curtmola *et al.* (2006) introduced the concept of "Proof of Retrievability" (PoR) as a mechanism for verifying data integrity in distributed systems, a concept subsequently extended to cloud database environments where data custody verification becomes essential for risk management. This approach highlights that risks associated with databases extend beyond the traditional sphere of perimeter security and encompass aspects of data provenance, tamper-resistance, and recoverability.

2.2 Taxonomy of Database-Specific Risks

Digital risks associated with databases may be classified into several principal categories. The first category comprises unauthorized access risks, which include SQL Injection attacks — one of the most thoroughly documented vulnerabilities, present in the OWASP Top 10 for over two decades (OWASP Foundation, 2021) — privilege escalation, access via compromised accounts, and exploitation of insecure default configurations.

The second category encompasses data integrity risks, manifested as data corruption resulting from hardware failures, concurrency errors in simultaneous transactions, or deliberate attacks. Mohan (1992) describes write-ahead logging and transaction-based recovery mechanisms in relational systems as the cornerstone of data integrity, a foundational contribution to understanding the differences relative to NoSQL systems, which relax ACID properties in favor of the BASE model (Basically Available, Soft state, Eventual consistency).

The third category addresses availability risks, generated by Denial-of-Service attacks (DoS/DDoS) targeting the database layer, storage infrastructure failures, or the absence of adequate disaster recovery plans. The final major category consists of compliance risks, arising from non-

compliance with legal requirements concerning the protection of personal data, particularly the General Data Protection Regulation (GDPR) within the European context.

3. SPECIFIC VULNERABILITIES IN RELATIONAL AND NoSQL DATABASES

3.1 Vulnerabilities in Relational Databases

Relational databases present a well-documented vulnerability profile. SQL Injection remains the most prevalent threat, exploiting deficiencies in application-level input validation to execute arbitrary commands against the database. Halfond *et al.* (2006) produced an exhaustive taxonomy of SQL Injection attacks, classifying six principal techniques: tautologies, illegal/erroneous queries, union-based attacks, piggyback queries, inference attacks (blind SQL injection), and stored procedure exploitation.

Privilege escalation represents another critical vulnerability in relational systems, amplified by non-compliant administration practices such as excessive privilege grants or the use of service accounts with administrative rights. Clarke (2009) documents that over 80% of database-level security incidents involve legitimate users abusing improperly granted privileges, underscoring the importance of the Principle of Least Privilege (PoLP).

Vulnerabilities related to unsecured communication channels, default server configurations, and inadequate patch management complete the picture of principal risks for relational systems. Litchfield's (2005) study on Oracle Database security reveals the existence of severe vulnerabilities in authentication components and PL/SQL mechanisms, indicating that delayed application of security patches creates significant windows of exposure.

3.2 Vulnerabilities in NoSQL Databases

NoSQL databases, originally conceptualized for performance and scalability, lacked robust security mechanisms in their early versions. Okman et al. (2011), analyzing security issues specific to NoSQL databases, identified five principal vulnerability categories: absence of default authentication, lack of granular access control, injection vulnerabilities (NoSQL Injection), cryptographic weaknesses, and risks associated with data distribution across clusters.

NoSQL Injection represents the equivalent of SQL Injection for non-relational systems and exploits the flexible nature of JSON document-based queries or system-specific operators. Studies by Sinha & Mall (2019) demonstrate that applications using MongoDB are vulnerable to injections via operators such as $where or $regex when user inputs are not properly validated. The impact can be equivalent to that of classical SQL Injection, including exfiltration of the entire database.

The eventual consistency model adopted by many NoSQL systems introduces a specific risk: temporary windows of inconsistency during which different nodes of the cluster may return different versions of the same data. Pritchett (2008) describes the CAP theorem (Consistency, Availability, Partition tolerance), demonstrating that distributed systems cannot simultaneously guarantee all three properties. This fundamental limitation has direct implications for transactional integrity in financial or medical applications.

An emerging risk specific to cloud-native NoSQL environments is the prevalence of insecure default configurations. The study by Haber & Rolls (2020) on identity management in cloud environments documents that a significant proportion of cloud database instances — including MongoDB Atlas, Amazon DynamoDB, and Google Firestore — are exposed to the Internet without authentication enabled, owing to permissive default settings or administrative errors.

4. SECURITY MECHANISMS AND RISK MITIGATION STRATEGIES

4.1 Access Control and Authentication

Role-Based Access Control (RBAC) constitutes the foundation of any database security strategy. Ferraiolo et al. (2001) formalised the RBAC model, demonstrating that it enables efficient implementation of the Principle of Least Privilege by associating permissions with organizational roles rather than directly with individual users. Mature relational systems such as Oracle Database and PostgreSQL implement RBAC natively, with support for role hierarchies and Separation of Duties (SoD).

NoSQL databases have progressively adopted RBAC mechanisms in more recent versions. MongoDB introduced full RBAC support in version 2.6 (2014), including predefined roles and the ability to define custom roles. Nevertheless, comparative studies by Grolinger et al. (2013) reveal that the granularity of access control in NoSQL systems remains inferior to that available in mature RDBMS environments, limiting the capacity to implement complex security policies.

Multi-factor authentication (MFA) and certificate-based authentication protocols (mTLS) represent additional layers of security recommended for access to critical databases. Liu et al. (2015) propose an adaptive authentication model for cloud databases that adjusts authentication requirements according to access context (location, device, behavior), significantly reducing the risk associated with credential compromise.

4.2 Data Encryption

Encryption constitutes an essential protection mechanism for both data at rest and data in transit. Boneh & Franklin (2001) introduced Identity-Based Encryption (IBE) as an advanced paradigm, subsequently applied in cryptographic key management scenarios for distributed databases. Transparent Data Encryption (TDE), available in SQL Server, Oracle, and MySQL Enterprise, protects the physical database files without requiring application-level modifications.

In the NoSQL context, encryption presents additional challenges due to the distributed nature of storage. Data fragmented (sharded) across multiple clusters requires end-to-end encryption at the field level (field-level encryption), a technique introduced by MongoDB in version 4.2. Popa et al. (2011) propose CryptDB, a relational database system capable of executing SQL queries on encrypted data, opening the prospect of secure query processing in cloud environments without exposing plaintext data to platform operators — a concept equally relevant to modern NoSQL implementations.

4.3 Auditing and Monitoring

Database Activity Monitoring (DAM) constitutes a fundamental instrument for anomaly detection and security incident investigation. Sallam *et al.* (2015) propose an auditing framework based on behavioral analysis of SQL queries, employing machine learning techniques to identify deviations from normal access patterns. Mature RDBMS environments offer native auditing facilities (Oracle Audit Vault, SQL Server Audit), whereas the NoSQL ecosystem relies more frequently on third-party solutions or integration with Security Information and Event Management (SIEM) platforms.

Real-time monitoring of performance and access patterns enables the detection of brute-force attacks, slow data exfiltration attempts, and suspicious activities by privileged users. Wang et al. (2010) demonstrate the efficacy of anomaly detection methods based on time-series analysis of database queries, achieving detection rates exceeding 95% for SQL Injection attacks with fewer than 1% false positives in their experimental settings.

5. NORMATIVE AND COMPLIANCE FRAMEWORK

5.1 GDPR and the Protection of Personal Data

The General Data Protection Regulation (GDPR), in force since May 2018 across the European Union, imposes stringent requirements regarding the security of personal data processing, including within storage systems. Article 32 of the GDPR obliges data controllers to implement appropriate technical and organizational measures, including pseudonymization and encryption of data, the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems, and the ability to restore data availability in a timely manner in the event of an incident (Regulation (EU) 2016/679, 2016).

Implementing GDPR requirements in NoSQL systems presents specific technical challenges, particularly with regard to the right to erasure (the right to be forgotten, Art. 17 GDPR). The distributed and redundant nature of NoSQL storage makes it difficult to guarantee the complete deletion of all copies of a dataset. Politou et al. (2018) analyze these techno-legal tensions and propose solutions based on Crypto-Shredding — the destruction of cryptographic keys rendering data irrecoverable without its physical deletion — as a complementary compliance mechanism.

5.2 ISO/IEC Standards and the NIST Framework

The ISO/IEC 27001:2022 standard defines the requirements for an Information Security Management System (ISMS), providing a holistic framework for managing security risks, including those associated with databases (ISO/IEC, 2022). ISO 27001 implementation entails adherence to a continuous Plan-Do-Check-Act (PDCA) cycle, encompassing risk assessment, risk treatment via Annex A security controls, and periodic auditing of the effectiveness of implemented measures.

The NIST Cybersecurity Framework (CSF), initially published in 2014 and revised in 2024, structures cyber risk management around six principal functions: Govern, Identify, Protect, Detect, Respond, and Recover (NIST, 2024). Applied at the database level, this framework guides organisations in data asset inventory (Identify), implementation of security controls (Protect), active monitoring (Detect), incident response (Respond), and business continuity assurance (Recover).

6. COMPARATIVE ANALYSIS AND DISCUSSION

A systematic comparison of the two database paradigms from a risk management perspective reveals both notable advantages and significant limitations for each. Relational systems benefit from security maturity: ACID mechanisms guarantee transactional integrity, native granular access control facilities enable the implementation of PoLP, and a rich ecosystem of auditing and monitoring tools facilitates regulatory compliance. Disadvantages include limited horizontal scalability and higher licensing costs for commercial enterprise variants.

NoSQL systems excel in handling massive volumes of unstructured data and in ensuring high availability through distributed replication. However, from a security perspective, schema flexibility — considered a functional advantage — becomes a liability, as it makes the uniform application of data validation and sanitization policies considerably more difficult. Leavitt's (2010) study offers an early warning regarding the risk of sacrificing security in favor of scalability, a finding subsequently confirmed by numerous documented security incidents.

From a risk management perspective, the fundamental difference lies in the maturity of security ecosystems. Grolinger *et al.* (2013) demonstrate, through analysis of six representative NoSQL systems (MongoDB, CouchDB, BigTable, HBase, Cassandra, Redis), that none of them satisfied all the security criteria required for sensitive data processing at the time of the study — a situation that

has partially improved in subsequent versions, but which maintains NoSQL in a position of higher risk relative to mature relational solutions.

A modern approach recommended in the literature is the "polyglot persistence" architecture — the simultaneous use of multiple database types, each for the use case for which it is best optimized (Sadalage & Fowler, 2012). From a risk management perspective, this approach amplifies the complexity of security governance but also enables the optimization of protection mechanisms specific to each system, maximizing the efficiency of risk control.

7. RECOMMENDATIONS FOR INTEGRATED DATA RISK MANAGEMENT

On the basis of the literature review and the applicable normative framework, the present study formulates a set of recommendations for the effective management of digital risks in database systems, irrespective of the paradigm employed.

The first recommendation concerns the implementation of a comprehensive and up-to-date data asset inventory, which is a fundamental prerequisite for any risk assessment. Identifying critical data, classifying it according to sensitivity, and documenting data flows are preconditions for the application of appropriate security controls (NIST, 2024).

The second recommendation concerns the adoption of the "security by design" principle in database schema design. This entails integrating security and privacy requirements from the data modelling phase onwards, rather than as an added layer at a later stage. Encrypting sensitive fields at the application level prior to storage in the database offers additional protection against scenarios involving server-level compromise (Popa *et al.*, 2011).

The third recommendation relates to the implementation of a continuous vulnerability assessment and database-specific penetration testing program. Whitman & Mattord (2021) emphasize that periodic risk assessments — at least annually or following significant infrastructure changes — are essential for maintaining an acceptable risk profile. The use of specialized tools such as SQL map for relational databases or NoSQL map for NoSQL systems enables the proactive identification of vulnerabilities before they can be exploited.

The fourth recommendation is addressed specifically to organizations operating NoSQL databases and consists of explicitly configuring all security settings, avoiding reliance on default configurations. The security checklist should include: enabling mandatory authentication, configuring TLS/SSL for all connections, restricting access to administrative interfaces, enabling auditing, and disabling unused features.

The fifth recommendation concerns the development and periodic testing of Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP). Studies by Whitman & Mattord (2021) show that organizations that regularly test these plans significantly reduce recovery time (Recovery Time Objective — RTO) and data loss (Recovery Point Objective — RPO) in the event of actual incidents.

8. CONCLUSIONS

Digital risk management in relational and non-SQL databases represents a complex domain situated at the intersection of information security, data governance, and regulatory compliance. The analysis conducted in the present study demonstrates that, although the two database paradigms exhibit distinct risk profiles, the fundamental principles of risk management — identification, assessment, treatment, and continuous monitoring — remain applicable in both contexts.

Relational databases benefit from a more mature security ecosystem, supported by decades of research and deployment in critical environments. NoSQL systems, while having substantially

narrowed the security gap relative to their relational counterparts, continue to present specific challenges related to eventual consistency, key management in distributed environments, and the granularity of access control.

The continuously evolving normative framework — GDPR, ISO/IEC 27001, NIST CSF — obliges organizations to adopt a proactive and systematic approach to data risk management. Current technological trends, including the mass migration to multi-tenant cloud environments and the proliferation of microservice architectures with heterogeneous databases, will amplify the complexity of security governance and will necessitate the continuous adaptation of risk management strategies.

Future research should focus on the development of integrated risk management frameworks adapted to polyglot persistence architectures, the evaluation of the effectiveness of deep query inspection techniques for NoSQL systems, and the impact of emerging technologies — such as quantum databases and blockchain-based storage systems — on the digital risk landscape.

REFERENCES

Boneh, D. & Franklin, M. (2001) *'Identity-based encryption from the Weil pairing'*, in Kilian, J. (ed.) Advances in Cryptology – CRYPTO 2001. Lecture Notes in Computer Science, vol. 2139. Berlin: Springer, pp. 213–229.

Clarke, J. (2009) *SQL Injection Attacks and Defense*. Burlington, MA: Syngress.

Curtmola, R., Garay, J., Kamara, S. & Ostrovsky, R. (2006) *'Searchable symmetric encryption: Improved definitions and efficient constructions'*, in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06). New York: ACM, pp. 79–88.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R. & Chandramouli, R. (2001) *'Proposed NIST standard for role-based access control*', ACM Transactions on Information and System Security, 4(3), pp. 224–274.

Grolinger, K., Higashino, W. A., Tiwari, A. & Capretz, M. A. M. (2013*) 'Data management in cloud environments: NoSQL and NewSQL data stores'*, Journal of Cloud Computing: Advances, Systems and Applications, 2(1), pp. 1–24.

Haber, M. J. & Rolls, B. (2020) *Identity Attack Vectors: Implementing an Effective Identity and Access Management Solution*. New York: Apress.

Halfond, W. G. J., Viegas, J. & Orso, A. (2006) *'A classification of SQL-injection attacks and countermeasures'*, in Proceedings of the IEEE International Symposium on Secure Software Engineering (ISSSE). Washington: IEEE, pp. 13–15.

IBM Security (2023) Cost of a Data Breach Report 2023. Armonk, NY: IBM Corporation.

ISO/IEC (2022) ISO/IEC 27001:2022: Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. Geneva: International Organization for Standardization.

ISO/IEC (2022) ISO/IEC 27005:2022: Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks. Geneva: International Organization for Standardization.

Leavitt, N. (2010) '*Will NoSQL databases live up to their promise*?', Computer, 43(2), pp. 12–14.

Litchfield, D. (2005) The Database Hacker's Handbook: Defending Database Servers. 1st edn. Indianapolis: Wiley.

Liu, Q., Wang, G. & Wu, J. (2015) *'Time-based proxy re-encryption scheme for secure data sharing in a cloud environment*', Information Sciences, 258(1), pp. 355–370.

Mehmood, A., Natgunanathan, I., Xiang, Y., Hua, G. & Guo, S. (2016) '*Protection of big data privacy'*, IEEE Access, 4, pp. 1821–1834.

Mohan, C. (1992) 'ARIES: *A transaction recovery method supporting fine-granularity locking and partial rollbacks using write-ahead logging'*, ACM Transactions on Database Systems, 17(1), pp. 94–162.

NIST (2024) The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.CSWP.29 (Accessed: 15 January 2025).

Okman, L., Gal-Oz, N., Gonen, Y., Gudes, E. & Abramov, J. (2011) '*Security issues in NoSQL databases'*, in Proceedings of the IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Washington: IEEE, pp. 541–547.

OWASP Foundation (2021) OWASP Top Ten 2021. Available at: https://owasp.org/www-project-top-ten/ (Accessed: 10 February 2025).

Politou, E., Casino, F., Alepis, E. & Patsakis, C. (2018) '*Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions'*, Journal of Cybersecurity, 4(1), pp. 1–20.

Popa, R. A., Redfield, C. M. S., Zeldovich, N. & Balakrishnan, H. (2011) *'CryptDB: Protecting confidentiality with encrypted query processing*', in Proceedings of the 23rd ACM Symposium on Operating Systems Principles (SOSP'11). New York: ACM, pp. 85–100.

Pritchett, D. (2008) '*BASE: An acid alternative'*, ACM Queue, 6(3), pp. 48–55.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, pp. 1–88.

Sadalage, P. J. & Fowler, M. (2012) *NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence.* Upper Saddle River, NJ: Addison-Wesley.

Sallam, A., Bertino, E., Hussain, S. R., Landers, D., Lefebure, R. M. & Railkar, R. (2015) *'DBSAFE – An anomaly detection system to protect databases from exfiltration attempts'*, IEEE Systems Journal, 9(4), pp. 1168–1180.

Sinha, S. & Mall, R. (2019) '*An efficient approach for preventing injection attacks in web applications'*, International Journal of Information Security, 18(6), pp. 777–791.

Tudorica, B. G. & Bucur, C. (2011) '*A comparison between several NoSQL databases with comments and notes'*, in Proceedings of the RoEduNet International Conference 10th Edition: Networking in Education and Research. Washington: IEEE, pp. 1–5.

Wang, L., Liu, A. & Bhatt, D. (2010) '*Specification-based intrusion detection for database systems'*, in Jonker, W. & Petković, M. (eds.) *Secure Data Management*. Lecture Notes in Computer Science, vol. 6358. Berlin: Springer, pp. 116–133.

Whitman, M. E. & Mattord, H. J. (2021) *Principles of Information Security*. 7th edn. Boston: Cengage Learning.

FROM THREAT INTELLIGENCE TO ECONOMIC METRICS: LLM-SUPPORTED CYBER RISKOPS FOR CONTINUOUS SV/ROSI ASSESSMENT

CZU: 004.056:005.342
DOI: https://doi.org/10.53486/tids2026.27

GHENADIE BELINSCHI
Academy of Economic Studies of Moldova (ASEM), Doctoral School, Doctoral Programme 521.03 "Economics and Management (Business and Professional Practice)", Republic of Moldova
e-mail: ghenadie.belinschi@ase.md
ORCID ID: 0009-0009-3361-9890;

IRINA DOROGAIA
Academy of Economic Studies of Moldova (ASEM), Department of Management and Entrepreneurship, Republic of Moldova
e-mail: dorogaia.irina.ion@ase.md
ORCID ID: 0000-0003-4625-8616

Abstract. This paper examines the gap between rapidly evolving cyber threats and the relatively static economic justification of cybersecurity innovations in organizations. Building on a risk-based view of information management and on the concept of Cyber RiskOps as a continuous risk-management cycle, we propose an LLM-supported pipeline that translates Threat Intelligence (TI) into auditable updates of scenario parameters used in economic metrics. The pipeline combines an information system passport—a structured register of information assets, business processes, dependencies, and controls—a scenario library, and external/internal signals. The large language model (LLM) is used strictly as an extraction and normalization component, not as an autonomous decision-making mechanism. It transforms unstructured TI into structured attributes, including actor, TTPs, affected technologies, exploitation maturity, and business-impact drivers, and maps them to scenarios through transparent scoring rules and human verification. The updated probabilities and loss magnitudes serve as inputs for the Saved Value of Information (SV) metric, defined as the avoided losses related to confidentiality, integrity, and availability, and for its linkage with Return on Security Investment (ROSI) when comparing security controls under an as-a-service subscription model. An illustrative SME case shows how faster parameter updates can change investment decisions: a package of controls that appears unprofitable under outdated assumptions may become ROSI-positive once TI-driven probability shifts are incorporated in a timely manner. The paper discusses governance requirements, including prompt and data control, audit trails, and segregation of duties, as well as limitations of the approach, such as uncertainty in loss estimation and LLM-specific risks, including hallucinations and prompt injection. The proposed approach supports doctoral research on improving information management through cybersecurity innovations by operationalizing continuous, evidence-based measurement of the economic value of security.

Keywords: LLM; threat intelligence; cyber risk quantification; ROSI; cybersecurity innovations; information management.

JEL Classification: M15; D81; O33

INTRODUCTION

Digital transformation makes information a key factor of production and a critical intangible asset for organizations. This is consistent with the information management perspective, which treats information as a managed resource (Rowley and Farrow, 2000). However, the economic effect of cybersecurity is largely indirect: rather than generating new revenue, security measures primarily

prevent or reduce losses caused by incidents, regulatory sanctions, downtime, and reputational damage. This complicates the investment case and requires decision-makers to rely on risk-based loss-prevention metrics, such as Return on Security Investment (ROSI) (Sonnenreich, Albanese and Stout, 2005), as well as other economic models of security investment (Gordon and Loeb, 2002; Beissel, 2016).

At the same time, the threat landscape is highly dynamic. Current threat reports document the growth of identity-based attacks, business email compromise (BEC), and malware-free intrusions, while generative AI reduces the cost of social engineering and increases the personalization and scalability of attacks (CrowdStrike, 2025; Check Point Research, 2025). In this context, static or infrequently updated risk registers produce outdated estimates of probabilities and loss magnitudes. As a result, SV/ROSI calculations may diverge from actual exposure, leading either to underinvestment in relevant controls or to overinvestment in measures that address an outdated threat profile.

In the doctoral research devoted to improving information management through cybersecurity innovations, we propose a measurable link between: (i) the "information system passport" as a structured representation of information assets, processes, and dependencies; (ii) scenario-based risk assessment; and (iii) the Saved Value of Information (SV) metric, understood as the value of information preserved through the avoidance of losses related to confidentiality, integrity, and availability. This triadic approach supports a managerial perspective in which information management and cybersecurity are integrated and assessed through measurable effects, rather than merely through compliance checklists.

This paper further develops the proposed approach by introducing a continuous updating mechanism inspired by Cyber RiskOps, which treats cyber-risk management as an operational cycle linking strategy, threat intelligence, execution of controls, and measurable outcomes (Castro, 2025; Leirvik, 2023). We argue that large language models (LLMs) can reduce analytical latency within this cycle, but only if their use is limited to auditable data-extraction tasks and they are embedded in the broader management process.

The study is guided by two research questions: RQ1: How can threat intelligence be translated into updates of scenario parameters for SV/ROSI calculations in an auditable and reproducible manner? RQ2: Under what conditions can faster parameter updates change the economic decision regarding cybersecurity innovations for organizations operating under subscription-based models?

The contribution of this paper is threefold. First, we propose an LLM-supported Cyber RiskOps pipeline that links unstructured Threat Intelligence (TI) with a scenario library and an information system passport. Second, we formalize the relationship between TI-driven updates and SV/ROSI calculation under uncertainty and governance constraints. Third, we illustrate the approach through a demonstration SME case study and discuss the limitations and control measures required for the responsible use of LLMs in risk analytics.

MAIN CONTENT

1. LITERATURE REVIEW

The evaluation of cybersecurity investments has a long history of combining technical risk analysis with economic decision-making. Classical approaches operationalize risk as the product of probability and impact and use derived metrics such as Single Loss Expectancy (SLE) and Annualized Loss Expectancy (ALE). In the corporate context, these metrics are often linked to ROI-type analysis through ROSI, which expresses net savings, understood as avoided losses, relative to the cost of a

security control (Sonnenreich, Albanese and Stout, 2005). The Gordon–Loeb model further emphasizes that optimal security expenditure is typically only a fraction of expected losses and depends on the vulnerability level of the information set being protected (Gordon and Loeb, 2002).

Despite their usefulness, economic metrics face practical limitations: loss magnitudes are uncertain, some impacts are intangible, and probability estimates are sensitive to both internal conditions and external threat dynamics (Beissel, 2016). As a result, many organizations still communicate cyber risks through qualitative heat maps. Modern approaches to cyber risk quantification (CRQ), such as FAIR (Factor Analysis of Information Risk), seek to improve consistency by decomposing risk into factors such as threat event frequency, vulnerability, and loss magnitude, while encouraging calibration, interval estimates, and Monte Carlo simulation (FAIR Institute, 2025). Frameworks and standards such as the NIST Cybersecurity Framework 2.0 and ISO/IEC 27001/27005 provide a process-oriented structure for identifying and managing cybersecurity risks and for linking security controls to desired outcomes (NIST, 2024; ISO/IEC, 2022a; ISO/IEC, 2022b).

From an operational perspective, the challenge lies not only in how metrics are calculated, but also in how their relevance is maintained over time. The concept of Cyber RiskOps proposes an operating model in which cyber risks are managed continuously across functional boundaries: strategy defines risk appetite and objectives, operations implement controls, and measurement continuously informs prioritization (Castro, 2025). Similar ideas are also found in the practical literature on cyber-risk management, which emphasizes continuous monitoring and integration with business processes (Leirvik, 2023).

Threat intelligence is one of the key external inputs that should update risk assumptions. However, in security operations centers (SOCs), TI is often consumed primarily as indicators and tactics, rather than translated into economic parameters. A significant gap lies in the absence of a standardized and auditable process for transforming unstructured TI narratives into the structured attributes required to update scenario probabilities and loss magnitudes.

Large language models (LLMs) offer the potential to reduce the manual workload associated with processing TI. They are effective in summarization, entity and relationship extraction, and mapping text to predefined taxonomies. At the same time, their use introduces new risks, including hallucinations, prompt injection, and uncontrolled leakage of sensitive data if models are deployed without appropriate governance. Professional communities increasingly emphasize that AI can both amplify threats and support defensive capabilities, which makes responsible implementation and control mechanisms essential (Check Point Research, 2025; NIST, 2025).

Thus, the research gap addressed by this paper lies in designing a governance-aware pipeline that uses LLMs as constrained extraction tools to integrate TI into continuous cyber-risk quantification and to support SV/ROSI-based decision-making in information management.

2. METHODOLOGY

The proposed approach is positioned as a measurement layer within the Cyber RiskOps cycle. Its purpose is to update scenario parameters—namely, probability and loss magnitude—on the basis of new threat-intelligence signals and to recalculate SV/ROSI for alternative cybersecurity innovations. The pipeline assumes that the organization already maintains a minimum set of governance artifacts typical of information-management and security programs: an inventory of information assets and systems, a control catalog, and a risk register. We structure these artifacts into three key components.

(1) Information System Passport (ISP). The ISP is a structured description of the organization's information-system landscape: critical business processes, information assets (datasets), supporting applications and infrastructure, owners, third parties, and dependencies on controls. Unlike a general IT inventory, the ISP is specifically designed to link risk to value: each asset is tagged with confidentiality, integrity, and availability (CIA) requirements and with business-impact drivers, such as acceptable downtime, regulatory exposure, and revenue dependency.

(2) Scenario Library. The organization defines a set of recurring cyber-risk scenarios relevant to its context. Each scenario k includes a brief description, a mapping to the affected ISP elements, a baseline probability p_k, a baseline loss magnitude L_k, and key control levers that can reduce p_k and/or L_k. Scenarios may be aligned with common threat categories, such as disruption caused by ransomware, business email compromise, identity takeover, cloud misconfiguration, or third-party compromise.

(3) Signal Streams. The pipeline uses both external and internal signals. External signals include TI reports, notifications, vendor bulletins, and industry alerts. Internal signals include incidents, near misses, audit results, and control-effectiveness metrics, such as MFA coverage, phishing click-through rate, and patch deployment delays.

For each scenario k, the expected losses at time t is defined as:

$$EL_k(t) = p_k(t) \times L_k(t) \quad (1)$$

where p_k(t) denotes the probability that scenario k materializes over the selected period, typically one year, and L_k(t) denotes the corresponding loss magnitude expressed in monetary terms. This definition is consistent with standard cyber-risk quantification practice and allows the SV metric to be interpreted as avoided expected losses.

LLM-supported extraction. In this context, the LLM is introduced as a text-to-structure component. The model is not allowed to directly assign risk values. Instead, it produces a structured extraction record for each TI item, including fields such as: (i) affected technologies and vendors; (ii) attack vectors and tactics/techniques, with mapping to MITRE ATT&CK where appropriate; (iii) sectoral relevance; (iv) exploitation maturity, such as theoretical, proof-of-concept, or observed exploitation; (v) potential business impacts and preconditions; and (vi) recommended mitigation measures. Each extraction record includes evidence pointers, such as text fragments and links, to ensure auditability.

Figure 1 summarizes the proposed pipeline and its main data flows.



Figure 1. LLM-supported Cyber RiskOps pipeline for the continuous updating of SV/ROSI.
Source: *author's own conceptualization.*

Matching and scoring. A deterministic matching function links each extraction record to one or more scenarios in the library according to explicit rules. For example, if TI indicates increased exploitation of cloud identity services and realistic voice impersonation, the matching function raises the signal score for scenarios related to identity compromise and BEC. The resulting score is then translated into scenario-parameter updates through bounded adjustments, for example:

$$p_k(t+1) = \text{clip}(p_k(t) \cdot (1 + \alpha \cdot S_k), p_{min}, p_{max}) \quad (2)$$

$$L_k(t+1) = \text{clip}(L_k(t) \cdot (1 + \beta \cdot I_k), L_{min}, L_{max}) \quad (3)$$

where S_k denotes the normalized signal score for probability, and I_k denotes the signal score for loss drivers. The parameters α and β are calibration coefficients selected by the organization. The clip() operator imposes predefined bounds and prevents overreaction to a single source. Importantly, final parameter updates must be approved by a human reviewer, such as the risk owner or an analyst, before they take effect in the risk register.

Economic calculation. The Saved Value of Information (SV) for a portfolio of controls c over a given period is calculated as the avoided expected losses across scenarios, comparing the baseline state (without the additional controls) with the post-implementation state (after the controls have been implemented):

$$SV_c = \Sigma_k [EL_k^{base} - EL_k^c] \quad (4)$$

where EL_k^base is calculated using the baseline parameters, and EL_k^c is calculated using the parameters after applying the portfolio of controls c. If the controls affect CIA dimensions differently, L_k can be decomposed into confidentiality, integrity, and availability components and then aggregated in a way that reflects the organization's priorities.

ROSI is used to normalize SV by the value of the control portfolio C_c:

$$ROSI_c = (SV_c - C_c) / C_c \quad (5)$$

This formulation is consistent with the ROSI literature and supports comparison across alternative control portfolios (Sonnenreich, Albanese and Stout, 2005). In subscription-based environments, C_c typically represents annual recurring costs, such as licences and managed services, whileSV_c is interpreted as annual avoided losses.

Accounting for uncertainty. Because both p_k and L_k are uncertain, the pipeline supports interval values rather than point estimates. An extraction record may include a qualitative confidence level, such as high, medium, or low, which is then converted into narrower or wider intervals. Organizations can perform sensitivity analysis by recalculating SV/ROSI across plausible parameter ranges or, when sufficient data are available, apply FAIR-style Monte Carlo simulation (FAIR Institute, 2025).

Governance and auditability. The use of LLMs in risk analytics requires controls similar to those applied to other high-impact decision-support systems. We propose the following minimum safeguards: (i) retrieval-only prompts that require the model to cite evidence fragments; (ii) separation of duties between TI ingestion, parameter approval, and the final investment decision; (iii) logging of prompts, model outputs, and reviewer decisions; (iv) data minimization, including a prohibition on sending sensitive internal logs to external models, and the use of secure environments; and (v) periodic validation against actual incidents and control-performance metrics in order to recalibrate α and β. The result is an auditable chain: TI source → structured extraction → scoring rule → parameter update → SV/ROSI calculation → management decision.

3. CASE STUDY

To demonstrate the impact of continuous parameter updates on the investment decision, we use a simplified SME case study. The organization is a professional services firm with approximately 25

employees, operating in a hybrid work model and relying on Microsoft 365, a cloud-based CRM, and online banking for daily operations. Following the dissertation approach, the firm maintains an Information System Passport (ISP) that identifies critical processes, including service delivery to clients, invoicing, and cash-flow management, as well as information assets, including client data, financial documents, and user credentials, together with their CIA requirements.

The scenario library includes three annual scenarios: (S1) ransomware-induced disruption of workstations and the file-sharing environment; (S2) business email compromise (BEC) and voice phishing (vishing) leading to fraudulent payments; and (S3) data leakage caused by SaaS misconfiguration or credential compromise. The baseline estimates for the next 12 months, prepared in Q1, are presented in Table 1 as the "outdated baseline (Q1)".

The cybersecurity innovation under consideration is an identity and email protection package that includes mandatory MFA with conditional access, enhanced payment-approval procedures, user training focused on AI-enabled social engineering, and a managed email-security service. The estimated annual recurring cost of the package is C = 1{,}600 EUR under a subscription model.

The expected control effect is modeled through scenario-specific reduction factors applied to the baseline probability and/or loss magnitude: the probability of ransomware disruption is reduced from 0.07 to 0.06; the probability of BEC is reduced by 50%, while the corresponding loss magnitude is reduced by 25%; and the probability of data leakage is reduced from 0.10 to 0.08, while the loss magnitude decreases from 15,000 EUR to 13,000 EUR.

With the outdated baseline, the total expected loss is EL_base = 4,690 EUR per year, while the expected loss after implementing the control package is EL_control = 3,080 EUR per year. This yields SV = 1,610 EUR per year and ROSI ≈ 0.6%. Under this assessment, the investment appears marginal and may be assigned a lower priority.

Next, the LLM-supported pipeline ingests new TI items describing an increase in AI-enabled impersonation and BEC campaigns targeting SMEs that use widely adopted cloud-based email platforms. After extraction, matching with scenario S2, and human review, the probability of BEC for the forthcoming period is updated from 0.12 to 0.22, forming the "TI-updated baseline." The remaining scenarios in this simplified example remain unchanged.

With this update, the total baseline expected loss increases to 5,890 EUR per year, while the expected loss after implementing the control package becomes 3,530 EUR per year, since the same relative control effect is applied to the updated probability. As a result, SV amounts to 2,360 EUR per year, and ROSI ≈ 47.5%. Therefore, continuous TI-based updating changes the investment decision: the same cybersecurity innovation becomes economically justified once the shift in the threat landscape is reflected in a timely manner.

Although the figures are illustrative, the case demonstrates the core mechanism: faster, evidence-based updates can change SV/ROSI results, re-prioritize control portfolios, and reduce the risk of resource misallocation caused by outdated assumptions. In practice, the approach can be extended by using interval estimates and by validating updates against internal incidents and control-effectiveness metrics.

Table 1. Scenario-Based Expected Losses under Outdated and TI-Updated Parameters: Demonstration Case.

Scenario	EL_base (outdated Q1), EUR	EL_control (outdated), EUR	EL_base (TI-outdated), EUR	EL_control (TI-outdated), EUR
S1: Ransomware-induced disruption	1,750	1,500	1,750	1,500
S2: BEC/vishing fraud	1,440	540	2,640	990
S3: SaaS data leakage	1,500	1,040	1,500	1,040
Total	**4,690**	**3,080**	**5,890**	**3,530**

Source: *authors' calculations.*

4. DISCUSSION AND LIMITATIONS

The proposed approach represents a pragmatic compromise between fully manual cyber-risk quantification and fully automated, opaque AI-based scoring. Its value lies not in replacing expert judgment, but in operationalizing the evidence flow from TI to economic metrics, which is often a bottleneck in organizations with limited analytical capacity. This is especially relevant in subscription-based environments, where cybersecurity innovations are purchased as a service and must be continuously validated against a changing exposure landscape.

However, several limitations must be acknowledged. First, loss assessment remains uncertain and context-dependent. Even with an information system passport, translating CIA requirements into monetary losses requires assumptions about downtime costs, recovery capabilities, contractual penalties, and reputational effects. Therefore, SV/ROSI results should be viewed as decision support under uncertainty rather than as precise forecasts.

Second, parameter updates may introduce volatility. Overreacting to a single report or a noisy signal can lead to fluctuations in prioritization. For this reason, the method relies on bounded updates via the clip function, calibration coefficients, and multi-source corroboration before substantial parameter changes are made. Organizations may also limit the update frequency, for example to a weekly cycle, in order to balance responsiveness and stability.

Third, LLM-specific risks require dedicated controls. Hallucinations may produce false mappings or “invent” facts if prompts are not sufficiently constrained. Prompt injection may occur when unverified TI content is passed to the model. Data-leakage risks arise when internal incident data or sensitive inventories are processed by external model providers. For these reasons, the use of LLMs should be limited to extraction from approved sources, supported by retrieval-based mechanisms and evidence citation, and embedded in an approval workflow with logging and segregation of duties. Emerging guidance on cybersecurity risk management for AI systems (NIST, 2025) may provide an additional governance reference point.

Finally, this paper demonstrates the approach using a simplified example. Full empirical validation would require longitudinal organizational data, comparison of decision outcomes with and without continuous updating, and assessment of analyst workload and error rates. These directions are planned as further work within the dissertation research programme.

CONCLUSIONS

This paper proposes an LLM-supported Cyber RiskOps pipeline for the continuous measurement of the economic effect of cybersecurity innovations. The central idea is to close the gap between dynamic threat intelligence (TI) and the relatively static risk parameters used in SV/ROSI calculations. The pipeline integrates three governance artifacts—the information system passport, the scenario library, and signal streams—while the LLM is used only for auditable extraction and normalization tasks.

By defining explicit matching and scoring rules and requiring human approval of parameter updates, the approach preserves transparency and supports an evidence-based audit trail from TI sources to updated scenario probabilities and loss magnitudes. The demonstration SME case study shows that timely TI-based updating can change the perceived economic attractiveness of a control portfolio: a package that appears marginal under outdated assumptions becomes ROSI-positive once the shift in the threat landscape is captured.

The proposed method supports the broader dissertation research programme on improving information management through cybersecurity innovations by providing a practical mechanism for the continuous measurement of value. Future work will focus on developing a dashboard prototype, integrating internal telemetry for improved calibration, and evaluating the approach on longitudinal datasets in order to quantify reductions in analytical latency and improvements in decision quality.

REFERENCES

Beissel, S. (2016) Cybersecurity Investments: Decision Support Under Economic Aspects of Safeguards and Breaches. Cham: Springer International Publishing. doi:10.1007/978-3-319-30460-1.

Castro, J.P. (2025) Cyber RiskOps: Bridging Strategy and Operations in Cybersecurity. ResearchGate. doi:10.13140/RG.2.2.36216.97282/1. Available at: https://www.researchgate.net/publication/388194428 [Accessed April 17, 2026].

Check Point Research (2025) AI Security Report 2025. Check Point Software Technologies. Available at: https://www.checkpoint.com/resources/items/report-ai-security-report-2025/ [Accessed April 17, 2026]

CrowdStrike (2025) European Threat Landscape Report 2025. CrowdStrike. Available at: https://www.crowdstrike.com/wp-content/uploads/2025/11/CrowdStrike-European-Threat-Landscape-Report-2025.pdf [Accessed 17 April 2026].

FAIR Institute (2025) Factor Analysis of Information Risk (FAIR) Standard v3.0 (January 2025). FAIR Institute. Available at: https://www.fairinstitute.org/hubfs/Standards%20Artifacts/Factor%20Analysis%20of%20Information%20Risk%20%28FAIR%29%20Standard%20v3.0%20%28January%202025%29.pdf [Accessed April 17, 2026].

Gordon, LA and Loeb, MP (2002) 'The economics of information security investment'. ACM Transactions on Information and System Security, 5(4), pp. 438–457. doi:10.1145/581271.581274.

ISO/IEC (2022a) ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: International Organization for Standardization.

ISO/IEC (2022b) ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva: International Organization for Standardization.

Leirvik, R. (2023) Understand, Manage, and Measure Cyber Risk: Practical Solutions for Creating a Sustainable Cyber Program. 2nd edn. Berkeley, CA: Apress.

NIST (2024) The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.CSWP.29 [Accessed April 17, 2026].

NIST (2025) Cybersecurity Framework Profile for Artificial Intelligence (AI) Profile: Preliminary Draft. NIST IR 8596 iprd. National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8596.iprd.pdf [Accessed April 17, 2026].

Rowley, J. and Farrow, J. (2000) Organizing Knowledge: An Introduction to Managing Access to Information. 3rd edn. Aldershot: Gower.

Sonnenreich, W., Albanese, J. and Stout, B. (2005) 'Return on security investment (ROSI): A practical quantitative model'. In: Proceedings of the 3rd International Workshop on Security in Information Systems (WOSIS 2005). pp. 239–252. doi:10.5220/0002580202390252.

ANALYSIS OF THE MAIN THREATS IN THE SPHERE OF CYBERSECURITY

CZU: 004.056:005.342
DOI: https://doi.org/10.53486/tids2026.28

OLGA PUGACHEVA
Francysk Skaryna Gomel State University
e-mail: OPugacheva@gsu.by
ORCID ID: 0000-0003-4554-0038

Abstract. This article analyzes the main threats in cybersecurity. To this end, it examines the key reasons for the relevance of this study for organizations and individuals seeking to ensure their security in the digital world. This study of the main threats in cybersecurity includes an analysis of quantitative data such as the increasing number of cyberattacks, the diversity of cyberattack methods and threat channels, the main areas of cyberattacks, the consequences of cyberattacks, and the types of stolen data, as well as technological changes associated with the use of artificial intelligence (AI).

As AI is becoming an important resource in the arsenal of cybercriminals, this article analyzes the main risks of using AI, the ways in which AI is used in the development and evolution of malware, and important aspects of using AI in social engineering. This allows us to draw conclusions about the need for organizations to develop strategies to minimize risks and ensure the safe use of AI technologies in information security, and for their specialists to constantly update their defense methods and respond to new threats.

The results demonstrate the novelty of the analysis, which encompasses a comprehensive analysis of current and future threats, taking into account the role of AI, including its use for malicious purposes and social engineering; identifying the dual role of AI – both as a defense tool and a means of complicating attacks; and examining current technological development trends and their impact on cybersecurity.

The practical significance of the study lies in its ability to help organizations and professionals understand and prepare for current threats; substantiate the need to develop AI-informed defense strategies; and help professionals develop skills for continually updating defense methods in a dynamically changing environment.

Keywords: analysis, cybersecurity, cyberattacks, threats, artificial intelligence

JEL Classification: A12, C8, O33, C45, Y10

INTRODUCTION

Analyzing the main cybersecurity threats is a crucial part of an information security strategy and an asset for any organization seeking to ensure its security in the digital world.

It is essential for the following key reasons (Pugacheva Olga, 2025):

– increased cyberattacks. Each year, we see an increase in the number and complexity of cyberattacks. Hackers are using increasingly sophisticated methods, making continuous threat monitoring and analysis essential;

– diversity of threats. Threats can range from simple viruses and malware to complex attacks such as phishing, DDoS attacks, supply chain attacks, and more. Understanding these threats allows organizations to better prepare and protect themselves;

– economic impact. Cyberattacks can have serious financial consequences for organizations, including data loss, reputational damage, and fines. Threat analysis helps minimize risks and losses;

– regulatory compliance. Many industries are subject to strict cybersecurity regulations. Threat analysis helps organizations meet these requirements and avoid legal consequences;

- technological change. The rapid advancement of technologies such as cloud computing, IoT (Internet of Things), and artificial intelligence (AI) is creating new vulnerabilities. Threat analysis enables the timely identification and remediation of these vulnerabilities;

- increased awareness. Threat analysis helps increase employee and management awareness of cybersecurity risks, leading to a more responsible security culture within the organization;

- forecasting and preventative measures. Understanding current and potential threats allows organizations not only to respond to incidents but also to take proactive measures to prevent them.

The purpose of this study is to analyze the main cybersecurity threats facing organizations so that they can build a robust defense system, which is impossible without up-to-date knowledge of current cyberattack trends.

RESEARCH OF THE MAJOR CYBERSECURITY THREATS

1. Analysis of the Number of Cyberattacks

Every year, experts note that the number of successful cyberattacks is rapidly growing, and their complexity and aggressiveness continue to increase. This trend is illustrated by the data presented in Figure 1.

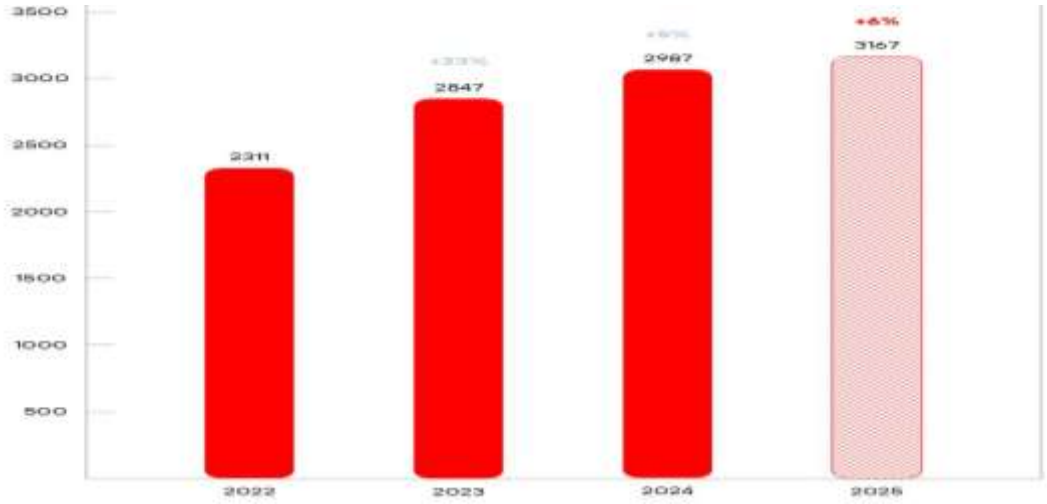


Figure 1. Number of successful attacks on organizations worldwide in 2022-2025.
Source: *Attack trends in 2026.*

The data shows that the total number of successful attacks on organizations globally was 6% higher in 2025 than in 2024, 11% higher in 2024 than in 2023, and 37% higher in 2023 than in 2022. Experts also note that because most cyberattacks are not made public due to reputational risks, it is impossible to calculate the exact number of threats.

2. Diversity of Cyberattack Methods and Threat Channels

As Figure 2 shows, the primary methods of cyberattacks on organizations worldwide in 2025 were malware (71%) and social engineering (51%). The share of successful malware-based attacks on organizations increased by 5 percentage points compared to last year, while the number of social engineering attacks remained unchanged.

The number of attacks using legitimate software doubled compared to 2024 and quadrupled compared to 2023, reaching 8% of total incidents.

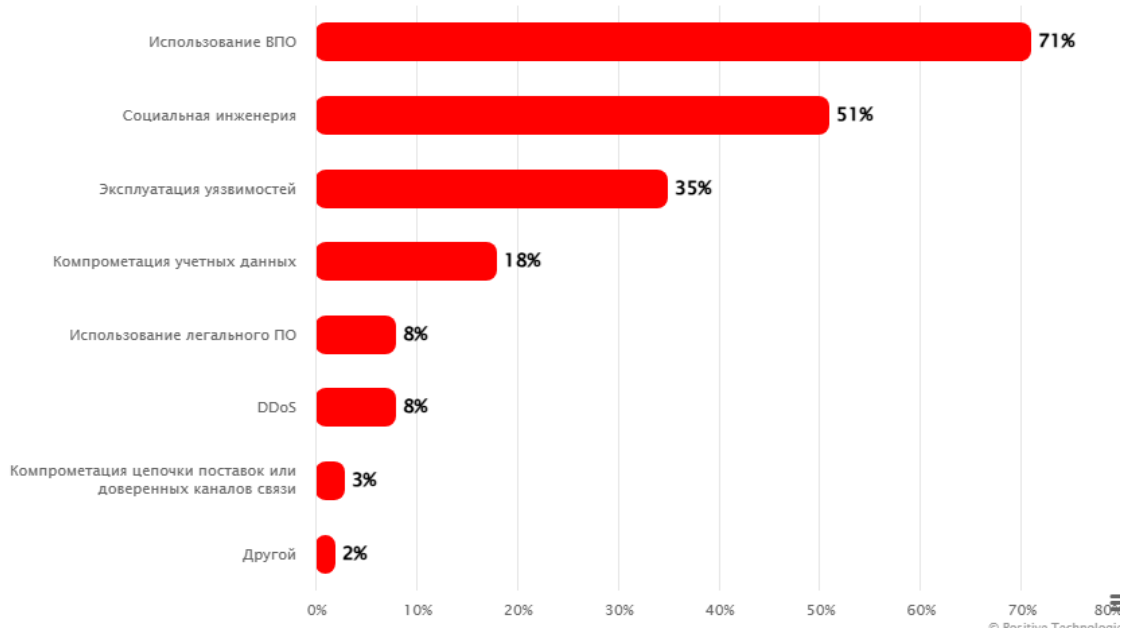


Figure 2. Attack methods on organizations (percentage of successful attacks) in 2025.
Source: *Attack trends in 2026.*

The social engineering channels used in attacks on organizations worldwide in 2025 are shown in Figure 3. The primary social engineering channel is email (86%). This is because attackers most often use phishing emails to infect victims with malware and further develop the attack. These are followed by organizational websites (23%), social media and instant messaging (6%), phone calls (3%), and other channels (2%).

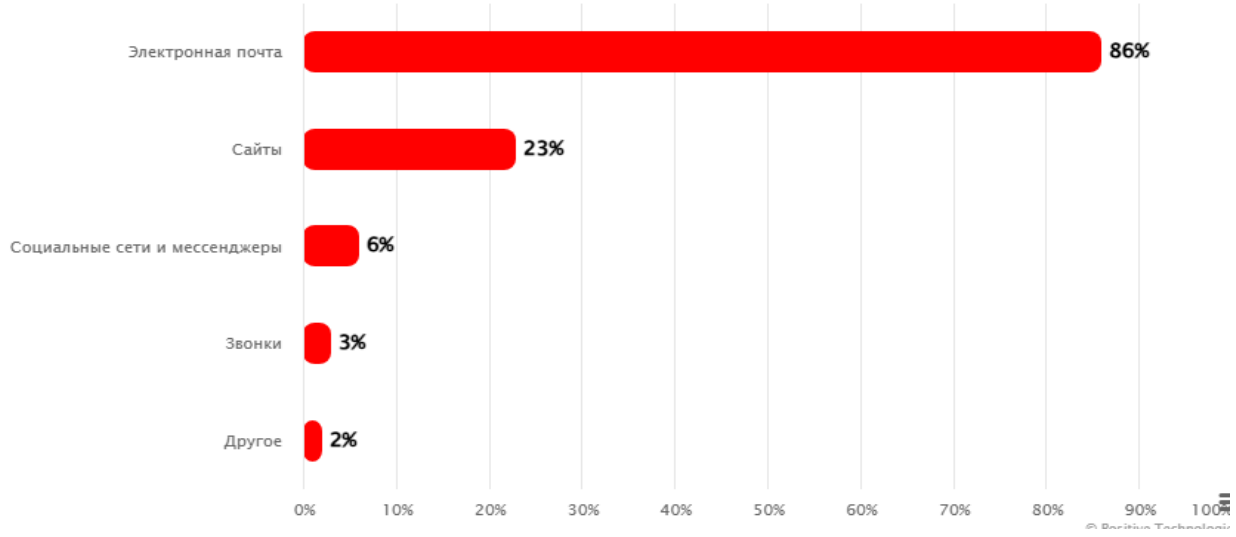


Figure 3. Social engineering channels in attacks on organizations around the world in 2025
Source: *Attack trends in 2026.*

3. Main Areas of Cyberattack

Victims of cyberattacks include a wide range of organizations, from small businesses to large corporations. Figure 4 shows the most vulnerable industries worldwide in 2025.

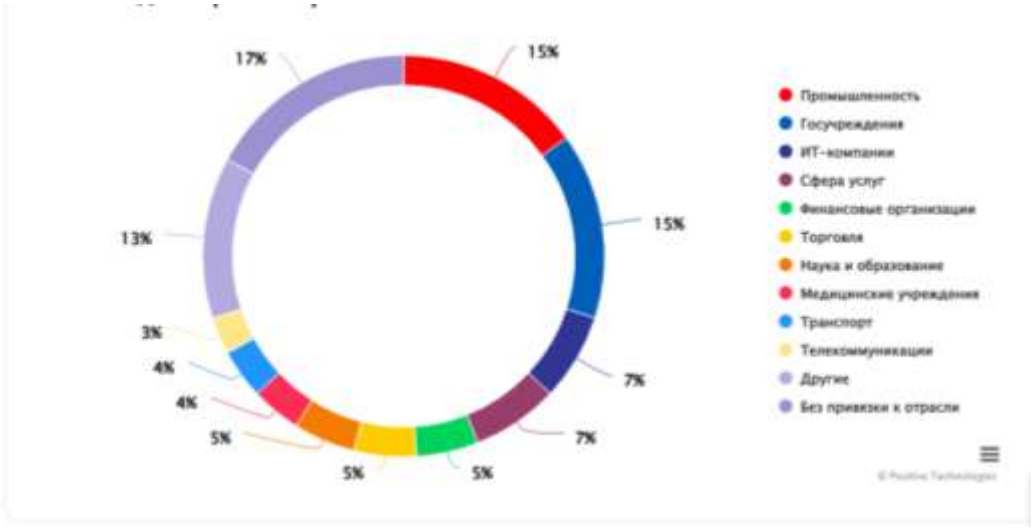


Figure 4. The areas of activity of organizations around the world subject to cyberattacks in 2025

Source: *Attack trends in 2026.*

The data shows that government agencies (15%), industrial enterprises (15%), and IT companies (7%) were the most frequently targeted sectors. New to the global attack landscape in 2025 is the service sector – hotels, cafes and restaurants, travel agencies, etc. – which has supplanted healthcare organizations, which have been a priority target for attackers in recent years. In 2025, it accounted for 7%. In 2024, healthcare was among the top five most attacked sectors (6%), and in 2023, it ranked second in terms of the number of cyberattacks.

4. Consequences of Cyberattacks and the main types of stolen data

Figure 5 shows the main consequences of cyberattacks in 2025. They show that nearly two-thirds (64%) of successful attacks on organizations resulted in confidential information leaks, while disruptions to the organization's core business accounted for 47%.

Comparing these figures to 2024, there is an increase in attacks associated with data leaks from 53% to 64%, and an increase in the proportion of successful attacks that resulted in business disruption from 31% to 47%.

Compared to 2024, the proportion of successful attacks that resulted in business disruption increased from 31% to 47%, and the percentage of attacks associated with data leaks increased from 53% to 64%.

Other consequences (use of organizational resources, damage to state interests, direct financial losses to the organization, etc.) together accounted for 27%.

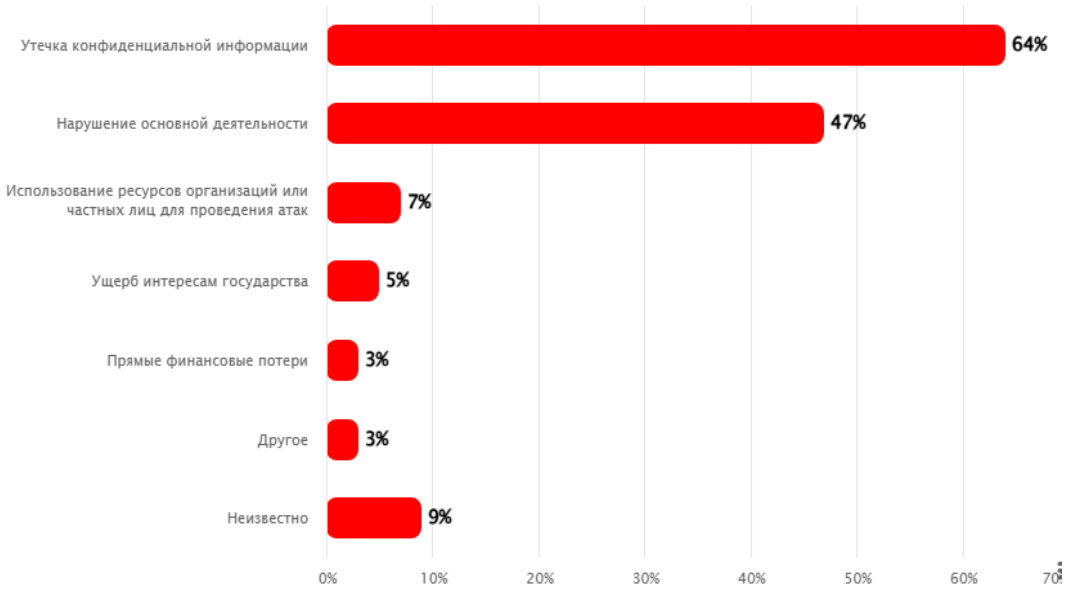


Figure 5. Main consequences of cyberattacks (percentage of successful attacks) in 2025.
Source: *Attack trends in 2026.*

The main types of stolen data in successful attacks on organizations are shown in Figure 6.

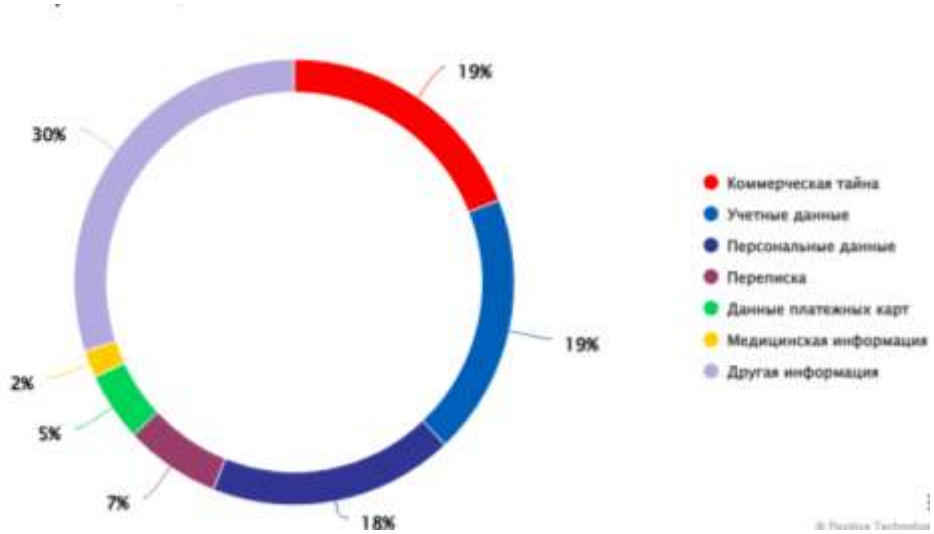


Figure 6 Types of stolen data in successful attacks on organizations
Source: *Attack trends in 2026.*

The most frequently stolen items from organizations were trade secrets (19%), credentials (19%), and personal data (18%).

Since 2024, there has been an increase in the theft of credentials from organizations and a decline in interest in personal information. This trend continued in 2025: credentials were stolen in 19% of attacks (an increase of 8 percentage points compared to 2023 and a decrease of 6 percentage points compared to 2022), while personal data was stolen in 18% (a decrease of 27 percentage points compared to 2023 and an increase of 18 percentage points compared to 2022). The share of trade secret leaks remains virtually unchanged year-over-year at 19%. Experts attribute the increased interest in credential theft to the fact that such data can be used by cybercriminals to carry out further attacks and/or sell on the shadow market.

5. Technological Changes Associated with the Use of AI Tools

Artificial intelligence is not only a tool for business and science, but also a new resource in the cybercriminal arsenal. The main risks of using AI, the ways in which AI is used in the development and evolution of malware, and important aspects of using AI in social engineering are presented in Table 1.

Table 1. Threats associated with the use of AI technologies

Threats associated with the use of AI technologies		
Risks of using AI and their characteristics	**Directions for the use of AI in the development and evolution of malware**	**Key aspects of using AI in social engineering**
1. Attack automation. AI can be used to automate cyberattacks such as phishing, password cracking, or distributed denial-of-service (DDoS) attacks. Algorithms can analyze vulnerabilities and find ways to exploit them faster and more efficiently than humans could.	1. Adaptive attacks. AI can be used to create malware that can adapt to different conditions and systems. For example, such programs can analyze the defense mechanisms on the target system and modify their attack methods to bypass these defenses.	1. Personalization of attacks. AI allows attackers to collect and analyze data about their victims, such as their interests, behavior, and social connections. This allows them to create personalized messages that are more convincing and believable, increasing the likelihood of an attack's success.
2. Advanced data analysis. AI can process and analyze large volumes of data, which can be used by attackers to identify vulnerabilities in security systems or to create targeted attacks based on collected user information.	2. Phishing automation. AI can be used to automate phishing attacks. Algorithms can analyze social media and other information sources to create convincing fake messages that are targeted to specific users based on their interests and behavior.	2. Phishing automation. AI can automate the creation of phishing emails and messages. Algorithms can generate multiple message variations tailored to specific audiences, making them more effective.
3. Creating fake content. Technologies such as generative neural networks can be used to create fake images, videos, or text, which can lead to disinformation and manipulation.	3. Malicious code generation. Using generative neural network technologies, it is possible to create new malicious code that is unique and less detectable by antivirus programs. This can significantly increase the effectiveness of malware.	3. Behavior analysis. AI can be used to analyze user behavior online, identifying patterns and anomalies. This helps attackers understand when and how best to attack, as well as predict how victims will react to certain actions.
4. Bypassing security systems. AI can be used to develop methods to bypass intrusion detection systems and other defense mechanisms, rendering them less effective.	4. Bypassing security systems. AI can analyze the behavior of security systems and find ways to evade their detection. For example, algorithms can study antivirus software patterns and adapt their actions to avoid detection.	4. Content generation. AI-based text generation technologies, such as GPT, can create plausible and well-formed messages. This allows attackers to generate fake messages from trusted sources, such as colleagues or well-known companies.
5. Vulnerabilities in AI systems themselves.	5. Targeted research.	5. Social media analysis.

Threats associated with the use of AI technologies		
Risks of using AI and their characteristics	**Directions for the use of AI in the development and evolution of malware**	**Key aspects of using AI in social engineering**
AI algorithms may contain vulnerabilities that can be exploited by attackers to manipulate results or gain access to sensitive information.	AI can be used to gather information about targets by analyzing data from open sources such as social media, websites, and databases. This allows attackers to better understand their victims and plan more effective attacks.	AI can analyze social media data to identify connections between people and their interests. Attackers can use this information to create more targeted attacks based on what interests the victim.
6. Ethical and legal issues. The use of AI in security may raise questions about privacy, human rights, and the legitimacy of such technologies.	6. Improved encryption. AI-based malware can use more sophisticated encryption methods to protect its components from analysis and detection, making it more resistant to attempts to neutralize it.	6. 6. Scenario Modelin. AI can help model various social engineering scenarios, allowing attackers to test different approaches and strategies to determine the most effective manipulation methods.
7. Errors and bias. AI algorithms can be error-prone or biased, which can lead to incorrect conclusions and actions regarding security.	7. Attack Scalability: With AI, attackers can quickly scale their attacks by using automated systems to launch multiple attacks simultaneously on different targets.	7. Vulnerability detection. AI can be used to analyze security systems and identify human vulnerabilities. For example, it can determine which employees are most susceptible to manipulation or how internal security policies can be circumvented.
8. Technology Dependency. Organizations' increasing reliance on AI systems may lead to risks associated with their failure or compromise.	8. Data-driven learning. Malware can learn from data from previous attacks to improve its methods and increase its effectiveness in the future. This allows it to evolve and adapt to new threats and defenses.	8. Big Data Processing. AI is capable of processing massive amounts of data from various sources, allowing attackers to quickly identify vulnerabilities and attack opportunities.

Source: *Pugacheva, O. V., 2024*

An analysis of the table's information allows us to draw the following conclusions:

- given the identified risks, it is important to develop strategies to minimize them and ensure the safe use of AI technologies in information security;

- AI significantly enhances the capabilities of malware, making it more complex, adaptive, and difficult to detect, creating significant challenges for cybersecurity professionals, who must constantly update their defenses and respond to new threats;

- AI significantly enhances the capabilities of social engineering, making attacks more targeted and effective. This creates significant challenges for organizations and individuals, who must be more aware of potential threats and develop critical thinking skills to protect against manipulation.

CONCLUSIONS

Research shows that recent years have seen a significant increase in the number, diversity, and distribution channels of cyberattacks, reinforcing the need for continuous improvement of security systems.

One of the current trends is the use of artificial intelligence by cybercriminals, enabling them to automate and sophisticate attacks, create new types of malware, and employ social engineering techniques. Despite the potential of AI to enhance security, its use for cybercriminal purposes requires special attention and the development of countermeasures.

To counter new types of threats and minimize risks, organizations must develop and implement comprehensive strategies that include constantly updating their defense and response methods, as well as training specialists.

The study's novelty lies in:

- a comprehensive analysis of current and future threats, taking into account the role of AI, including its use for malicious purposes and social engineering;
- identifying the dual role of AI – both as a defense tool and a means of complicating attacks;
- examining current technological development trends and their impact on cybersecurity.

The study's practical significance lies in its ability to help organizations and professionals understand and prepare for current threats; substantiate the need to develop AI-inclusive defense strategies; and help professionals develop skills to continually update their defense methods in a dynamically changing environment.

REFERENCES

Attack trends in 2026, 2026. Available at: https://ptsecurity.com/research/analytics/trendy-atak-v-2026-godu/#id8 [Accessed 10.03.2026].

Pugacheva, Olga, 2025. Innovative technologies in educational activities and ensuring digital security «Technological innovations in digital security», international conference (1; 2025; Chişinău). Proceedings of the First Edition of the International Conference «Technological innovations in digital security», May 15-16, 2025, Chişinău / scientific committee: Stratan Alexandru. – Chişinău: SEP ASEM, 2025. – 256 p. (pp. 168-175).

Pugacheva, O. V., 2024. Use of artificial intelligence in the economy and society: directions, problems and regulation. *Proceedings of the F. Skorina Gomel State University*, No. 5 (146). pp. 136-141.

FROM SECURITY TO EDUCATION: CHOOSING PROGRAMMING LANGUAGES FOR CS1 AND CS2

CZU: [004.056:004.43]:378
DOI: https://doi.org/10.53486/tids2026.29

ZINOVIA TOACĂ
Academy of Economic Studies of Moldova,
e-mail: toaca@ase.md
ORCID ID: 0000-0002-8304-1961

LUCIA GUJUMAN
Academy of Economic Studies of Moldova,
e-mail: gujuman.lucia@ase.md
ORCID ID: 0000-0001-7940-4291

Abstract. One of the main problems in the process of developing and using computer systems is software security. C++ is one of the languages used in the development of high-performance applications and complex software infrastructures. This language provides direct control over memory and system resources, but this can lead to security vulnerabilities. The way to avoid these problems is to follow good practices in the programming process, such as using modern language mechanisms, validating input data, avoiding unnecessary manual memory management, using automatic analysis procedures. Security is not a final stage of the programming process, but a principle from the first line of code. The C++ language is in continuous development and one of the issues addressed is the security of the written code. Today, such mechanisms as RAI (Resource Acquisition Yes Initialization), smart pointers, modern standard libraries and advanced static code analysis tools, which are a significant support in code security, reducing the risk of memory errors and increasing software reliability. In this context, teaching the C++ language in university programs in the field of information technologies remains essential for training specialists capable of understanding the internal functioning of computer systems, resource management and the development of high-performance applications. The study of this language not only contributes to the development of algorithmic thinking, understanding computer architecture but also to the formation of the necessary skills for the development of critical systems. This article analyzes the experience of universities in selecting programming languages for CS1[1] and CS2[2] courses.

Keywords: C++, software security, memory vulnerabilities, buffer overflow, RAII, smart pointers, secure programming, computer science education.

JEL Classification: A23, C88, I23

INTRODUCTION

Society's increasing dependence on networked software systems is accompanied by an increase in their vulnerability. This leads to loss and compromise of sensitive data, system damage, loss of productivity and financial losses. There is increasing evidence that criminals consider vulnerabilities in software systems as a tool to achieve their goals, thus software vulnerabilities are discovered (Seacord, 2013) at a rate of over 4,000 per year. These vulnerabilities are caused by software designs and implementations that do not adequately protect systems, by development practices that do not focus enough on eliminating implementation defects and that lead to security errors. Currently there

[1] Computer science 1
[2] Computer science 2

is little evidence of improving the security of most products; many software developers do not understand the lessons learned about the causes of vulnerabilities or do not apply adequate mitigation strategies. CERT/CC (Computer Emergency Response Team Coordination Center) continues to observe the same types of vulnerabilities in newer versions of products that were discovered in previous versions. The same is confirmed by recent empirical studies (Gueye & Mell, 2021)

C/C++ programming languages are low-level and offer the programmer the ability to manage memory and hardware resources. This is one of the reasons why these languages are quite efficient for developing high-performance applications, thus being widely used (Stroustrup, 2015) in the development of operating systems, embedded systems, financial applications and critical software infrastructures.

Studying the C/C++ programming languages is necessary and useful in the process of training specialists (Aljas et al., 2023) in the field of information technologies, because it develops algorithmic thinking, deep understanding of memory, and promotes the development of good code writing practices. And this requires that attention to detail be paid to the learning process. Moreover, the experience of programming in C/C++ creates premises for the easy acquisition of other programming languages, such as Python, Java, C#.

1. Unsafe programming practices and common errors that can lead to vulnerabilities

The main causes of software vulnerabilities, such as buffer overflows, integer range errors, and invalid format strings, are improper code writing practices. According to CERT guidelines, one of the main causes of vulnerability in information systems is improper memory management (Seacord, 2013). The CERT C/C++ Secure Coding standard defines a set of rules that must be taken into account in the code writing process to prevent software vulnerabilities. In the paper (SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems (2016 Edition), nd) vulnerabilities are aggregated into 15 groups. It is noteworthy that each type of vulnerability is initially presented through non-compliant code, and then the solution is proposed, which leads to the development of less vulnerable code. Most of the vulnerabilities included in the source target basic, initial knowledge in C/C++ programming. This moment confirms once again that securing an application is not the final stage of the project, but it must be a concern from the first line of code written and these skills must be developed starting from the first lessons in the field. In **Error! Reference source not found.**, the most relevant rules have been selected, which must be implemented, developed to students in the process of teaching the subject "Computer Programming".

Table 1. CERT rules relevant to preventing vulnerabilities in C/C++

CERT rule code	Description	Vulnerability type prevented	Example of risk	Recommendation
EXP33-C	Don't use uninitialized variables	Undefined behavior	using a random value	Initialize all variables
MEM30-C	Do not access memory after it has been freed	Use-after-free	invalid pointer dereferences	Use smart pointers
MEM31-C	Frees dynamically allocated memory	Memory Leake	excessive memory consumption	Uses RAII
ARR30-C	Do not access elements outside the bounds of an array	Buffer overflow	buffer overflow	Check the dimensions
STR31-C	Provides enough space for strings	Buffer overflow	strcpy dangerous	Use safe features

Table 1 (Continued)

CERT rule code	Description	Vulnerability type prevented	Example of risk	Recommendation
INT30-C	Avoid numeric overflow	Integer overflow	incorrect values	Check numerical limits
EXP34-C	Do not dereference null pointers	Null pointer dereferences	application crash	Check pointers
FIO34-C	Check for errors in file operations	I/O errors	incorrect read/write	Error handling
ERR33-C	Detects and handles all errors	Logical vulnerabilities	incorrect execution	Use exceptions
MSC00-C	Write clear and secure code	General errors	hard-to-maintain code	Meets standards

Source: *(SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems (2016 Edition) , nd)*

2. Comparing the security of the main programming languages

In the process of developing modern programming languages, one of the main criteria in choosing the technologies used for application development is software security. In this context, languages such as Rust, Java, Python have been designed with additional mechanisms to protect against common classes of vulnerabilities, especially those associated with memory management. Therefore, a comparative analysis (**Error! Reference source not found.**) between these languages provides a useful perspective on the advantages and limitations of each language from a security point of view.

Table 2. Comparison of memory security mechanisms in major programming languages

Characteristic	C++	Rust	Java	Python
Memory management model	manual (new / delete) + RAII	ownership + borrowing	garbage collection	garbage collection
Detecting memory errors	mostly at runtime	mostly at compilation	runtime	Runtime
Typical vulnerabilities	buffer overflow, dangling pointers, use-after-free	very rare (verified at compilation)	low (memory isolation)	LOWER
Memory control	very high	high	Limited	very limited
Performance	very high	very high	high	Moderate
Implicit safety	moderate	very high	high	High
Modern protection mechanisms	RAII, smart pointers, sanitizers	borrow checker	sandbox, garbage collector	runtime safety
Main areas of use	operating systems, embedded, HPC	secure systems, distributed systems	enterprise applications	scripting, data science

Source: *Developed by the author based on (Seacord, 2013), (Klabnik & Nichols, nd), (Grgic et al., 2018; Gueye & Mell, 2021; Stroustrup, 2015)*

Comparing these languages highlights that memory security is directly influenced by the resource management model adopted by each language. C/C++ languages offer the highest level of control over memory, which allows for performance optimization, but also involves significant risks of vulnerabilities if good programming practices are not followed.

Rust introduces an innovative model based on ownership and borrowing, which allows for the detection of many memory errors at compile time. Java and Python use garbage collection mechanisms. collection, reducing the risk of vulnerabilities such as memory leaks or invalid pointer dereferences, but partially sacrificing control over resources.

3. Implications for university education

The dilemma of which programming language should be taken as a beginner CS1[3] and CS2-course is a concern of several researchers. It is obvious that there is no single answer. From the experiments exposed in (Ali & Qayyum, 2021) it was concluded that, if the goal is speed, efficiency and reliability, then C++ is the king of all languages, taking the lead from C, as it offers broader support for approaches due to the support for OOP (Object Oriented Programming), which is missing in C. When developing system software, such as drivers and operating systems, C holds strong compared to C++. Java is the middle ground among all languages; considering that C is complex and has the speed that Python lacks. The authors (Ali & Qayyum, 2021a) consider Java to be a good choice because it not only provides support for "Write Once Run Anywhere", but automatically applies optimizations, something that a novice programmer may not be familiar with. Python is best used if writing software where speed is not a major concern. It is also an excellent choice for beginners and for fields such as Data Science and Artificial Intelligence, due to the large number of libraries it offers. At the same time, the languages C, C++, Java are considered the most difficult to learn (Gomes *et al.*, 2026) .

In 2017, Murphy, Crick and Davenport (Murphy *et al.*, 2017) analyzed introductory programming courses offered in 80 undergraduate Computer Science programmers at UK universities, analyzing the languages, paradigms and tools used in these courses. Java appears to be the dominant language, being used in more than half of the courses, despite Python being considered more accessible for both teaching and learning and the fact that students are generally not experts in programming. The C family of languages (C, C++ and C#) is used in almost a third of cases. The predominant paradigms were object-oriented (50%), followed by procedural (33.8%) and finally functional (8.75%).

In 2018, the paper (Avoris, 2018) presented the results on higher education institutions in Greece, using a public database containing information on study programs, courses and recommended textbooks, with a focus on pedagogical approaches, programming languages and tools used. The C language was identified as the most used language in the analyzed programming courses, present in 37% of the courses, followed by MATLAB (17%) and Basic (11%). According to the results of various studies, Java and Python remain, however, the most popular languages for teaching beginner programmers (Siegfried *et al.*, 2021) . The same study shows that 88% of all schools surveyed use only one of the four programming languages (Java, Python, C++ and C), with Python adoption constantly increasing to the detriment of the other languages. Java continues to be the most popular choice for CS2 courses, followed by C++ but with a significant difference.

In 2024, (Mason *et al.*, 2024) researchers conducted a global study of introductory programming courses, involving instructors from 18 countries across six continents. The study identified Python and Java as the most commonly used programming languages, each accounting for approximately 40% of the courses analyzed. Other languages, such as C++ and C, also appeared with significant frequency (12% and 10%, respectively). JavaScript, Racket, Scala, Go, and Bash were also mentioned, but more marginally, the latter two being used in conjunction with another

[3] **CS1** and **CS2** are standard names used in computer science education for **the first two fundamental programming courses** in university.

programming language. Among the factors influencing language choice, pedagogical benefits were the most important, followed by platform independence and cost/accessibility for students. Industry relevance was also mentioned, but to a lesser extent than in previous regional studies. The study also revealed regional variations, with Python dominating the Americas and Java being more prevalent in Oceania. Regarding the paradigm taught, the results show: procedural (54%), followed by object-oriented (41%) and functional (5%).

For the study (Gomes *et al.*, 2026), institutions were selected using the 2023 Shanghai Ranking for Computer Science and Engineering. Finally, programming languages were successfully identified in 150 courses, including 83 CS1 courses and 67 CS2 courses, from a total of 83 institutions in 14 countries, representing four continents: North America, Asia, Europe and Oceania. According to the study, Java, Python, C and C++ are the programming languages most often chosen for the two initial courses. Java is the most used language in the two introductory programming courses, which are required in 55 (36.7%) of the courses analyzed. It is significant that it is the most used language in CS2, 38 courses – (56.7%) and the second - in CS1- in at least 16 (19.3%) courses. Of the 13 institutions that use the same language in both introductory courses, 10 use Java. Python is second in the choice ranking, but is the main choice for introductory programming courses, with at least 27 occurrences (32.5%). However, it is chosen less often for CS2, dropping to fourth place, with only 5 occurrences (7.5%). C and C++, sometimes used together, are the third and fourth most used programming languages, respectively, with a balanced presence in CS1 and CS2. As a required language, C appears in 27 courses (18.0%), being used 14 times in CS1 (16.9%) and 13 times in CS2 (19.4%). C++, on the other hand, is required in 19 courses (12.7%), with 10 in CS1 (12.7%) and 9 in CS2 (13.5%). Two institutions use C++ in both courses.

The transition between programming languages is also important. (**Error! Reference source not found.**). The most widespread transition is from Python to Java, occurring in 12 institutions, followed by C to Java (6 institutions), Python to C (5), and Python to C++ (4).

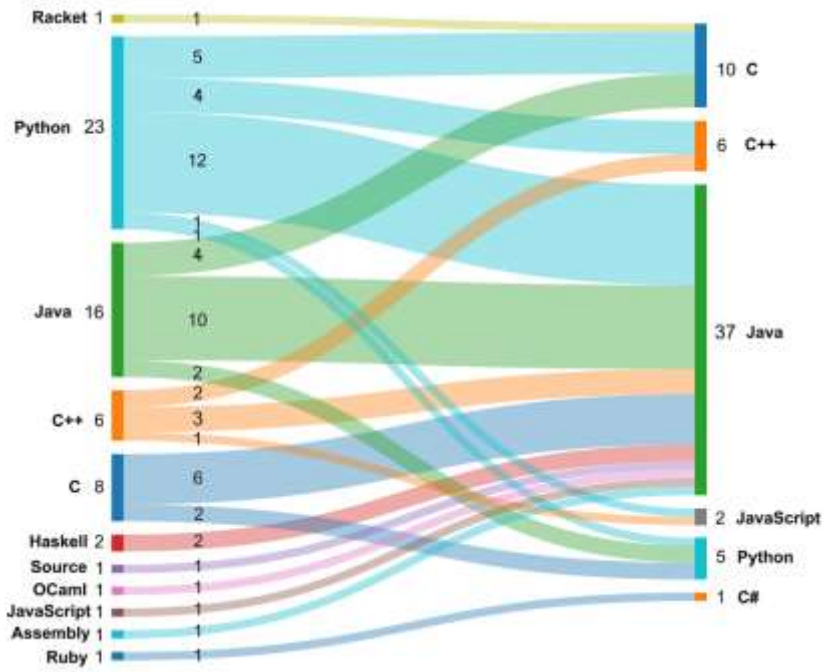


Figure 1. Programming language transition between CS1 and CS2 courses. The width of each band represents the number of institutions transitioning from one language to another.
Source: *(Gomes et al., 2026)*

4. Studying languages within CS1 and CS2 courses in the Republic of Moldova

Analysis of the UTM website the curriculum for specialties in the field 0613 Software and Application Development indicates that CS1 is the discipline "Computer Programming", where C/C++ is taught, and CS2 can be considered the disciplines "Applied Programming Techniques" in some specialties, and "Programming Techniques" in others, where the Python language is taught. The discipline "Object-Oriented Programming" is found in semester 3, but due to the lack of information on the site, it was not determined which programming language is taught.

Within USM , in the plans for programs in the same field in semester 1 there is the discipline "Fundamentals of Programming", and in semester 2 there are the disciplines "Object-Oriented Programming" and "Phyton for Applications". Due to the lack of information on the university website, it is not known which programming languages, except for the last discipline.

Teachers choose a programming language based on its features. For example, Python is valued for its relative ease and readability, Java is valued for its emphasis on object-oriented approaches, and learning C++ allows users to develop an understanding of memory management and resource utilization (Ali & Qayyum, 2021b). In a beginner programming course, best practices should be emphasized, as students' bad habits persist if not reinforced (Dougherty, 2023). The C++ programming language, although a relatively old language, has been updated with new versions regularly since 2011, at a rate of once every three years. Each new version contains important features that make C++ more complex for backward compatibility, but often introduces new features to simplify the process of developing computer projects while respecting cybersecurity requirements. (Seacord, 2020). Currently, the C++23 version is used, and the C++26 version is in the process of being developed.[4]

CONCLUSIONS

Pregnancy universities, which educate specialists in the field of information technologies is to educate primarily algorithmic thinking. In the current conditions, when cyber vulnerability is becoming increasingly important, the educational process must explore programming practices that will help students avoid developing bad habits and will allow them to develop secure programs during their professional careers. From the analysis presented, the programming languages C and C++ are the most vulnerable in this context. On the net textbooks can be found that address the fundamental programming errors in C and C++ that lead to the most common, dangerous, and disruptive software vulnerabilities recorded since the founding of CERT in 1988. The book "Secure Coding in C and C++" (Seacord, 2013) provides both an in-depth engineering analysis of the programming errors that led to these vulnerabilities, as well as mitigation strategies that can be applied effectively and pragmatically to reduce or eliminate the risk of exploitation. Such textbooks can serve as support for cybersecurity disciplines, both in undergraduate and graduate study programs, and would serve as significant support in formulating individual assignments for students, which would allow them to advance in the field, to become established specialists. In the process of teaching programming languages in the first year of a bachelor's degree, especially in the first semester, it is more complicated to pay special attention to security issues, especially when the teacher is primarily tasked with developing programming skills. It is necessary to mention that the skills of first-year bachelor's students to write code are very different: from "never wrote code" to "wrote code in languages such as C++, Java, Python". Some of those who have programming skills have quite in-depth knowledge.

[4]https://isocpp.org/std/status

The choice of programming languages taught in CS1 and CS2 depends on the objectives of the study program. Another important factor is the current requirements of the labor market. It is possible that this choice should also be influenced by the complexity of the language taught.

REFERENCES

Ali, S., & Qayyum, S. (2021). *A Pragmatic Comparison of Four Different Programming Languages*. https://doi.org/10.14293/S2199-1006.1.SOR-.PP5RV1O.v1

Aljas, J., Amores , H., & Lincopinis , D. (2023). *An Overview on C++ Programming Language*.

Avouris, N. (2018). Introduction to computing: A survey of courses in Greek higher education institutions. *Proceedings of the 22nd Pan- Hellenic Conference on Informatics*, 64–69. https://doi.org/10.1145/3291533.3291549

Dougherty, RE (2023). *Creation of a CS1 Course with Modern C++ Principles*. https://arxiv.org/abs/2311.07807

Gomes, JP, Monteiro, R., Moreira, AS, Mendonça, V., Pinho, A., & Cunha, CR (2026). Teaching introductory programming in top universities: A global study of languages, paradigms, assessment, and AI. *Journal of Computer Languages*, *86*, 101384. https://doi.org/10.1016/j.cola.2025.101384

Grgic, H., Mihaljevic, B., & Radovan, A. (2018). Comparison of garbage collectors in Java programming language. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1539–1544. https://doi.org/10.23919/MIPRO.2018.8400277

Gueye, A., & Mell , P. (2021). *A Historical and sTATISTICS Study of the Software Vulnerability Landscape*. https://arxiv.org/abs/2102.01722

Klabnik, S., & Nichols, C. *The Rust Programming Language*. https://doc.rust-lang.org/book/ch03-01-variables-and-mutability.html Accessed 09.02.2026

Mason, R., Simon, Becker, BA, Crick, T., & Davenport, JH (2024). A Global Survey of Introductory Programming Courses. *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1*, 799–805. https://doi.org/10.1145/3626252.3630761

Murphy, E., Crick, T., & Davenport, JH (2017). An Analysis of Introductory Programming Courses at UK Universities. *The Art, Science, and Engineering of Programming*, *1* (2), 18. https://doi.org/10.22152/programming-journal.org/2017/1/18

Seacord, RC (2013). *Secure coding in C and C++* (2nd ed.). Addison- Wesley.

Seacord, RC (2020). Effective C. *Computer*, *53* (11), 79–82. https://doi.org/10.1109/MC.2020.3016369

SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems (2016 Edition) . (n.d.)

Siegfried, RM, Herbert-Berger, KG, Leune , K., & Siegfried, JP (2021). Trends Of Commonly Used Programming Languages in CS1 and CS2 Learning. *2021 16th International Conference on Computer Science & Education (ICCSE)*, 407–412. https://doi.org/10.1109/ICCSE51940.2021.9569444

Stroustrup, B. (2015). *The C++ programming language: C++ 11* (4th ed., 4th print). Addison- Wesley.

INFORMATION SECURITY IN DIGITAL AGRO-TOURISM: CHALLENGES ASSOCIATED WITH IoT AND BIG DATA TECHNOLOGIES

CZU: 004.056:[338.48:004.738.5]
DOI: https://doi.org/10.53486/tids2026.30

SVETLANA CEBAN
ASEM, Chisinau, MD 2005, Republic of Moldova
e-mail: ceban.svetlana@ase.md
ORCID ID: 0009-0006-5957-7666

Abstract. This paper examines the main information security risks related to the use of Internet of Things (IoT) and Big Data technologies in agro-tourism. Digital technologies help agro-tourism businesses promote their services, communicate with customers and manage reservations. However, using online platforms and connected devices can also create security problems, especially when personal data is collected and stored.
The main aim of this study is to identify the security risks associated with these technologies and examine how agro-tourism businesses can manage them. The research is based on a review of scientific publications and institutional materials related to digital transformation, tourism and information security.
The analysis identifies several important issues, including unauthorized access to customer information, security weaknesses in connected devices, dependence on external service providers and limited staff awareness of cybersecurity risks. The study also presents possible measures that businesses can consider to protect information and use digital services more safely.
The findings suggest that information security requires attention not only to technology, but also to staff responsibilities and the management of digital services. Further research involving agro-tourism enterprises in the Republic of Moldova is needed to better understand how these risks are managed in practice.

Keywords: agro-tourism, digital transformation, information security, Internet of Things (IoT), big data, rural development

JEL Classification: L83, O33, Q16, M15

INTRODUCTION

Organizations engaged in tourism activities use online platforms to present their services, communicate with visitors and manage bookings. These platforms are particularly useful for agro-tourism businesses, as they allow potential visitors to plan their visits to rural tourism destinations remotely. Digital systems make an important contribution to the coordination of daily activities. However, each platform used or connected device raises questions about who has access to the information, how securely it is protected against unauthorized access, where it is stored and what level of protection is provided. These questions become more relevant when IoT devices and Big Data applications are introduced (Li *et al.*, 2018; OECD, 2020).

Information security is an important concern for small agro-tourism enterprises, where limited financial resources and the need for technical equipment may involve additional costs. Digital booking and payment platforms collect and store customers' personal data. Data protection is a major concern, and if data is not properly managed, agro-tourism organizations may face risks that could affect both their customers and their own activities. The scientific literature identifies this issue as a major risk requiring particular attention. However, the present study does not measure the frequency of such incidents.

Research on digitalization and digital transformation highlights major changes in organizational structures and management practices (Vial, 2019; Warner and Wäger, 2019). This perspective is

relevant to the agro-tourism sector, as the use of digital technologies also involves responsibilities related to personal data protection, system maintenance and the management of potential risks. In this context, the article raises the following question: What are the main information security challenges associated with the use of IoT and Big Data technologies in digital agro-tourism?

1. MATERIALS AND METHODS

This study analyzes published scientific research and institutional materials related to digital transformation, tourism, the Internet of Things (IoT), Big Data, and information security. The study relies on secondary sources of information, without conducting interviews, field observations, or original technical testing. Therefore, the analysis highlights the main categories of potential risks and the management measures used to address them, without estimating the frequency of incidents occurring in agro-tourism enterprises.

The analysis initially identifies the security issues presented in the selected publications. Subsequently, a comparative analysis identifies the differences between risks associated with connected devices, customer data processing, and the use of third-party platforms. In the final stage, the findings are synthesized into a structured framework that includes the identified risks, potential consequences, and relevant management measures to address them. The comparison is interpretive in nature, and no statistical meta-analysis was conducted.

The synthesis is organized around six main themes: personal data protection, unauthorized access, vulnerabilities of IoT devices, governance of systems that process large volumes of data, staff understanding of information security, and dependence on external service providers. These themes provide a practical framework for examining how technical and organizational decisions interact in the agro-tourism sector.

2. RESULTS AND DISCUSSION

The scientific literature examined indicates that security issues may arise at different stages of digital processes carried out within an agro-tourism enterprise. For example, making a reservation may involve the use of customers' personal data and an external platform, while a connected sensor may require an additional account or a new network connection.

The consequences are influenced by the systems used and the security measures implemented. Thus, the following analysis distinguishes between different types of risk exposure, without assuming that all digital technologies present the same type of risk.

Customer data management represents one of the areas exposed to security risks.

Reservation and payment processes may require the use of customers' names, contact details, and transaction information, some of which may be processed through external services. The main management aspects that need to be considered include data access, data retention periods, and the distribution of responsibilities between the enterprise and its service providers.

The literature on digital transformation provides a basis for examining these issues, although it does not, on its own, establish how widespread these problems are among agro-tourism enterprises in the Republic of Moldova (Vial, 2019).

Another important challenge is associated with IoT devices used in agro-tourism environments. Smart sensors, monitoring systems and connected devices are increasingly used for resource management, environmental monitoring and enhancing tourist experience. However, these devices are often vulnerable to cyberattacks due to weak authentication mechanisms, outdated software and

lack of security updates. These weaknesses may allow unauthorized access and create security problems for the systems used by the business.

Using external platforms can also create some challenges for agro-tourism businesses. For example, a business may use one platform for bookings and another for communication or data storage. These services make daily work easier because the business does not need to manage all the systems itself. However, it is still important to ensure that the services remain available, control who can access the information, and understand how customer data is used and protected.

Furthermore, insufficient cybersecurity awareness among staff and managers significantly increases the exposure to security threats. In many cases, employees are not trained to recognize phishing attacks, manage secure passwords or follow basic data protection practices. When employees are not familiar with basic security rules, mistakes may occur that put business information at risk. This review brings together the main technical and organizational risks, as well as those related to external service providers, in the context of agro-tourism. The study does not aim to measure the level of cybersecurity in rural businesses. Instead, it highlights the main issues that managers should consider when choosing and using digital services.

The main information security challenges identified in digital agro-tourism systems are summarized in Figure 1.



Figure 1. Information Security Challenges in Digital Agro-Tourism Systems.
Source: *Author's own elaboration.*

These findings show why agro-tourism businesses need to consider security when using digital technologies.

The main risks identified in the analysis can also be systematized according to the digital component involved, the possible impact on agro-tourism enterprises and the recommended security measures, as shown in Table 1.

Table 1. Main Information Security Challenges in Digital Agro-Tourism Enterprises.

Digital component	Main security risk	Possible impact	Recommended measure
IoT devices and sensors	Unauthorized access, weak authentication	System compromise, operational disruption	Strong authentication, regular updates
Online booking platforms	Exposure of customer and payment data	Data breaches, loss of customer trust	Secure storage, encryption, access control
Big Data systems	Misuse of personal and behavioral data	Privacy violations, reputational damage	Data governance and anonymization
Cloud services	Dependence on external providers	Service interruption, limited data control	Backup systems and provider assessment
Staff digital tools	Phishing, weak passwords, human error	Account compromise, financial and reputational risks	Cybersecurity training and password policies

Source: *Author's own elaboration based on Vial (2019), Gretzel et al. (2015) and Li et al. (2018).*

Table 1 presents the main digital technologies, their security risks, possible effects on business activities, and measures that can help reduce these risks. The table shows that different technologies need different security measures. For example, connected devices need regular updates and secure access, while customer data must be protected through clear rules on who can use and manage it. Staff training is also important for all these activities.

In the Republic of Moldova, this table can help agro-tourism businesses better understand the security risks related to digital technologies. Online advertising and booking platforms are useful for rural tourism, but this study does not provide direct information about how widely these services are used or how often cybersecurity incidents occur in Moldova. More research involving local agro-tourism businesses is needed to understand which risks are most important and how they can be managed in practice (World Tourism Organization, 2023; Biroul Național de Statistică, 2024; European Commission, 2021).

The use of digital technologies also raises questions about the long-term development of agro-tourism businesses. When these businesses depend on online platforms and digital systems, they need to consider how to protect customer information and keep their services working. Basic security measures can help reduce problems and maintain customer trust.

At the same time, digital security has become closely connected to the reputation and market position of agro-tourism enterprises. Tourists increasingly rely on online reservations, digital communication and electronic payments when choosing tourism services. Any cybersecurity incident involving personal data or online transactions may negatively affect customer confidence and reduce the competitiveness of rural tourism destinations. Therefore, information security should be integrated not only into technological management, but also into strategic planning and sustainable rural tourism development policies (Vial, 2019; OECD, 2020; UN Tourism, 2023).

3. PRACTICAL RECOMMENDATIONS FOR STRENGTHENING INFORMATION SECURITY IN DIGITAL AGRO-TOURISM

The risk categories discussed above highlight several management measures that agro-tourism enterprises can adapt to the systems they use. These are recommendations based on the review of scientific literature, rather than measures whose effectiveness was tested in the present study. The usefulness of these recommendations depends on the size of the enterprise, the services it uses, and the types of information it processes.

One important recommendation is that agro-tourism businesses should implement stronger access control measures, including secure password policies, multi-factor authentication and restricted access to sensitive data. These measures reduce the risk of unauthorized access to digital platforms, booking systems and internal databases.

Regular software updates and technical maintenance of IoT devices are also essential for preventing cyberattacks and reducing system vulnerabilities. Smart sensors and connected devices should be monitored continuously to ensure secure operation and timely detection of security incidents.

Customer information, booking records and payment data should also be protected through encryption and secure storage solutions. Data protection policies should comply with digital privacy standards and ensure the confidentiality and integrity of sensitive information.

Another important recommendation is the development of cybersecurity awareness among staff and managers. Employee training in recognizing phishing attempts, managing passwords securely and applying basic digital protection practices can significantly reduce human-related security risks.

Finally, agro-tourism enterprises should integrate cybersecurity into their broader digital transformation strategy. Information security should be approached not only as a technical issue, but also as a managerial and strategic component of sustainable business development.

These recommendations may help agro-tourism businesses protect customer information, reduce security risks and use digital services more safely (Vial, 2019; Gretzel et al., 2015; OECD, 2020).

The main practical measures that can be implemented by agro-tourism enterprises include the following:

- implementation of secure password policies;
- regular software and firmware updates for IoT devices;
- encryption of customer and payment data;
- employee cybersecurity awareness training;
- secure cloud data management;
- data backup and recovery planning;
- periodic cybersecurity risk assessment;
- compliance with cybersecurity and data protection regulations.

CONCLUSIONS

The literature review identifies several issues that require attention when IoT technologies, applications that process large amounts of data, and online services are used in agro-tourism. These include access to customer information, maintenance of connected devices, dependence on service providers, and staff practices. These issues are connected, but they require different security measures. The analysis provides a structured overview of possible risks without showing that a specific percentage of agro-tourism enterprises has experienced cyberattacks.

One of the main results of the study is the grouping of security issues according to digital components and the management measures needed. In this way, information security is not only a separate technical activity. It also requires decisions about the distribution of responsibilities, cooperation with service providers, and procedures followed by staff. This interpretation is consistent with the approaches presented in the literature on organizational digital transformation (Vial, 2019; Warner and Wäger, 2019).

The study is based on a qualitative analysis of secondary information sources and has certain limitations. The research did not include a representative sample of agro-tourism enterprises or actual data on cybersecurity incidents. In addition, no testing of IoT devices was carried out during the research. Future research could include interviews and surveys with owners of agro-tourism enterprises in the Republic of Moldova. This could help provide a clearer understanding of how digital technologies are used, what security measures are currently in place, and which of the proposed recommendations could be applied in practice.

The proposed framework can help organize future research on digital risks in rural tourism. Its importance lies in identifying the main factors that need to be examined in relation to data, devices, service providers, and staff practices. However, it should not be considered a validated model for evaluating cybersecurity performance.

For managers of agro-tourism enterprises and local stakeholders, the first step is to examine how digital services are used and to establish responsibilities for protecting the information they

process. Introducing basic security measures and reviewing relationships with service providers can contribute to safer and more stable business operations.

However, further research and analysis based on data collected directly from enterprises in the Republic of Moldova are needed to determine which of the proposed measures should be applied first and to evaluate their results.

REFERENCES

Biroul Național de Statistică, 2024. *Activitatea turistică a agenților de turism și turoperatorilor în anul 2023*. Available at: https://statistica.gov.md/ro/activitatea-turistica-a-agentiilor-de-turism-si-turoperatorilor-in-anul-2023-9491_60952.html [Accessed 10 January 2026]

European Commission, 2021. *Digital Transformation of Tourism*. Available at: https://ec.europa.eu [Accessed 10 January 2026].

Gretzel, U., Sigala, M., Xiang, Z. and Koo, C., 2015. Smart tourism: foundations and developments. *Electronic Markets*, 25(3), pp.179–188.

Li, L., Su, F., Zhang, W. and Mao, J.-Y., 2018. Digital transformation by SME entrepreneurs: A capability perspective. *Information Systems Journal*, 28(6), pp.1129–1157.

OECD, 2020. *Tourism Trends and Policies 2020*. Paris: OECD Publishing.

World Tourism Organization, 2023. Tourism and Rural Development: A Policy Perspective. Madrid: UNWTO. https://doi.org/10.18111/9789284424306.

Vial, G., 2019. Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 28(2), pp.118–144.

Warner, K.S.R. and Wäger, M., 2019. Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, 52(3), pp.326–349.

SECURITY CHALLENGES IN VIDEO CONFERENCING APPLICATIONS: A CASE STUDY ON MICROSOFT TEAMS

CZU: 004.056:004.738.52
DOI: https://doi.org/10.53486/tids2026.31

AURELIU ZGUREANU
Academy of Economic Studies of Moldova (ASEM)
e-mail: zgureanu.aureliu@ase.md
ORCID ID: 0000-0003-3301-2457

SERGHEI OPREA
Academy of Economic Studies of Moldova (ASEM)
e-mail: oprea.serghei@ase.md
ORCID ID: 0000-0003-3759-8598

Abstract. The rapid expansion of remote work and digital collaboration has positioned video conferencing platforms at the centre of organisational communication infrastructure. Microsoft Teams, with over 320 million monthly active users across more than one million organisations worldwide, has become a primary target for a wide spectrum of cyber threats. This paper investigates the security challenges inherent to video conferencing applications, with a focused case study on Microsoft Teams app. The research examines the threat landscape through five interconnected dimensions: technical vulnerabilities exploitable at the protocol and application layer; social engineering and phishing campaigns exploiting user trust within the platform; data privacy risks arising from inadequate encryption, misconfigured permissions, and insecure third-party integrations; regulatory compliance challenges under frameworks such as the GDPR and HIPAA and the human factors that amplify technological vulnerabilities. Based on peer-reviewed academic literature, official Microsoft security documentation, threat intelligence reports from organisations including Check Point Research and Microsoft DART, and disclosed CVE records, the paper constructs a comprehensive threat taxonomy. Specific attack techniques examined include the GIFShell attack chain enabling covert data exfiltration through legitimate Microsoft infrastructure, remote code execution vulnerabilities triggered via adversary-crafted meeting invitations, identity spoofing through webhook payload manipulation, and state-sponsored social engineering campaigns attributed to the Midnight Blizzard threat actor. The paper further analyses the permission escalation risks within the Teams add-on ecosystem and the privacy side-channels introduced by virtual backgrounds and auxiliary devices. The findings reveal that the security posture of Microsoft Teams is compromised not solely by software defects but by systemic design trade-offs that prioritise usability and interoperability. Mitigation recommendations include technical hardening measures, governance frameworks, and user education programmes. This research contributes to the growing body of knowledge on enterprise collaboration platform security and provides practitioners with actionable guidance for securing video conferencing environments.

Keywords: Microsoft Teams, video conferencing security, cybersecurity, social engineering, data privacy, GDPR compliance.

JEL Classification: M15, K24, O33.

INTRODUCTION

The COVID-19 pandemic beginning in early 2020 sped up the use of video call platforms in most industries, including education, healthcare, government, and the private sector. What had once been a temporary solution became critical. Microsoft Teams became one of the major platforms during this time. Its rise was facilitated by the deep integration of the Microsoft 365 suite and its

business tools. By 2024, Microsoft Teams reached over 320 million daily active users, greatly increasing its strategic importance, and its attractiveness as a target by threat actors. (Charikov and Vanunu, 2025).

Research into security issues on different video conferencing platforms expanded significantly. Kagan *et al.* (2020) demonstrated that malicious actors could exploit publicly accessible meeting links to collect biometric data from unsuspecting participants. This data may include facial images, voice samples, and other types of data. The authors also showed that deep-learning algorithms could be used to identify a person in others different meetings, raising severe privacy issues. Alammary *et al.* (2022), used the Knowledge-Attitudes-Behaviours mode to survey data from 307 faculty members across 43 different universities in Saudi Arabia. Then they showed that the level of video conference security settings is "poor" and emphasizes the human factor as the most significant vulnerability. The threat modelling study published by Hasan and Hasan (2022) used the widely known STRIDE framework - Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege - on different video conferencing tools and effectively constructed an exhaustive list of risk categories applicable directly also to Teams.

Microsoft Teams continues to be a popular tool within organizations worldwide, thus, suggesting a need for continued research and security assessments.

Bobby Rauch revealed the GIFShell attack chain on September 2022, which showed that by chaining together seven vulnerabilities in Microsoft Teams, a covert reverse shell could be created that exfiltrated commands and data via Microsoft's own infrastructure (Rauch, 2022). Microsoft released fixes for CVE-2023-29328 and CVE-2023-29330 in August 2023, both of which are critical remote code execution vulnerabilities that could be exploited by getting a target user to join an adversary's Teams meeting (Munshaw, 2023). Additionally, Charikov and Vanunu (2025) identified a series of notification manipulation and message spoofing vulnerabilities that allow for identity impersonation on the Teams platform, which are officially tracked as CVE-2024-38197. In parallel, Microsoft's threat intel revealed that APT29, a state-funded Russian threat actor, used Teams as a channel for a spear-phishing attack to obtain credentials from government and critical infrastructure organizations (Intelligence, M.T., 2023).

This paper provides an analysis of Microsoft Teams security - the technological vulnerabilities, threat analysis, and industry compliance frameworks. It aims to lay down the imperative security challenges posed by Microsoft Teams within an evidence-based analytical framework. The analysis of the security challenges posed by Microsoft Teams will be broken down into implicit threat actors and APT analysis, various attack mechanisms and their relative effectiveness, the severity of violation and defensive mechanisms in place, and technical and non-technical solutions to address the security challenges in a vertical and horizontal stance.

MAIN CONTENT

1. Platform Architecture and Security Model

Microsoft Teams is built on Microsoft 365's hyper-scale cloud platform, combining proprietary protocols and standard protocols. Secure Real-time Transport Protocol (SRTP) is used to deliver audio and video streams, and all data in transit is encrypted and protected by Transport Layer Security (TLS). Data in Microsoft's data centers is secured by BitLocker, and any files in OneDrive or SharePoint inherit the encryption schemes of those services. The application's desktop client is built on Electron, a framework that embeds a Chromium-based browser engine to render web technologies

as native desktop applications. This architectural option presents the most important security risk. Electron does not enforce encrypted or protected file storage by default, meaning that local Teams log files - which may contain session tokens and sensitive metadata - are accessible to any process running under the user's account. This exposure was a foundational prerequisite for the GIFShell attack. (Keusseyan, 2024). This Security flaw was a founding condition of the GIFShell assault. Microsoft Teams uses Azure AD as the primary provider, and Microsoft provides authentication mechanisms that are required by the platform. All authentication mechanisms are based on the OpenID Connect and OAuth 2.0 processes. This creates the option for, and in some cases the obligation for implementers to use, multi-factor authentication. Azure AD creates the conditions for Microsoft Teams to have fine-grained control mechanisms.

Research made available in 2025 on arXiv showed that an automated testing tool dubbed TAI found 41 host APIs which can be manipulated by add-ons for permission escalation, thus allowing access to documents, spreadsheets, and shared drives that are outside the scope of the add-on's permissions.

2. Technical Vulnerabilities and Attack Techniques

The Microsoft Teams software can be attacked in various ways, but the most concerning of these involve RCE vulnerabilities, including CVE-2023-29328 and CVE-2023-29330. Munshaw (2023) says that both vulnerabilities allow an attacker to send a Teams meeting invite, and the recipient does not need to take any other action to participate in the meeting and thus be attacked, which significantly lower the barrier to exploit. Having an RCE vulnerability that does not require an attacker to pre-coordinate with a target or exploit a vulnerability on the target to gain a foothold is especially dangerous for RCE vulnerabilities in Microsoft Teams.

In 2022, Rauch introduced the GIFShell technique, which is a covert channel attack that allows the attacker to send text and lead the recipient to an attacker designated website using created API requests. This allows a user to bypass the Teams restriction on sharing outside of the Teams community and send a file to appear as benign images, Teams' retrieval of GIF images from attacker-controlled servers, and the embedding of executable commands within base64-encoded GIF filenames. Since the exfiltration pathway along with the telemetry traffic is a normal Teams traffic, the activity is unlikely to be flagged by EDR or other network monitoring systems. Microsoft said that the GIFShell technique is a post-exploitation technique and does not need an urgent fix (as of 2022, this technique is more or less a GIF hacking channel).

Table 1. Classification of Security Threats in Microsoft Teams

Threat Category	Attack Vector	Key CVE / Case Study
Remote Code Execution	Malicious meeting links	CVE-2023-29328, CVE-2023-29330
Identity Spoofing	Webhook payload forgery	CVE-2024-38197 (Check Point, 2025)
Data Exfiltration	GIF-embedded commands	GIFShell chain (Rauch, 2022)
Social Engineering	Cross-tenant vishing	Midnight Blizzard (Microsoft, 2023)
Privilege Escalation	Third-party add-on abuse	TAI tool findings (Wan et al, 2025)
Privacy Side-Channel	Virtual background instability	He & Lei (2021)

Source: *Compiled by the author based on Intelligence, M.T. (2023), Microsoft (2023b)*, *Microsoft (2026), Charikov and Vanunu (2025), Rauch (2022), Wan et al. (2025).*

Identity spoofing allows deception of users by having them believe a message has originated from a trusted contact. A technique of this kind of deception, described by Charikov and Vanunu (2025), is employing bots and webhooks to generate message payloads that falsify sender attributes. Check Point Research discovered that these bots and webhooks modified messages to appear as if they originated from Teams executives or other trusted users. The CVE-2024-38197 vulnerability has been classified with a medium severity rating. This classification suggests that some degree of attacker access is required to the organization's tenant. The researchers have, however, demonstrated a proof of concept that amplifies the risk of business email compromise (BEC) style activities in the Teams environment.

3. Social Engineering and Phishing via Microsoft Teams

Instead of short phishing messages, social engineering has developed into sophisticated intrusion campaigns. Midnight Blizzard, also known as APT29, Cozy Bear, and NOBELIUM, compromised multiple Microsoft 365 small business tenants and created domains to impersonate the Microsoft 365 technical support. Several messages were sent to the Microsoft 365 ‘Teams’ to the employees and contractors of the government and critical infrastructure, suggesting a type of support request to approve multi-factor authentication during an assumed Microsoft 365 technical support scenario. This, among others, is one of the campaigns described in the 2023 Microsoft Threat Intelligence report. The latest sophisticated campaign has also been revealed by the Microsoft Detection and Response Team during the 2026 Microsoft Threat Intelligence report. While DART was engaged to the customer in November 2025, a persistent voice phishing campaign through Microsoft 365 Teams was documented. Impersonating from the Microsoft 365 IT Helpdesk, the customer DART employees were called multiple times. The employees were prompted to open the Microsoft 365 Teams remote control feature; Quick Assist, from which the phishing Helpdesk was able to take full control of the devices, conduct reconnaissance, lateral movement and access the Microsoft 365 domains and the Windows Server domain controllers. Microsoft has also documented the activities of a group of fraudsters who referred to themselves as the UNC6692 group, during an April 2026 Microsoft Threat Intelligence Report. This group has also used a similar methodology as described above, but further advanced by creating and deploying a custom malware dubbed SNOW and a malicious browser extension.

According to Gogia's (Swain, 2026) description, this depicts a less traditional variety of phishing he describes as “guided execution.” In this variation, attackers prematurely integrate themselves into legitimate enterprise workflows for the purpose of guiding their victim to execute a series of actions that result in the granting of access permissions. He & Lei (2021) describe a more nuanced general social engineering threat. They describe the reality that virtual backgrounds in modern video conferencing solutions may not be entirely virtual, which may inadvertently compromise the physical social environment of the target that social engineering efforts are aimed at, revealing new information to the social engineer of potential.

4. Data Privacy and Regulatory Compliance

Microsoft Teams operates within a broad compliance ecosystem. Based on compliance with numerous regulatory frameworks, including HIPAA, GDPR, FedRAMP, SOC 1, SOC 2, and FERPA, Teams facilitates compliance with over 90 different regulations and laws. Microsoft includes Teams in compliance with regulations for GDPR, HIPAA, and FedRAMP, among others (Microsoft Pulse 2025). While Microsoft operates as a data processor for customers in GDPR compliance, Microsoft

provides Standard Contractual Clauses (SCCs) in place of GDPR compliance for cross-border data transfers from the European Economic Area (Microsoft (2023a), Microsoft (2023b)).

Implementing Teams to support compliance is only the first step, as there are considerable compliance related demands on the organization. The European Banking Authority (EBA 2025) Microsoft Teams Data Protection Notice describes the types of processed personal data. These data types consist of biometric data, voice and meeting recordings, etc. The transfer of sensitive data is prohibited without explicit user consent. One of the compliance gaps is that Microsoft 365 average retention is 30 to 90 days, however, regulated industries (mostly, financial services) have to comply with long retention (up to 7 years) requirements (FINRA 4511), and, as a result, require 3rd party archiving services (Clarke, 2025).

Data Compliance is complicated with various archiving requirements. While data is stored in the regional Microsoft 365 compliance instance, it is also persistently stored in multiple instances of compliance data in the Microsoft 365 ecosystem.

Organizations subject to stringent data sovereignty protocols - including (but not limited to) defence, health care, and government sectors - must assess their data residency setup and, if applicable, implement Microsoft Teams in government cloud (GCC) or sovereign cloud implementations. The assertion made by the GDPR that encryption is a consequence modifier for breach notifications speaks to and creates an argument for the necessity that all data pathways in Microsoft Teams be configured such that there is a strict adherence to encryption by way of the protocols TLS and SRTP (Microsoft Learn, GDPR, 2025).

5. Materials and Methods

This research adopts a qualitative systematic review framework to collate evidence across several categories: (1) peer-reviewed papers accessed through arXiv, PubMed Central, and publisher internet gateways, chosen for their relevance to security in online videoconferencing in general, and Microsoft Teams in particular; (2) exposed vulnerabilities in the Common Vulnerabilities and Exposures (CVE) database, along with patch Tuesday advisories; (3) threat intelligence reports from Microsoft's Detection and Response Team, Microsoft Threat Intelligence, and Check Point Research; (4) Microsoft's technical documentation located on Microsoft Learn and in The Microsoft Trust Centre; and (5) Microsoft's GDPR documentation and European Banking Authority regulatory documentation.

Sources were judged based on four characteristics: recency (sources published from March 2020 to the present for their relevance to the post-pandemic context), authoritativeness (published and peer-reviewed papers and reports from established security research organisations), relevance (applicability to Microsoft Teams and/or the security of video conferencing), and methodological rigor (research incorporating threat models, or experimental frameworks, or validated instruments). The STRIDE model of threat is utilized to construct the threat taxonomy illustrated in this paper, in accordance with the Hasan and Hasan (2022) study. The yield of this taxonomy is shown in Table 1.

6. Results and Discussion

The sources collectively demonstrate a complex threat scenario for Microsoft Teams comprising multiple technical, human, and regulatory layers. The technical threat derives from the Electron-based desktop client, which creates a persistent attack surface that still requires constant vigilance even if the code is patched. Electron prioritizes platform bridging for the sake of convenience over containing the filesystem, which is the underlying root of the desktop client attack surface. The reemergence of RCE vulnerabilities in the meeting subsystem (CVE-2023-29328, CVE-

2023-29330) signifies a sustained challenge in containing an untrusted input that is capable of exploiting the meeting subsystem and other complex media processing pipelines.

From a human perspective, the combination of two trends poses a notable threat. The first is the declining notion of an "inside versus outside" boundary of communications in the context of Teams. The second is social engineering, in which exploitation of this boundary is becoming systematically more complex. As Kaur (Swain, 2026) noted, collaboration platforms that enable real-time interaction allow for a more believable and actual instance of an IT personnel impersonation in comparison to more traditional email-based phishing. The interaction, in this instance, takes place in a channel that users implicit trust toward Teams and collaboration platform communications. This finding corroborates the low usability awareness scores attained by Alammary et al. (2022), signifying that user training in and of itself is insufficient.

While vendor threat modelling, in general, is characterized by distinctive limitations, the GIFShell experiment is a particularly appropriate and illustrative example of such limitations. Microsoft's definition of the GIFShell attack is a post-exploitation technique that lies outside the vendor's concerns for "immediate" or "near-term" mitigation. This post hoc evaluation of the attack is the result of a low contextual security boundary that fails to capture the cumulative nature of the risk that follows from multiple rounds of design violations of a low company security threshold.

From a risk management viewpoint, we should assess the likelihood of threat actors capitalizing on a particular vulnerability, as opposed to the single, arbitrary severity of a vulnerability. Here, the likelihood is, indeed, affirmative.

The disagreement in the privacy regulatory layer is once more the distance of Microsoft's assurances of compliance and the real compliance Microsoft achieves. The GDPR mandates that the organisational customer that deploys Microsoft Teams must, among other things, appoint a Data Protection Officer, issue privacy notices, and carry out and maintain Records of Processing Activities. The EBA's formal data protection notice for Teams illustrates this point: even a sophisticated financial regulator requires a dedicated legal instrument to govern its own use of the platform.

CONCLUSIONS

This work provided an insight into the Microsoft Teams platform and its most critical security issues when using video conferencing software. The evidence demonstrates that the platform's threat landscape encompasses technical vulnerabilities at the application and framework layers, sophisticated social engineering campaigns conducted by both cybercriminal and state-sponsored threat actors, data privacy risks arising from design trade-offs and third-party integrations, and significant organisational compliance burdens under major data protection regulatory frameworks.

The novelty of this research lies in its integrative approach, combining CVE-level technical analysis, security psychopathy of active threats, and regulatory compliance frameworks to form an integrated and unified threat taxonomy. Additionally, it provides fundamental evidence against the hypothesis which suggests enterprise-level video conferencing software that provides substantial compliance frameworks is secure. Also, security posture is the outcome of a combination of a user's deployment structure, behaviour, and governance as a regulation.

This work recommends an integrated view of security posture at the philosophy level which mainly includes the extensibility of policy and technical control to address the gaps in framework security posture.

- Technical control options include disallowing inter-tenant communication, deactivation of Quick Assist, enacting SMB signing, enforcement of MFA, and removal of remote access;
- Policy control options include implementation of DLP frameworks and defining retention schedules;
- Programs to educate users on the risks of Teams social engineering;
- Comprehensive oversight of Teams users to increase ID access control via adjustment of Security Information Event Management (SIEM) structures to allow for the oversight and control of foreign access.

Future research directions include longitudinal analysis of the effectiveness of user training interventions in reducing Teams-based social engineering susceptibility, empirical evaluation of the security impact of the new Teams client architecture released in 2024, and comparative analysis of security postures across competing enterprise collaboration platforms. A limitation of this study is its reliance on publicly disclosed vulnerabilities and threat intelligence; zero-day vulnerabilities actively exploited in the wild remain, by definition, uncharacterised in the open literature.

REFERENCES

Alammary, A., Alshaikh, M. and Pratama, A.R. (2022). Awareness of security and privacy settings in video conferencing apps among faculty during the COVID-19 pandemic. *PeerJ Computer Science*, 8, p.e1021. doi:https://doi.org/10.7717/peerj-cs.1021.

Charikov, A. and Vanunu, O. (2025). *Exploiting Microsoft Teams: Impersonation and Spoofing Vulnerabilities Exposed Microsoft Teams Vulnerabilities Uncovered*. [online] Check Point Research. Available at: https://research.checkpoint.com/2025/microsoft-teams-impersonation-and-spoofing-vulnerabilities-exposed/.

Clarke, J. (2024). *Microsoft Teams Compliance: GDPR, FINRA*. [online] Global Relay. Available at: https://www.globalrelay.com/resources/the-compliance-hub/compliance-insights/mirosoft-teams-compliance-gdpr-finra/.

European Banking Authority (EBA) (2025). *Privacy notice on processing personal data in Microsoft Teams*. [online] Available at: https://eba.europa.eu/sites/default/files/document_library/General%20Pages/Legal%20notice%20page/930896/Data%20Protection%20Notice%20on%20the%20Use%20of%20Microsoft%20Teams.pdf.

Hasan, R. and Hasan, R. (2022). Threat model and security analysis of video conferencing systems as a communication paradigm during the COVID-19 pandemic. In: *Novel AI and Data Science Advancements for Sustainability in the Era of COVID-19*. [online] Academic Press, pp.181–199. doi:https://doi.org/10.1016/b978-0-323-90054-6.00009-x.

He, S. and Lei, Y. (2021). *The privacy protection effectiveness of the video conference platforms' virtual background and the privacy concerns from the end-users*. [online] arXiv.org. Available at: https://arxiv.org/abs/2110.12493 [Accessed 29 Apr. 2026].

Intelligence, M.T. (2023). *Midnight Blizzard conducts targeted social engineering over Microsoft Teams*. [online] Microsoft Security Blog. Available at: https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/.

Kagan, D., Alpert, G.F. and Fire, M. (2020). Zooming Into Video Conferencing Privacy and Security Threats. *arXiv:2007.01059 [cs]*. [online] Available at: https://arxiv.org/abs/2007.01059.

Keusseyan, R. (2024). *Public Security Announcement: Microsoft Teams Vulnerabilities*. [online] Isec7.com.

Available at: https://blog.isec7.com/en/public-security-announcement-microsoft-teams-vulnerabilities [Accessed 29 Apr. 2026].

Microsoft (2023a). *General Data Protection Regulation - Microsoft GDPR*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr.

Microsoft (2023b). *Overview of security and compliance - Microsoft Teams*. [online] learn.microsoft.com. Available at: https://learn.microsoft.com/en-us/microsoftteams/security-compliance-overview.

Microsoft (2026). *Cross-tenant helpdesk impersonation to data exfiltration: A human-operated intrusion playbook | Microsoft Security Blog*. [online] Microsoft Security Blog. Available at: https://www.microsoft.com/en-us/security/blog/2026/04/18/crosstenant-helpdesk-impersonation-data-exfiltration-human-operated-intrusion-playbook/ [Accessed 29 Apr. 2026].

Microsoft Pulse. (2020). *Our commitment to privacy and security in Microsoft Teams*. [online] Available at: https://pulse.microsoft.com/en/work-productivity-en/na/fa2-our-commitment-to-privacy-and-security-in-microsoft-teams/.

Munshaw, J. (2023). *Six critical vulnerabilities included in August's Microsoft security update*. [online] Cisco Talos Blog. Available at: https://blog.talosintelligence.com/patch-tuesday-august-2023/ [Accessed 28 Apr. 2026].

Rauch, B., 2022. *GIFShell — covert attack chain and exfiltration via Microsoft Teams GIFs*. Medium/BleepingComputer disclosure, September 2022.

Swain, G. (2026). *Attackers abuse Microsoft Teams to impersonate the IT helpdesk in a new enterprise intrusion playbook*. [online] CSO Online. Available at: https://www.csoonline.com/article/4160858/ [Accessed 28 Apr. 2026].

Wan, L., Yan, C., Meng, M.H., Wang, K., Wang, H., Bai, G. and Dong, J.S. (2025). *Beyond the Scope: Security Testing of Permission Management in Team Workspace*. [online] arXiv.org. Available at: https://arxiv.org/abs/2506.17317 [Accessed 28 Apr. 2026].

THE ECONOMICS OF DIGITAL CRIME: UNDERSTANDING THE CYBERCRIME VALUE CHAIN

CZU: 343.9:007.52+004.056
DOI: https://doi.org/10.53486/tids2026.32

DAVID NAVAS
Financial University under the Government of the Russian Federation
e-mail: d.navvas@gmail.com
ORCID ID: 0009-0008-7333-5991

IVAN KULAKOV
Financial University under the Government of the Russian Federation
e-mail: kulakovi849@gmail.com
ORCID ID: 0009-0007-8824-9239

DINARA ORLOVA
DSC, Professor, Department of Economics
Financial University under the Government of the Russian Federation
e-mail: DROrlova@fa.ru
ORCID ID: 0000-0002-2901-070X

Abstract. Cybercrime has developed into a global market in which different participants supply distinct services rather than carrying out every stage of an attack themselves. The resulting division of labour links malware developers, access sellers, platform operators and financial intermediaries in arrangements that resemble commercial supply chains. This article considers the economic implications of that shift, focusing on how specialization, digital platforms and technological change shape the organization and durability of illicit online markets.

The discussion draws on Transaction Cost Economics, Platform Economy Theory and Value Chain Theory to examine how these markets are organized. It considers Initial Access Brokers, Ransomware-as-a-Service arrangements, darknet marketplaces, cryptocurrency-related laundering services and the growing use of artificial intelligence. Particular emphasis is placed on the business arrangements behind these activities: affiliate relationships, outsourced tasks, specialized suppliers and platforms that can serve many participants at once.

Evidence from cybersecurity reports, threat intelligence publications and law-enforcement assessments points to a recurring economic problem: some cybercriminal operations can be initiated at a modest cost while exposing victims to much larger losses. Marketplaces also help otherwise anonymous buyers and sellers locate one another, assess counterparties and arrange transactions. AI tools may reduce the time and expertise needed for certain tasks, although their effects differ across activities and are not always straightforward to measure.

The analysis therefore treats cybercrime as more than a collection of technical incidents. It is also a cross-border system of incentives, exchanges and specialized services. This perspective suggests that technical defenses are necessary but insufficient on their own: interventions must also address the markets, intermediaries and financial incentives that allow criminal operations to continue.

Keywords: Cybercrime economy, cybercrime value chain, ransomware-as-a-service, darknet platforms, digital crime monetization, artificial intelligence in cybercrime.

JEL Classification: K42, O33, L86

INTRODUCTION

The organization of cybercrime has changed considerably over the last twenty years. An attack that once might have depended on one individual carrying out several tasks can now involve separate providers of software, infrastructure, stolen access and payment services. These participants need not belong to a single organization; they may cooperate only for a particular transaction. In this respect, parts of the underground economy have begun to resemble legitimate digital industries, with recognizable divisions of labour, intermediaries and methods of generating revenue. Such arrangements make it easier to repeat operations and replace individual participants when necessary.

As economic activity has moved online, the possible consequences of cybercrime have grown with it. Cybersecurity Ventures (2025) projects annual worldwide cybercrime damages above USD 10.5 trillion, although estimates of this kind should be read as projections rather than observed criminal revenue. Businesses now rely heavily on cloud services, remote access, electronic payments and digitally connected suppliers. Each dependency can create an additional point of exposure. The resulting risks are not confined to technology companies: public authorities, banks, hospitals, multinational businesses and operators of essential infrastructure all depend on systems that can be disrupted or misused.

Greater spending on cybersecurity and closer cooperation between enforcement agencies have not removed the incentives behind cybercrime. An important reason is the gap between what an attacker may need to spend and what a successful incident can cost the victim. Certain phishing or credential-theft operations require limited infrastructure, while the consequences can include business interruption, remediation expenses and direct financial loss. Not every attempt succeeds, and criminal revenue is not the same as victim damage. Nevertheless, the possibility of substantial returns from comparatively inexpensive operations helps explain why new participants continue to enter these markets.

Crime-as-a-Service (CaaS) has made this division of labour especially visible. Ransomware-as-a-Service (RaaS), Malware-as-a-Service (MaaS) and phishing-as-a-service arrangements allow one participant to use tools or infrastructure supplied by another. A buyer may therefore avoid developing software, maintaining servers or acquiring every relevant skill independently. Darknet marketplaces and encrypted channels provide venues where these services can be advertised and negotiated. The practical consequence is a lower entry threshold for some criminal activities and a market in which specialized suppliers can serve multiple customers.

These exchanges face a problem familiar to economists: participants often know little about the people on the other side of a transaction. Darknet marketplaces respond with mechanisms that also appear in lawful online commerce, including seller ratings, escrow arrangements, dispute procedures and verification systems. None of these features eliminates fraud or guarantees trust. They can, however, make transactions more predictable and reduce the effort involved in finding a counterparty. Where a platform attracts enough buyers and sellers, its growing network may encourage additional specialization and trading activity.

Artificial intelligence adds another layer to these developments. Generative tools can assist with drafting persuasive messages in several languages, adapting social-engineering material and automating parts of an operation. Deepfake audio and video also create opportunities for impersonation. The economic significance lies partly in the time and skill required to perform these tasks: where automation works reliably, it may lower the marginal cost of repeating them. The extent of that advantage depends on the type of attack, however, and should not be assumed to be identical across all criminal activities.

This article examines the relationships connecting participants in the cybercrime value chain and asks why these arrangements can persist despite defensive and enforcement efforts. Transaction Cost Economics helps explain exchanges between unfamiliar actors; Platform Economy Theory sheds light on the role of marketplaces and network effects; and Value Chain Theory clarifies the separation of tasks. The discussion concentrates on access brokers, ransomware operations, darknet trading venues, cryptocurrency-related financial services and the use of AI in criminal workflows.

The analysis is based on published cybersecurity assessments, threat intelligence research, law-enforcement material and established economic literature. These sources do not provide a complete picture of hidden markets, and estimates of costs, proceeds and losses are not always directly comparable. Even with those limitations, they reveal organizational patterns that cannot be explained solely by software vulnerabilities. The central argument is that the structure of criminal markets matters: technical controls may stop particular attacks, while changes to incentives and intermediary services may affect the conditions under which new attacks are organized.

THE CYBERCRIME VALUE CHAIN

A defining feature of contemporary cybercrime is that its participants can divide an operation into separate, tradable tasks. The person who obtains access to a company network may never deploy the ransomware used against it, and the developer of that ransomware may have no direct contact with the victim. These relationships create a loose production network rather than a single, self-contained group. Specialization can improve the quality of particular services and allow operations to expand without every participant acquiring the same expertise. It can also make the wider market difficult to disrupt by targeting one actor.

Porter (1985) introduced the value-chain framework to describe how interconnected activities contribute to the production of economic value. Applied to cybercrime, the framework draws attention to the sequence of services needed to turn a technical opportunity into illicit proceeds. Infrastructure, unauthorized access, exploitation, monetization and movement of funds may be handled by different suppliers. This is not to suggest that criminal and lawful production are equivalent, but the comparison helps identify where participants specialize, exchange services and shift costs or risks onto others.

An operation commonly begins with tools and infrastructure. Developers and service providers may supply malicious software, phishing kits, credential-stealing programs, exploit tools or hosting arrangements that other actors subsequently use. Rather than selling every product outright, some suppliers rely on subscriptions or a share of the proceeds. Ransomware-as-a-Service (RaaS) illustrates the arrangement: one group maintains the software and supporting infrastructure, while affiliates select victims and conduct attacks. Payments are then divided according to the parties' agreement. Malware-as-a-Service (MaaS) follows a related logic. By separating development from deployment, these models allow participants with different skills and resources to cooperate without forming a conventional organization.

Unauthorized access to an organization's systems has itself become a product. Initial Access Brokers (IABs) focus on obtaining and selling that access rather than necessarily using it for extortion or fraud. Their customers may be other criminal actors seeking an entry point for a later operation. Listings can circulate through darknet marketplaces or encrypted channels, with the value of an offer shaped by the target and the privileges available. Access can originate in phishing, exploited VPN weaknesses, credential stuffing, malware infections, attempts against Remote Desktop Protocol

(RDP) services or assistance from insiders. The broker's role separates the acquisition of access from the decisions made after a compromise.

The existence of a market for initial access shows how even an early stage of an attack can be priced and traded. Threat intelligence reports describe offers ranging from several hundred dollars to tens of thousands, depending on the organization's characteristics and the level of control provided. These figures should be understood as reported market observations, not a uniform price schedule. A buyer who already has the required tools can purchase access instead of spending time obtaining it. Meanwhile, a seller can specialize in finding entry points without taking on every risk associated with the subsequent attack.

Remote access services are important in this market because organizations use them to support ordinary work. RDP and VPN connections became particularly significant as remote working arrangements expanded. Their usefulness also creates opportunities when credentials are stolen, authentication is weak or exposed services are inadequately secured. Criminal actors may search for reachable RDP systems and attempt to enter using compromised credentials or password-guessing techniques. A valid VPN account can likewise provide a route into an internal environment. In both cases, the economic value of access comes from the fact that it can be transferred to another participant for further exploitation.

Phishing and social engineering remain attractive methods of obtaining credentials because a single campaign can reach many potential victims. Messages may appear to come from banks, software vendors, IT staff or senior managers, and their purpose is to persuade recipients to disclose information or open harmful material. AI tools can make such messages easier to draft, translate and tailor to particular contexts. That capability may reduce preparation time and help attackers operate across languages. Whether it increases success rates in a given campaign is an empirical question, but it clearly changes the resources needed to produce plausible-looking fraudulent communications.

Once access has been obtained, the next participants may investigate the compromised environment, seek higher privileges, maintain their foothold, extract information or install ransomware. Extortion has also become more varied. In a so-called double-extortion incident, attackers combine encryption with threats to disclose stolen data. Triple-extortion schemes may add pressure on customers, partners or other parties connected to the victim. These tactics matter economically because they create several possible sources of leverage over the same organization, even when the technical stages of an attack are carried out by different people.

The monetization stage turns access, information or disruption into a possible source of income. Payments may come from ransomware demands, financial fraud, stolen assets or the resale of data. Underground markets list different kinds of information, including medical records, payment details, wallet credentials and complete identity profiles sometimes called 'fullz'. Their prices vary because not all stolen data are equally useful or easy to exploit. Factors such as freshness, completeness, scarcity and the effort required to use the information can affect what a buyer is willing to pay. A listing price, however, should not be confused with a completed sale or realized profit.

Darknet marketplaces provide a meeting point for suppliers and customers who might otherwise struggle to locate one another. They may host offers involving malicious software, compromised accounts, access services and ways to move illicit funds. Because the parties are often anonymous, uncertainty about delivery and payment is especially pronounced. Escrow, seller histories, reviews and dispute procedures attempt to address that uncertainty, although manipulation and outright fraud remain possible. The comparison with legitimate digital platforms is therefore organizational rather

than moral: both types of intermediary can lower search and coordination costs by bringing separate sides of a market together.

After obtaining proceeds, criminal actors may seek to move or convert them in ways that complicate investigation. Reported methods include cryptocurrency mixers, decentralized exchanges, peer-to-peer transfers and privacy-oriented assets such as Monero. Some services perform these functions for other participants and charge a fee. This creates another area of specialization within the wider market. It is important, however, not to treat every use of a privacy technology or decentralized financial service as criminal; the relevant issue here is the use of such arrangements to handle proceeds of illegal activity.

Seen as a whole, the value chain reveals a market held together by transactions between specialists. Developers, brokers, affiliates, marketplace operators and financial intermediaries can exchange services without taking responsibility for an entire operation. This arrangement resembles outsourcing in lawful industries, even though its purpose and consequences are fundamentally different. It helps explain how criminal activity can continue across borders and why the disruption of one supplier may leave other parts of the market functioning. The resulting damage can be substantial even when individual stages are comparatively inexpensive.

ECONOMICS OF CYBERCRIME

The economic importance of cybercrime has increased as firms, public institutions and households have become more dependent on connected technologies. Cloud services, remote access and digital payments support legitimate growth, but they also widen the range of systems that can be attacked or misused. Cybersecurity Ventures (2025) projects worldwide cybercrime damages exceeding USD 10.5 trillion per year. The estimate conveys the possible scale of the problem, although projected aggregate losses should not be read as a direct measure of money earned by criminals. Distinguishing these concepts is essential when examining incentives and profitability.

A useful starting point is the difference between the resources needed to attempt an attack and the losses a victim may suffer if it succeeds. Some forms of cybercrime can be repeated with relatively little additional expenditure once the tools and infrastructure are available. They can also be conducted across national borders without the same physical presence required in many traditional crimes. Yet low apparent entry costs do not mean every operation is profitable: unsuccessful attempts, purchased services, failed payments and enforcement risks also matter. The economic attraction lies in the possibility that a successful operation produces returns much larger than the initial outlay.

Ransomware operations illustrate how the organization of production affects costs. A developer may concentrate on maintaining software and infrastructure while affiliates carry out attacks against particular targets. Revenue-sharing agreements then allocate proceeds between those involved. The model resembles a franchise in its division of responsibilities, although relationships between participants may be unstable and subject to conflict. For a developer, recruiting affiliates can extend reach without managing each incident directly. For an affiliate, using an existing service may be less demanding than building the required tools independently. These incentives help explain the persistence of ransomware markets.

The gap between attack expenditure and victim damage is particularly visible when an incident interrupts business operations. A criminal actor might purchase credentials, a phishing kit or access to a network at a comparatively modest price. The affected organization, by contrast, may face downtime, investigation expenses, lost business, reputational harm and regulatory consequences, in

addition to any direct payment or theft. Those losses cannot automatically be counted as the attacker's revenue or return on investment (ROI). They do, however, show how a small expenditure on one side of a transaction can impose much larger costs on the other.

Figure 1 compares estimated attack costs with potential financial damage across several categories of cybercrime. It is intended to illustrate the scale of possible differences rather than to provide a direct calculation of criminal profits.



Figure 1. Relationship Between Average Attack Costs and Potential Financial Damage in Cybercrime Operations.

Source: *Developed by the author based on data from Cybersecurity Ventures (2025), IBM (2024), Coveware(2024), Microsoft (2024), and Chainalysis (2025).*

Figure 1 highlights the potential disparity between the resources associated with an attack and the damage that may follow. Phishing and credential theft appear at the lower-cost end of the comparison, while ransomware and supply-chain incidents may be associated with much larger losses. These categories are not directly interchangeable, and the plotted figures should not be interpreted as a consistent measure of expected returns. The comparison nevertheless helps explain the incentive problem: the expenditure required to initiate an incident may be small relative to the disruption imposed on an organization.

Markets for criminal services also change the economics of participation. A darknet platform can bring together people who sell access, software or other services and those who want to purchase them. Ratings, escrow, vendor verification and dispute procedures may reduce the time spent searching and negotiating, even where no legal contract can be enforced. This resembles the transaction-cost problem discussed by Coase (1937) and Williamson (1985). The platform does not eliminate uncertainty, but it can provide informal arrangements that make repeated exchanges possible between participants who would otherwise have difficulty trusting one another.

Network effects offer a further explanation for the attraction of established marketplaces. More buyers can encourage additional sellers to list specialized services; a broader range of sellers may, in turn, make the platform more useful to buyers. Access brokers, malware developers and financial

intermediaries may therefore concentrate where they expect to find demand. This feedback can support liquidity and specialization, although it also makes successful platforms visible to investigators and vulnerable to disruption. The market is thus shaped by competing pressures: the benefits of concentration and the risks that accompany it.

Artificial intelligence may influence this structure by changing how much time and expertise particular tasks require. Generative systems can help produce tailored phishing messages, translate fraudulent communications and imitate the style of trusted individuals. Synthetic voices and deepfake media create additional opportunities for deception in financial and social-engineering schemes. AI tools may also assist with coding or information gathering. These uses do not make sophisticated attacks effortless, but they can shift some work from specialist operators to widely available software, altering the division of labour within criminal markets.

From an economic perspective, the important question is whether these tools reduce the additional cost of repeating an operation. Where AI can reliably automate drafting, translation or routine preparation, the same actor may be able to produce more material in less time. Other stages still require judgment, access and technical knowledge. It is therefore more accurate to describe AI as a potential source of productivity gains than as a universal explanation for cybercrime growth. Its effect on participation and scale will depend on the tasks being automated and the defenses encountered.

The resilience of these markets creates difficulties for enforcement. Removing a prominent ransomware group or shutting down a marketplace can interrupt particular relationships and impose real costs on participants. Yet developers, affiliates and brokers may move to another venue or establish new identities when their tools and contacts remain available. The modular structure of the market makes substitution possible. This does not mean enforcement is ineffective; rather, it suggests that lasting disruption may require attention to the relationships and services that allow operations to be reassembled after an intervention.

Cybercrime is therefore sustained by more than the availability of vulnerable systems. Specialized suppliers, digital marketplaces, automation and ways to transfer proceeds affect the cost of participation and the likelihood that an operation can be organized. Their interaction can make criminal activity scalable even when particular actors disappear. An economic analysis complements technical cybersecurity by identifying the incentives and intermediary services behind attacks. Policies that change those incentives may be as important as measures that address individual vulnerabilities or incidents.

CONCLUSION

The evidence considered in this article points to a significant organizational change in cybercrime. Instead of relying exclusively on individuals who perform every task, many operations now draw on networks of specialized suppliers. Malware developers, Initial Access Brokers, ransomware affiliates, marketplace operators and financial intermediaries can contribute separate services to a common sequence of activities. This division of labour makes it easier to combine expertise and replace individual providers. It also means that understanding a single attack is not always enough to understand the market that made the attack possible.

The analysis also shows why concepts from platform economics are useful. Darknet marketplaces connect suppliers and buyers and may reduce search, bargaining and coordination costs through reviews, escrow and dispute procedures. Crime-as-a-Service models separate the production of tools from their use, enabling participants to purchase capabilities they do not possess themselves.

AI may extend this process by reducing the time needed for selected tasks. Together, these developments help explain the organizational flexibility of cybercrime without implying that every criminal operation follows the same model.

Enforcement faces the challenge of disrupting relationships rather than only individual offenders or pieces of infrastructure. When a platform closes, some participants may migrate; when a group is dismantled, affiliates may seek new partners. Such adaptation is possible because many services are transferable across organizations. This does not diminish the value of investigations, arrests or technical takedowns. It indicates that the broader effects of these actions should also be assessed in terms of market access, replacement costs and the ability of criminal participants to rebuild their networks.

Cybercrime should consequently be studied as both a security problem and an economic system. Technical vulnerabilities help explain how attacks occur, while specialization, transaction costs and incentives help explain why particular forms of criminal activity continue. A more effective response will combine defensive improvements with efforts to disrupt the services, financial channels and market arrangements that support repeated operations. Examining those underlying structures provides a clearer basis for evaluating which interventions are likely to produce lasting effects.

REFERENCES

Chainalysis, 2025. *The Chainalysis Crypto Crime Report*. Available at: https://www.chainalysis.com/ [Accessed 14 May 2026].

Coase, R.H., 1937. The nature of the firm. *Economica*, 4(16), pp. 386–405.

Coveware, 2024. *Quarterly Ransomware Reports*. Available at: https://www.coveware.com/blog [Accessed 12 May 2026].

CrowdStrike, 2025. *Global Threat Report 2025*. Available at: https://www.crowdstrike.com/global-threat-report/ [Accessed 14 May 2026].

Cyberint, 2025. *Initial Access Broker Report 2025*. Available at: https://e.cyberint.com/hubfs/IAB%20Report%202025.pdf [Accessed 15 May 2026].

Cybersecurity Ventures, 2025. *Official Cybercrime Report 2025*. Available at: https://cybersecurityventures.com/official-cybercrime-report-2025/ [Accessed 15 May 2026].

Europol, 2024. *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Available at: https://cybilportal.org/publications/internet-organised-crime-threat-assessment-iocta-2024/ [Accessed 15 May 2026].

Group-IB, 2025. *High-Tech Crime Trends 2025*. Available at: https://www.group-ib.com/landing/high-tech-crime-trends-2025/ [Accessed 14 May 2026].

IBM Security, 2024. *Cost of a Data Breach Report 2024*. Available at: https://www.ibm.com/reports/data-breach [Accessed 12 May 2026].

Microsoft, 2024. *Microsoft Digital Defense Report 2024*. Available at: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2024 [Accessed 12 May 2026].

Porter, M.E., 1985. *Competitive Advantage: Creating and Sustaining Superior Performance*. New York: Free Press.

Rochet, J.-C. and Tirole, J., 2003. Platform competition in two-sided markets. *Journal of the European Economic Association*, 1(4), pp. 990–1029.

Sophos, 2024. *The State of Ransomware 2024*. Available at: https://www.sophos.com/en-us/content/state-of-ransomware [Accessed 14 May 2026].

Williamson, O.E., 1985. *The Economic Institutions of Capitalism*. New York: Free Press.

Zscaler ThreatLabz, 2025. *AI phishing and cyber threat report*. Available at: https://www.zscaler.com/resources/security-terms-glossary/what-is-ai-phishing [Accessed 15 May 2026].

HUMAN FACTORS IN CYBERSECURITY: FROM HUMAN ERROR TO SOCIO-TECHNICAL RESILIENCE

CZU: 005.331:004.056
DOI: https://doi.org/10.53486/tids2026.33

EVELINA STEBNITSKAIA
Financial University under the Government of Russian Federation
e-mail: thestebev@gmail.com
ORCID ID: 0009-0006-5279-8255

DARIA KOZLOVA
Financial University under the Government of Russian Federation
e-mail: dasha280206k@gmail.com
ORCID ID: 0009-0009-6981-0259

DINARA R. ORLOVA
DSC, Professor, Department of Economics
Financial University under the Government of the Russian Federation
e-mail: DROrlova@fa.ru
ORCID ID: 0000-0002-2901-070X

Abstract. This paper examines human factors in cybersecurity as structural drivers of cyber risk rather than as residual deviations from otherwise secure technical systems. Although cybersecurity discourse still often describes users as the weakest link, contemporary research shows that breaches are more accurately produced through the interaction of cognitive limits, behavioural tendencies, interface design, organisational climate and adversarial manipulation of context. The paper aims to analyse the main cognitive, behavioural and organisational human factors that intensify cyber vulnerability and to formulate mitigation strategies that reduce risk without undermining legitimate work practices. Methodologically, the study adopts a critical integrative literature review that synthesises peer-reviewed research published between 2018 and 2025 together with foundational work in human error theory and behavioural decision-making. The analysis is organised around seven domains: human error, cognitive bias, phishing susceptibility, authentication behaviour, organisational security climate, training effectiveness and human-centred design. The review demonstrates that users do not fail simply because they are careless. Slips, lapses and mistakes are amplified by fatigue, divided attention, ambiguous interfaces, time pressure and contradictory productivity incentives. Phishing succeeds not only because messages are deceptive, but because recipients interpret cues through work context and fast, heuristic processing. Authentication failures likewise arise from the security-usability trade-off that encourages password reuse, approval fatigue and informal workarounds. At the organisational level, leadership visibility, procedural justice, policy congruence and peer norms improve voluntary compliance more reliably than fear-based messaging alone. The paper argues that resilient cybersecurity requires a shift from a blame-oriented paradigm to a socio-technical model that treats users as adaptive actors who must be supported by secure systems, credible governance and continuous learning. It concludes that the strongest approach combines human-risk assessment, phishing-resistant authentication, repeated context-aware training, forgiving interfaces, behavioural metrics and no-blame reporting.

Keywords: human factors in cybersecurity, socio-technical security, phishing susceptibility, security climate, authentication behaviour, human-centred design

JEL Classification: D91, M15, O33

INTRODUCTION

Cybersecurity breaches are often narrated as technical failures, yet the decisive moment in many incidents is behavioural rather than purely computational. A malicious email is opened, a credential is reused, an alert is dismissed, a policy is bypassed for the sake of continuity, or a manager delays remediation because the threat appears abstract. These episodes are not peripheral to cybersecurity; they are central to it. The latest Verizon DBIR executive summary still reports that the human element is implicated in roughly 60 per cent of analysed breaches, which confirms that cyber risk is generated at the intersection of human conduct, organisational incentives and technical architecture (Verizon, 2025).

The core problem addressed in this paper is the persistent gap between formal security policy and everyday user behaviour. Organisations publish password rules, mandate secure data handling, deploy multi-factor authentication and conduct awareness campaigns, yet employees still click on phishing links, share credentials, disable protections, or invent workarounds that restore convenience at the expense of resilience. This gap cannot be understood adequately through a purely technical lens because policy non-compliance is frequently rooted in overload, ambiguity, competing goals, weak security climate, or poor usability rather than deliberate negligence alone.

Recent literature illuminates different parts of this puzzle. Ncubukezit (2022) shows how recurrent human errors undermine small-business security. Barre et al. (2025) examine the role of cognitive biases in cyber-risk communication between boards and CISOs. Greene *et al.* (2018) demonstrate that phishing susceptibility is strongly shaped by work context rather than message content alone. Gwebu and Wang (2024) analyse the defining features of a robust information security climate. Aldawood and Skinner (2019) explain why many awareness programmes underperform, while Zimmermann *et al.* (2024) challenge the deeply rooted image of users as enemies rather than partners. Read together, these studies suggest a common theoretical proposition: cyber vulnerability is produced by socio-technical interaction, not by user defect in isolation.

Accordingly, the aim of this paper is to analyse how cognitive, behavioural and organisational human factors generate cybersecurity vulnerability and to propose academically grounded mitigations. The objectives are fourfold: to identify recurrent human vulnerabilities in contemporary cyber incidents; to evaluate the explanatory value of human error theory, bounded rationality and organisational climate perspectives; to assess the strengths and limits of training and authentication interventions; and to provide recommendations for human-centred cyber resilience. The originality of the paper lies in integrating these strands into a single analytical framework that treats human behaviour not as an afterthought to technical security, but as one of its governing conditions.

MAIN CONTENT

1. Materials and Methods

This study uses a critical integrative literature review as its principal method. Rather than merely listing prior findings, the review compares explanatory mechanisms across bodies of research and develops a conceptual synthesis. The core materials consist of peer-reviewed journal articles, conference papers, institutional publications and one carefully selected academic thesis published mainly between 2018 and 2025, supplemented by foundational works on human error and judgement under uncertainty.

The literature was selected according to thematic relevance to seven analytical domains: user error, cognitive bias, phishing and social engineering, authentication adoption, organisational security

climate, training effectiveness and human-centred security design. Analytically, the sources were organised into three interacting levels. The first level is cognitive and concerns attention, memory, heuristics and bias. The second is behavioural and concerns situated action, routine, impulsivity and compliance under workload. The third is organisational and concerns leadership, norms, incentives, procedural justice and the design of work systems. This multilevel perspective is necessary because the same failure event may be interpreted differently depending on the unit of analysis.

The method has two limitations that should be acknowledged. First, the study is a conceptual synthesis rather than a primary empirical investigation, so its contribution is interpretive and prescriptive rather than statistically causal. Secondly, the reviewed studies employ heterogeneous designs, including literature reviews, field experiments, organisational surveys, conference papers and conceptual articles, which means that direct comparison requires analytical judgement. Nevertheless, this diversity is also a strength, because human factors in cybersecurity are irreducibly interdisciplinary and cannot be captured through a single methodological lens.

2. Human Error as a Structural Cybersecurity Variable

Human error remains one of the most widely cited explanations for cyber incidents, but the concept is often used too loosely. In classical human factors research, error is not a homogeneous category. Reason (1990) distinguishes among slips, lapses and mistakes. Slips are failures of execution despite a correct intention; lapses are failures of memory or recall; and mistakes arise when the intention itself is flawed because the actor applies the wrong rule, mental model or judgement. This taxonomy is especially valuable for cybersecurity because it differentiates interface-induced action failures, memory burden and deeper failures of understanding.

Ncubukezit (2022) argues that recurrent human errors constitute a major cybersecurity concern for small businesses and identifies ignorance, poor decision-making, technical errors and skills- or policy-related failures as recurring sources of vulnerability. The broader implication is that error is rarely random. Users send information to the wrong recipient, misconfigure permissions, ignore software updates, or approve suspicious requests within environments defined by interruptions, multitasking, weak feedback and contradictory deadlines. Contemporary breach reporting supports this structural interpretation: even under a relatively strict coding framework, Verizon (2025) still attributes about 60 per cent of analysed breaches to the human element.

For this reason, the phrase weakest link is analytically insufficient. It individualises what is often a system output. Fatigue, alert saturation, divided attention and constant context switching make slips and lapses more probable, while poorly translated policies and weak workflow support make mistakes more likely. A rigorous approach to human error in cybersecurity therefore asks not only who erred, but what properties of the task, interface, workflow and governance made the error foreseeable.

3. Cognitive Biases, Heuristics and Risk Perception

Human behaviour in cybersecurity is shaped not only by error in the narrow sense, but also by ordinary patterns of judgement under uncertainty. Kahneman (2011) describes the fast, intuitive operations of System 1 and the slower, reflective operations of System 2. In routine organisational life, System 1 often dominates because people must act quickly, triage information and preserve cognitive resources. The consequence is not irrationality in an absolute sense, but bounded rationality: people make workable decisions under constraint, often at the cost of systematic bias.

In cybersecurity, optimism bias encourages the belief that one is less likely than others to become a victim. Confirmation bias leads users and managers alike to privilege cues that fit existing

expectations, such as assuming that a familiar-looking invoice or routine service notice is legitimate. Status quo bias encourages employees and executives to preserve insecure but familiar practices because change introduces friction, learning costs and uncertainty. Barre *et al.* (2025) show that such biases are especially consequential in cybersecurity governance, where boards and CISOs must interpret uncertain risk signals and communicate them across professional boundaries. Distorted risk perception at this level can lead to underinvestment, symbolic compliance and dangerous overconfidence.

The significance of cognitive bias lies in its cross-level character. The same mechanisms that help an employee process inbox traffic quickly can also cause a board to minimise abstract cyber exposure if no dramatic incident has recently occurred. Bias is therefore not a problem of end users only. It permeates the whole governance chain, from frontline message handling to strategic decision-making. Effective mitigation requires interventions that slow high-stakes decisions, improve the salience of risk-relevant cues and reduce the need for users to infer security significance from ambiguous signals.

4. Phishing as a Context-Sensitive Behavioural Attack

Phishing is frequently discussed as an issue of message deception, yet the evidence shows that it is more accurately understood as a context-sensitive behavioural attack. Greene *et al.* (2018), drawing on 4.5 years of embedded phishing exercises in a U.S. government research environment, found that user context was a significant explanatory variable in phishing susceptibility. Their key contribution is not simply that some users click more than others, but that clickers and non-clickers attend to different cues and interpret the same cues differently depending on how closely a message aligns with ongoing work tasks.

This finding has far-reaching implications. Urgency does not work in isolation; it works because it resonates with organisational expectations of responsiveness. Likewise, polished visual design, familiar senders, invoice language, delivery notifications and workflow plausibility all operate through situated interpretation. Phishing exploits normal organisational routines rather than isolated cognitive defects. Susceptibility therefore increases under time pressure, cognitive overload and cultures in which speed is rewarded more visibly than verification.

Simulated phishing campaigns remain useful, but only when they are treated as diagnostic instruments rather than tools of humiliation. Their principal value lies in identifying high-risk contexts, communication patterns and role-specific vulnerabilities. Used well, they reveal whether certain teams are structurally exposed because of job design, customer-facing responsibilities or dense transactional communication. Phishing defence should therefore move beyond the generic lesson to be careful and toward the redesign of cues, workflows and escalation paths so that suspicious requests become easier to pause, verify and report.

5. Authentication, Memory Burden and MFA Fatigue

Authentication is a classic site of tension between security and usability. Password systems rely heavily on human memory, yet strong password guidance typically demands length, uniqueness, complexity and regular management across many accounts. The predictable result is password reuse, insecure storage practices, low-quality coping strategies and eventual fatigue. In practice, users do not reject security because they oppose it in principle; they reject authentication regimes that impose excessive cognitive or temporal cost for uncertain benefit.

Karuppiah (2025) synthesises behavioural, usability and organisational factors influencing MFA adoption and shows that acceptance depends not only on security awareness, but also on

workflow disruption, recovery design, rigidity of enforcement and perceived fairness of rollout. Marky *et al.* (2022) likewise demonstrate that many users view two-factor authentication as necessary but annoying: they accept the protective rationale while simultaneously experiencing friction, interruption and resentment. This helps explain why approval fatigue, prompt habituation and informal bypass behaviour persist even after organisations deploy technically stronger controls.

The implication is not that authentication should be relaxed, but that it should be redesigned around human capability. Password managers reduce memory burden and password reuse. Biometrics and device-based authentication can improve convenience when implemented with careful privacy and recovery safeguards. Most importantly, phishing-resistant approaches such as syncable authenticators or passkeys can reduce dependence on manual code entry and shared secrets. NIST guidance explicitly recognises that properly configured syncable authenticators can support AAL2 while advancing broader adoption of phishing-resistant authentication (Galluzzo *et al.*, 2024). The strategic lesson is clear: the most resilient authentication systems are those that strengthen security by removing unnecessary human strain.

6. Organisational Security Climate and Voluntary Compliance

Cybersecurity behaviour is not produced by individual psychology alone; it is also shaped by the normative environment of the organisation. Gwebu and Wang (2024) define a robust information security climate as one in which security expectations are understandable, supported, enacted consistently and integrated into daily work. In such settings, employees perceive that secure behaviour is genuinely expected, practically enabled and fairly evaluated.

This perspective is important because procedural justice matters. Users are more likely to comply voluntarily when they believe policies are reasonable, leadership models the same standards and reporting channels are credible. Conversely, when management celebrates productivity while informally rewarding policy circumvention, staff learn that security is rhetorical rather than real. The organisational climate then teaches employees to treat policy as a symbolic layer to be worked around whenever deadlines, customer pressure or convenience demand it.

A strong security climate therefore depends on leadership visibility, policy congruence, peer norms and support resources. It is not enough to issue directives. Secure behaviour becomes stable only when the organisation reduces conflict between operational success and policy compliance. This is why mature security culture is less about slogans than about governance design: incentives, managerial conduct, reporting practices and everyday workflow must all signal that security is a shared institutional norm rather than a private burden placed on users.

7. Training Effectiveness Beyond Awareness Rituals

Security training is one of the most widespread responses to human cyber risk, yet its effectiveness is often overstated. Aldawood and Skinner (2019) show that many social engineering awareness programmes suffer from familiar weaknesses: limited budgets, weak tailoring, insufficient reinforcement and poor alignment with the changing tactics of attackers. One-time annual training may satisfy audit expectations, but it rarely produces durable behavioural change.

The problem is partly pedagogical and partly contextual. People forget abstract warnings when those warnings are detached from real tasks, real incentives and real moments of vulnerability. Repeated, interactive and role-specific interventions are more effective because they embed learning in practice rather than in symbolic compliance rituals. Training also works better when it is

immediately connected to suspicious events, simulated exercises or just-in-time warnings that appear inside the workflow where a risky decision is actually being made.

Training outcomes are further moderated by differences in digital literacy, professional role and prior experience. A homogeneous programme delivered to heterogeneous users will predictably underperform. This does not mean awareness initiatives are futile. It means they should be reframed as continuous learning systems that support recognition, reporting and recovery. The relevant metric is not whether employees attended a session, but whether they become more capable of noticing, pausing, escalating and learning from suspicious events over time.

8. Human-Centred Cybersecurity Design

Human-centred cybersecurity begins from the premise that people are not merely hazards to be constrained, but also partners whose capabilities can be cultivated. Zimmermann *et al.* (2024) argue that the traditional view of users as enemies has encouraged constraining approaches that limit action without adequately addressing the social and organisational conditions of secure behaviour. Their alternative is an enabling approach that treats humans as resources for resilience rather than residual sources of failure.

In design terms, this means reducing unnecessary friction, preserving user autonomy where possible and making security cues meaningful at the point of action. Warnings should communicate why a risk matters, not simply block action with generic alarm language. Interfaces should preserve evidence of origin, make verification easier than improvisation and support recovery when users make mistakes. Secure design is forgiving design: it assumes fallibility and builds in pathways for correction, escalation and learning.

This approach does not reject technical controls. It repositions them within a broader socio-technical strategy. Minimal-friction defaults, meaningful feedback, just-in-time prompts, safer recovery flows and behavioural nudges can all improve outcomes without treating the user as a problem to be neutralised. The deeper contribution of human-centred design is normative: it shifts cybersecurity from a logic of suspicion toward a logic of support.

9. Recommendations for Practice and Research

The synthesis developed in this paper supports five strategic recommendations. First, organisations should conduct human-risk assessments that examine roles, workflows and interfaces rather than relying solely on compliance checklists. The central question should be where security depends on hurried interpretation, memory load or ambiguous signals, because these are precisely the points at which slips, lapses and bias become likely. Secondly, organisations should redesign high-risk interfaces according to forgiving and human-centred principles. Security controls should communicate clearly, preserve provenance information and reduce unnecessary dependence on recall and manual verification.

Thirdly, authentication should migrate toward low-memory and phishing-resistant solutions, including password managers, well-designed MFA, resilient recovery flows and passkey-based approaches where appropriate. Fourthly, training should become continuous, role-sensitive and behaviourally measured. The goal is not symbolic awareness, but demonstrable improvement in detection, reporting and recovery. Fifthly, organisations should institutionalise no-blame reporting for near misses, suspicious events and honest mistakes. Harper (2023) is especially useful here in linking human-based cyber behaviour to practical mitigation: learning is suppressed when users

expect ridicule or punishment, yet early reporting is exactly what allows small failures to be contained before they become major incidents.

For researchers, the field now needs more longitudinal and interdisciplinary work. Future studies should compare how cognitive bias, interface design and security climate interact over time, test whether behavioural metrics can be collected ethically and validly, and examine how artificial intelligence changes both attack persuasion and defensive support. The most promising agenda is one that moves beyond the binary opposition between user failure and technical control and instead studies cybersecurity as a dynamic ecology of perception, workload, authority, design and adaptation.

CONCLUSIONS

This paper has argued that human factors in cybersecurity should be understood as a central domain of analysis rather than as a residual explanation for failures that technology did not prevent. Human error, cognitive bias, phishing susceptibility, authentication fatigue, organisational climate and training effectiveness are not separate problems; they are interconnected expressions of how people act in complex digital environments under constraint. The common lesson across the literature is that insecure behaviour is frequently predictable and often induced by the structure of work itself.

The significance and originality of the paper lie in bringing together human error theory, behavioural decision theory and organisational climate research into a unified account of cyber resilience. This synthesis helps explain why technical controls underperform when they are layered onto cognitively overloaded users and weak organisational systems. It also supports a more mature normative position: resilient cybersecurity does not arise from demanding flawless behaviour, but from designing institutions and interfaces that make secure action credible, legible and sustainable.

The paper has several limitations. It is based on conceptual synthesis rather than primary data collection, and some reviewed studies are context-specific, especially those focused on particular organisations or sectors. Future research should therefore test the proposed framework through cross-sector longitudinal studies, experimental work on warning design and organisational field studies on security climate, reporting culture and authentication behaviour. Even so, the current evidence is sufficient to reject simplistic blame narratives. In cybersecurity, the human factor is not merely the weakest link; properly understood and properly supported, it is also one of the strongest levers for resilience.

REFERENCES

Aldawood, H. and Skinner, G. (2019) ‘Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues’, *Future Internet*, 11(3), p. 73.

Barre, G., Huygh, T., Nguyen, D.K. and Nuijten, A. (2025) ‘Towards understanding cognitive biases in cybersecurity governance’, in Pucihar, A., Kljajić Borštnar, M., Blatnik, S., Marolt, M., Bons, R.W.H., Smit, K. and Glowatz, M. (eds.) *38th Bled eConference: Empowering Transformation: Shaping Digital Futures for All: Conference Proceedings*. Maribor: University of Maribor Press, pp. 737–744.

Galluzzo, R., Regenscheid, A., Temoshok, D. and LaSalle, C. (2024) *Incorporating Syncable Authenticators Into NIST SP 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management*. Gaithersburg, MD: National Institute of Standards and Technology.

Greene, K.K., Steves, M.P., Theofanos, M. and Kostick, J.A. (2018) ‘User context: an explanatory variable in phishing susceptibility’, in *Proceedings of the Network and Distributed System Security Symposium, Workshop on Usable Security*. San Diego, CA, 18 February 2018. Reston.

Gwebu, K.L. and Wang, J. (2024) 'The defining features of a robust information security climate', *Computers & Security*, 142, 103891.

Harper, J.W. (2023) 'Cybersecurity: a review of human-based behavior and best practices to mitigate risk', *Issues in Information Systems*, 24(4), pp. 247–254.

Kahneman, D. (2011) *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

Karuppiah, S.P. (2025) *Understanding the behaviour of business users in multi-factor authentication adoption*. Master's thesis. Lappeenranta–Lahti University of Technology LUT.

Marky, K., Ragozin, K., Chernyshov, G., Matviienko, A., Schmitz, M., Mühlhäuser, M., Eghtebas, C. and Kunze, K. (2022) 'Nah, it's just annoying!' A deep dive into user perceptions of two-factor authentication, *ACM Transactions on Computer-Human Interaction*, 29(5), pp. 1–32.

Ncubukezit, T. (2022) 'Human errors: a cybersecurity concern and the weakest link to small businesses', *International Conference on Cyber Warfare and Security*, 17(1), pp. 395–403.

Reason, J. (1990) *Human Error*. Cambridge: Cambridge University Press.

Verizon (2025) *2025 Data Breach Investigations Report: Executive Summary*.

Zimmermann, V., Schöni, L., Schaltegger, T., Ambuehl, B., Knieps, M. and Ebert, N. (2024) 'Human-centered cybersecurity revisited: from enemies to partners', *Communications of the ACM*, 67(11), pp. 72–81.

CYBERSECURITY MANAGEMENT MODELS IN HIGHER EDUCATION INSTITUTIONS ACCORDING TO NIS2 REQUIREMENTS

CZU: 378:[005:004.056]
DOI: https://doi.org/10.53486/tids2026.34

KRASIMIR SHISHMANOV
D. A. Tsenov Academy of Economics, Bulgaria
e-mail: k.shishmanov@uni-svishtov.bg
ORCID ID: 0000-0001-9874-2149

YURIY KUZNETSOV
D. A. Tsenov Academy of Economics, Bulgaria
e-mail: y.kuznetsov@uni-svishtov.bg
ORCID ID: 0009-0009-3569-7614

ISKREN TAIROV
D. A. Tsenov Academy of Economics, Bulgaria
e-mail: i.tairov@uni-svishtov.bg
ORCID ID: 0000-0002-2971-5451

Abstract. Higher education institutions (HEIs) are increasingly exposed to cybersecurity threats due to the growing reliance on digital platforms, cloud services, and the handling of sensitive research and personal data. The EU NIS2 Directive establishes a regulatory framework that strengthens cybersecurity obligations, including risk management, incident reporting, policy implementation, and staff awareness. This paper explores internationally recognized cybersecurity management models – ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, and maturity models – and examines their application in higher education settings. A comparative mapping illustrates how these models help HEIs achieve compliance with NIS2 requirements while enhancing their overall cybersecurity posture. The paper also discusses specific challenges, such as limited budgets, technical expertise, and cultural barriers, and provides practical recommendations for gradual and sustainable adoption of cybersecurity practices in universities.

Keywords: cybersecurity, higher education, NIS2, models.

JEL Classification: L86

INTRODUCTION

In the digital era, higher education institutions (HEIs) face increasing cybersecurity threats due to the vast amount of sensitive data they process, including research findings, student records, and intellectual property (Salam *et al.*, 2026). The adoption of robust cybersecurity management models is therefore critical to protect institutional assets and ensure operational continuity. The EU Directive on Security of Network and Information Systems (NIS2) provides a regulatory framework that aims to enhance cybersecurity resilience across member states, including obligations for higher education institutions (European Commission, 2022). This research examines cybersecurity management models applicable to HEIs and evaluates their alignment with NIS2 requirements.

1. Materials and Methods

1.1. Materials

The study focuses on the following materials:

- **NIS2 Directive** – official EU regulatory text and ENISA guidance (European Commission, 2022).
- **Cybersecurity Management Models**:
  - ISO/IEC 27001: Information Security Management System (Calder, 2008)
  - NIST Cybersecurity Framework (NIST, 2018)
  - COBIT 2019 (ISACA, 2021)
  - Cybersecurity Maturity Models (Bada *et al.*, 2019)

These frameworks were selected due to their wide adoption in organizational cybersecurity and compatibility with NIS2 requirements.

1.2 Methods

- A comparative literature review was conducted to analyze how each model addresses NIS2 requirements.
- Mapping of NIS2 obligations to cybersecurity management models was performed, identifying practical strategies for implementation in HEIs.
- Analysis of challenges and recommendations for adoption was derived from case studies and peer-reviewed publications in the field of cybersecurity in higher education (Afolalu and Tsoeu, 2025).

2. Results and Discussion

2.1. Overview of NIS2 Directive

NIS2 is a legislative update to the original NIS Directive, expanding its scope and strengthening security obligations for organizations considered essential or important for societal functions, including universities (European Commission, 2022). Key requirements include:

1. **Risk assessment and management** – Organizations must identify and manage risks to network and information systems.
2. **Incident reporting** – Significant cybersecurity incidents must be reported promptly, typically within 24 hours.
3. **Implementation of security policies** – Organizations must develop internal security policies and incident response plans.
4. **Training and awareness** – Staff must be regularly trained to recognize and respond to cybersecurity threats.

NIS2 emphasizes not only technical measures but also organizational and governance aspects, aligning with global standards for information security.

2.2. Cybersecurity Management Models

Several internationally recognized models can guide HEIs in implementing NIS2-compliant cybersecurity programs:

2.2.1 ISO/IEC 27001

ISO/IEC 27001 defines requirements for an Information Security Management System (ISMS), focusing on continuous risk assessment and mitigation (Kitsios, 2023). It provides a structured approach to information security governance and is widely adopted in educational institutions (Calder, 2008).

2.2.2 NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF), developed in 2014 by the U.S. National Institute of Standards and Technology is based on five functions: Identify, Protect, Detect, Respond, and

Recover (NIST, 2018). Its flexibility makes it suitable for universities with diverse IT infrastructures, integrating technical and administrative controls to manage cyber risks effectively (Riega *et al.,* 2025).

2.2.3 COBIT

COBIT(Control Objectives for Information Technologies) offers a governance and management framework for IT, ensuring alignment with organizational goals and regulatory requirements (ISACA, 2021). Its focus on performance measurement and control is particularly useful for HEIs needing to demonstrate compliance with NIS2.

2.2.4 Maturity Models

Maturity models assess the current state of cybersecurity capabilities and guide incremental improvements. Universities can use these models to benchmark their security posture and align with NIS2's risk-based approach (Papachristofis *et al.,* 2025).

2.3. Application in Higher Education Institutions

Universities face unique cybersecurity challenges, including open network environments, remote learning platforms, and sensitive research data. Applying the aforementioned models helps address these risks:

- **Centralized Security Operations Center (SOC)** – Monitoring and response to cyber incidents in real-time.
- **Regular audits and penetration testing** – Ensuring vulnerabilities are identified and remediated.
- **Policy development and training** – Formal policies and continuous awareness programs for staff and students.

Integration with NIS2 ensures that these practices are not only effective but also compliant, with documented risk assessments, incident response procedures, and reporting mechanisms (Mentzelou *et al.,* 2025).

To provide a clear overview of how higher education institutions can implement NIS2 requirements using various cybersecurity management models, Table 1 maps the main NIS2 obligations to ISO/IEC 27001, NIST CSF, COBIT, and maturity models. This mapping illustrates practical approaches for universities to ensure compliance and strengthen their cybersecurity posture.

Table 1: Mapping NIS2 Requirements to Cybersecurity Management Models in Higher Education Institutions

NIS2 Requirement	ISO/IEC 27001	NIST Cybersecurity Framework	COBIT	Maturity Models	Example Implementation in Universities
Risk Assessment & Management	Risk assessment procedures, controls selection	Identify function: Asset management, risk analysis	Risk management and governance objectives	Evaluate current cybersecurity maturity and gaps	Conduct annual risk assessment of IT systems and research databases
Incident Reporting	Incident management and corrective actions	Respond function: Incident response plans	Monitor and report incidents to management	Track incident response capability in maturity assessment	Establish SOC and formal reporting channels within 24 hours

NIS2 Requirement	ISO/IEC 27001	NIST Cybersecurity Framework	COBIT	Maturity Models	Example Implementation in Universities
Security Policies & Procedures	Information security policies, documentation	Protect function: Access control, awareness training	Define and enforce IT governance policies	Policy maturity evaluation	Develop policies for data protection, cloud use, and remote access
Training & Awareness	Staff awareness programs	Protect & Detect: Awareness, monitoring	Performance metrics for staff compliance	Assess staff training effectiveness	Regular cybersecurity workshops for faculty and students
Continuous Improvement	Internal audits, management reviews	Recover function: Lessons learned, improvements	Measure performance and controls effectiveness	Stage-wise maturity improvement plan	Quarterly review of security controls, update based on audit findings

2.4. Challenges and Recommendations

Higher education institutions face several unique challenges when implementing cybersecurity measures in accordance with NIS2v (Zaid, 2024). One of the primary obstacles is budgetary constraints. Universities often operate with limited financial resources, which can restrict their ability to invest in advanced security technologies, hire specialized cybersecurity personnel, or maintain continuous monitoring systems. This financial limitation makes it difficult to implement comprehensive solutions across all departments and services, potentially leaving some assets more vulnerable than others (Ghulam, 2025).

Another significant challenge is the limited technical expertise among academic and administrative staff. While IT departments may possess skilled personnel, faculty and researchers often lack the knowledge required to identify and respond to emerging cyber threats. This gap can result in unintentional exposure of sensitive data, improper configuration of systems, or delayed reporting of incidents, which are critical under NIS2 requirements (Torgersen *et al.,* 2025).

Additionally, there is a cultural resistance to stringent security policies within academic environments. Universities traditionally promote openness, collaboration, and the free exchange of knowledge, which can conflict with strict access controls, data classification, and compliance procedures (Ulven and Wangen, 2021). Introducing security measures may be perceived as cumbersome or restrictive, leading to inconsistent adoption across departments.

To address these challenges, a gradual and strategic approach is recommended. Universities should prioritize the implementation of Information Security Management Systems (ISMS) and other cybersecurity frameworks in critical areas first, such as research databases, student information systems, and administrative networks. This allows institutions to allocate limited resources effectively while building internal expertise over time.

Investment in continuous training and awareness programs is essential to equip both technical staff and faculty with the knowledge to identify threats, follow best practices, and respond appropriately to incidents. Workshops, online modules, and simulated cyber exercises can help foster a culture of security awareness without compromising the collaborative nature of academic work (Marhad *et al.,* 2024).

Finally, collaboration and knowledge sharing – both internally across departments and externally with other universities or national agencies – can strengthen cybersecurity resilience. By sharing best practices, threat intelligence, and incident experiences, institutions can improve their response capabilities and reduce the learning curve associated with new regulations like NIS2. This cooperative approach ensures that universities not only comply with regulatory requirements but also cultivate a proactive, sustainable cybersecurity posture (ENISA, 2022).

CONCLUSIONS

Higher education institutions are increasingly exposed to complex and evolving cyber threats due to the growing digitalization of academic processes, cloud-based platforms, and the handling of highly sensitive research and personal data. The NIS2 Directive provides a structured legal and regulatory framework, setting clear requirements for risk management, incident reporting, the implementation of security policies, and staff training. Compliance with NIS2 is not only a legal obligation but also a strategic necessity to maintain trust, protect institutional reputation, and ensure uninterrupted academic and research activities (European Commission, 2022).

Implementing internationally recognized cybersecurity management models, such as ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, and maturity models, offers universities practical tools to systematically assess risks, monitor security controls, and continuously improve their cybersecurity posture. These frameworks facilitate alignment with NIS2 requirements, allowing universities to document policies, respond effectively to incidents, and measure progress over time (Calder, 2008).

Moreover, adopting a holistic approach that integrates technical solutions, governance structures, and cultural awareness within the academic community is crucial. This ensures that security measures are not seen merely as regulatory compliance tasks but as essential elements that support innovation, collaboration, and the protection of intellectual and personal assets. By gradually embedding these models into daily operations, universities can overcome challenges related to budget limitations, skill gaps, and cultural resistance, ultimately fostering a resilient cybersecurity environment.

In conclusion, the combination of NIS2 requirements and well-established cybersecurity management models provides higher education institutions with a comprehensive roadmap for strengthening their security capabilities. Beyond compliance, this approach promotes a proactive, adaptive, and sustainable cybersecurity culture, ensuring that universities remain safe, trusted, and capable of fulfilling their academic and research missions in an increasingly interconnected digital landscape.

REFERENCES

Afolalu, O., and Tsoeu, M. S., 2025. Cybersecurity in Higher Education Institutions: A Systematic Review of Emerging Trends, Challenges and Solutions. *Future Internet*, 17(12).

Bada, A., Sasse, M. A., and Nurse, J. R. C, 2019. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?., pp. 118-131

Calder, A., 2008. ISO27001 / ISO27002 - A Pocket Guide:IT Governance Publishing.

ENISA, 2022. Cybersecurity Education Initiatives in the EU Member States. Available at: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states [Accessed 25 04 2026].

European Commission, (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555 [Accessed 20 04 2026].

Ghulam, A., 2025. Cybersecurity Governance and Policy Development in Higher Education Institutions: A Strategic Framework for Resilience and Compliance.

ISACA, 2021. COBIT 2019 Framework: Governance & Management Objectives. Available at: https://www.isaca.org/resources/cobit [Accessed 27 04 2026].

Kitsios, F., Chatzidimitriou, E., and Kamariotou, M, 2023. The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability*, 15(7).

Marhad, S., Goni, S. and Sani, M., 2024. mplementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review. *Environment-Behaviour Proceedings Journal*, (9), pp. 197-203.

Mentzelou, K., Chountalas, P. T., Kitsios, F. C., Magoutas, A. I., and Dasaklis, T. K., 2025. Identifying and Modeling Barriers to Compliance with the NIS2 Directive: A DEMATEL Approach. *Journal of Cybersecurity and Privacy*, 5(4). NIST, 2018. Cybersecurity Framework. Available at: https://www.nist.gov/cyberframework/csf-11-archive [Accessed 02 05 2026].

Papachristofis, K., Vardoulias, G., and Vavousis, K., 2025. Developing cyber-resistivity maturity and scoring framework (CRMSF) for any size of organization. *International Journal of Information Security*, 24.

Riega, J., Riega, Y., Soto, M., and Salas-Riega, J., 2025. Cybersecurity and the NIST Framework: A Systematic Review of its Implementation and Effectiveness Against Cyber Threats. *International Journal of Advanced Computer Science and Applications*, 16(6).

Salam, M., Bakar, K., Ghani, A., and Aman, A., 2026. Cybersecurity in Higher Education Institutions Digitalisation: Addressing Threats and Vulnerabilities. *Sage Open*, 16(1).

Torgersen, L., Noble, E., Ask, T., and Knox, B., 2025. Strengths and Knowledge Gaps Identified From Cybersecurity Education and Training Programs, and the Implications for Operational Technology Personnel in Critical Infrastructures: A Scoping Review. *IEEE Access*.

Ulven, J. B., and Wangen, G., 2021. Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, 13(2).

Zaid, M., 2024. Cybersecurity Education in Higher Institutions: Addressing Challenges and Fostering Awareness

METAMORPHOSES OF THE SHADOW DIGITAL ECONOMY

CZU: 343.9:004.056
DOI: https://doi.org/10.53486/tids2026.35

SERGHEI OHRIMENCO
Academia of Economic Studies of Moldova
e-mail: osa@ase.md
ORCID ID: 0000-0002-6734-4321

DINARA ORLOVA
Financial University under the Government of the Russian Federation
e-mail: DOrlova@fa.ru
ORCID ID: 0000-0002-2901-070X

GHENADIE BELINSCHI
Academia of Economic Studies of Moldova
e-mail: gennadie.belinschi@ase.md
ORCID ID: 0009-0009-3361-9890

Abstract. This research analyses the shadow digital economy (SDE) as an ecosystem for the development of cybercrime. The SDE is viewed not as a collection of isolated illegal incidents, but as a digital shadow market environment in which illicit products, services, infrastructure and coordination mechanisms are organized in a quasi-market form. The term 'Metacrime' is used to denote the supra-systemic level of such an environment, understood as the service-market-based and reproducible criminal core of the SDE. The following are systematically explored: a research gap in the literature; the conceptual and methodological foundations of the study; umbrella models and the multi-level architecture of Metacrime; rent-seeking mechanisms and investment-reinvestment cycles; as well as the transformation of the classical SDE in immersive and virtual-active environments. Attention is also paid to the interpretation of Metacrime as crime in the Metaverse – a new segment of the SDE.

Keywords: Shadow Digital Economy, Cybersecurity, Metacrime, Metaverse

JEL Classification: D47, D74, D82, E26, K24, O17

INTRODUCTION

It should be noted that the digitalization of the global economy is having a direct impact on the development of platform markets, the proliferation of cloud services, artificial intelligence, blockchain solutions, digital twins, XR/AR/VR and next-generation communication networks. All of the above has led to the creation of a qualitatively new techno-economic environment, within which not only knowledge but also labor itself, identity, property, governance, payments, access to services and infrastructure, and much more are being transformed into digital form.

This environment is not limited to e-commerce or online communication in the traditional sense. It brings together hybrid industrial, medical, educational and social cyberspaces, where physical and virtual realms increasingly interact through digital twins, immersive technologies and interfaces, distributed data and platform coordination.

On the one hand, the growth and expansion of the legal digital economy also give rise to its shadow side. On the other hand, it is precisely where digital value is concentrated that forms of its covert appropriation, redistribution, blocking, imitation and monetization emerge. This is precisely why cybercrime, as a phenomenon and a product of the digital economy in the modern context, cannot

be adequately described and represented solely as a collection of cyberattacks, cyber incidents or computer offences. This phenomenon is increasingly taking on the characteristics of a service economy, in which complex unlawful activities are broken down into separate functions, packaged as products and services, supported by infrastructure, promoted through platforms, facilitated by intermediation and trust mechanisms, and then monetized and reinvested. Moreover, this phenomenon is successfully described by a set of simulation models, which will be discussed later.

I. ANALYSIS OF THE NEW ENVIRONMENT

The shadow digital economy is like an iceberg: only the tip is visible above the water, gleaming in plain sight. We have no idea what wave of technological processes is surging beneath the surface, how many people are working to sustain this hidden system, what management models are being devised to achieve its goals, or what abyss of human drama remains concealed beyond the boundaries of the conventional economy.

To analyses this environment, the concept of the shadow digital economy is used as an indirect shadow market environment in which illegal products, services, infrastructures and coordination mechanisms are organized in a quasi-market form. The supra-systemic level of this environment is designated as Metacrime — the criminal core of the SDE, in which disparate unlawful practices coalesce into a stable architecture of services, roles, markets, rent-seeking positions and investment-reinvestment cycles. In contrast to the narrow interpretation of Metacrime as crime in the Metaverse, as proposed in some contemporary literature, this article offers a broader political-economic interpretation of the concept.

The aim of this article is to develop and propose a comprehensive analytical model of the shadow digital economy (SDE) as an ecosystem for the development of cybercrime, and to demonstrate how it reproduces itself through service models, the life cycle of destructive digital value, rent-seeking mechanisms, and transformation in immersive and virtual-active environments. To achieve this objective, the following tasks have been set and are being addressed:

- to identify and define a research gap in the literature;
- to establish the conceptual and methodological foundations for the analysis of the SDE;
- to propose an aggregated architecture of Metacrime umbrella models;
- to describe the operational logic of the SDE by mapping out all stages of the product and service lifecycle;
- to reveal the rent-seeking nature and investment-reinvestment cycles of Metacrime;
- to demonstrate how the classical TCE model transforms into the Metaverse, the industrial Metaverse and other immersive environments.

II. LITERATURE REVIEW

This study employs a systematic review of scholarly and practitioner literature and reports from research organizations specializing in cybersecurity and its economic aspects. We use these sources to synthesize existing knowledge and identify emerging trends related to the shadow digital economy. The study included a review of scientific databases, including Google Scholar, IEEE, and Scopus. Keywords for identifying sources included terms such as Cybersecurity, Shadow Digital Economic, Cybercrime, Dark Markets, Metacrime, Metaverse and other.

The current literature on this subject can be divided into several groups, each of which covers only part of the subject area in question.

The first group consists of works directly devoted to Metacrime. There are not many of them as yet, which in itself indicates that the topic has not been explored in depth. Most notably, almost all of these publications consider Metacrime in a narrow sense — as crime in the Metaverse, in immersive environments and surrounding virtual assets, avatars, digital identity, virtual property and issues of legal regulation. Authors (Zhou, 2024) and (Tiwari, 2025) examine this topic in detail and link the emergence of the Metaverse to the rise of 'Metacrimes'—a new category of criminal activity taking place in the Metaverse, which poses a challenge not only to traditional cybercrime but also to existing law enforcement structures. Five general characteristics of these crimes are identified: classification of crimes, continuous evolution, hyperspatial-temporal scope (global scale), anonymity and governance issues. The second paper describes a mechanism whereby the Metaverse provides extensive and unique opportunities for committing crimes, or 'Metacrimes', which challenge existing law enforcement efforts and regulatory frameworks. Three main challenges in combating Metacrimes are identified: the lack of specialized jurisdictions, the absence of clear property rights, and difficulties regarding the liability of avatars.

Another piece of work that calls for greater attention to Metacrime is the article Andreas Karapatakis «Metaverse crimes in virtual (Un)reality: Fraud and sexual offences under English law» (Karapatakis, 2025), which states that the Metaverse is a virtual environment that uses technology to simulate the real world. The author examines issues related to criminal activity in the Metaverse. Given the potential applications of AI, cryptocurrencies and non-fungible tokens, he identifies three main problems: 1) decentralization, 2) user anonymity and 3) lack of regulation.

It is also worth highlighting the work G.M.Bovenzi (Bovenzi, 2023), which states that, as regards the topic of Metacrime, the precise boundaries have not yet been defined and there is no criminal liability for acts committed in the Metaverse.

It is worth noting this seminal work Eldar Haber "The Criminal Metaverse" (Haber, 2024), which demonstrates that virtual worlds are not mere fantasy; they open up new possibilities whilst simultaneously raising fears regarding criminal activity (financial and property crimes, crimes against the person, etc.). The author points out that immersive technologies may undermine criminal law, as they could lead to atypical crimes not described in the criminal code or in legal literature. In describing the taxonomy of crimes in the Metaverse, the author focuses on a fundamental conceptual question: is criminal law necessary to maintain order in a virtual society? His taxonomy relates both to behavior within the Metaverse and to explicit violations. In conclusion, the author puts forward the thesis that the Metaverse is unlikely to be free from crime. There should be no doubt that regulating the Metaverse, let alone its criminal aspects, will be no easy task. It will take time and effort before platforms, users and the state fully grasp the implications of using such technologies and their impact on our daily lives.

Another significant piece of work is an article by a group of authors «A scoping study of crime facilitated by the Metaverse» (Gómez-Quintero, 2024). The authors note that the Metaverse represents an emerging convergence of technologies and, unfortunately, the implications of these new technologies for crime and security are often overlooked. The authors anticipate the types of crime that the Metaverse may facilitate and present the results of a study conducted using the nominal group technique (NGT). Their findings provide a better understanding of the most dangerous and likely criminal threats that the Metaverse may give rise to and, consequently, help stakeholders priorities the crimes on which they should focus.

The second group comprises works that explore issues relating to cybercrime and digital forensics. These include works such as (Steinmetz, 2023), Author advances a theoretically informed realist criminology of computer crime. In other book (Baker, 2020), presents new research in artificial intelligence (AI) and law, with special reference to criminal justice. Next book "Cybercrime: An encyclopedia of digital crime" (Marion, 2020), is an encyclopedia that systematically examines Ransomware, Phishing, Identity Theft, Viruses, DDoS Attacks, Malware, Cyberterrorism, Hacking and etc. Pall Watters in the book "Cybercrime and cybersecurity" (Watters, 2023). indicates: "The field of cybersecurity and cybercrime is a critical and rapidly evolving area of study. As our society becomes more and more reliant on technology, the risks of cybercrime increase. This book provides a comprehensive introduction to the field, covering both cybercrime and cybersecurity."

A wonderful textbook has been prepared Alex Alexandrou "Cybercrime and Information Technology Theory and Practice: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices" (Alexandrou, 2021). It states many books cover investigations, forensic recovery, and presentation of evidence, and others explain computer and network security, this book explores both, explaining the essential principles governing computers, wireless and mobile devices, the Internet of Things, cloud systems, and their significant vulnerabilities. This book deserves special attention Pierre Skorich and Matthew Manning "Insider Threat: A Systemic Approach" (Skorich, 2024), in which the authors establishing a new framework for understanding insider risk by focusing on systems of organization within large enterprises, including public, private, and not-for-profit sectors, this book analyses practices to better assess, prevent, detect, and respond to insider risk and protect assets and public good. Researchers are particularly interested in Nir Kshetri's book on the global cybercrime industry (Kshetri, 2010). Specifically, he points out «The cybercrime industry is a comparatively young area of inquiry. While there has been an agreement that the global cybercrime industry is tremendously huge, little is known about its exact size and structure. Very few published studies have examined economic and institutional factors that influence strategies and behaviors of various actors associated with the cybercrime industry. Theorists are also debating as to the best way to comprehend the actions of cyber criminals and hackers and the symbiotic relationships they have with various players».

The third group relates to literature on the shadow economy and its digital representation Works F. Schneider (Schneider, 2013) subsequent studies show that the shadow economy has a solid institutional foundation, whereas research by a group of authors (Ohrimenco, 2026), (Ohrimenco, 2023) allows us to directly refer to the SDE as a specific form of a digitally mediated shadow market embedded in information ecosystems.

The fourth group includes research on the metaverse, digital twins, blockchain, Web3, Industry 4.0/5.0, and the industrial metaverse. These sources are important because they demonstrate the emergence of new objects of digital value—virtual property, NFTs, digital real estate, self-identity authentication, digital twins, tokenized assets, and new platform-based frameworks for ownership and exchange. However, even within this group, the technological, legal, or industry-specific perspective predominates.

III. KEY BUSINESS MODELS AND ARCHITECTURE

The most common mistake in describing cybercrime is when researchers either focus solely on specific cyberattack techniques or reduce the topic to a mere list of X-*as-a-Service* models. However, the service format alone does not constitute a complete business model. Within the digital crime ecosystem, it is necessary to distinguish between:

- forms of packaging the function (e.g., *as-a-Service*);
- mechanisms for its operational implementation;
- the business models themselves, as sustainable schemes for the production, coordination, and extraction of destructive digital value.

At the *micro level*, Metacrime can be represented by individual tools, access points, a set of malicious functions, service units, infrastructure modules, and individual exchange entities. This is where the primary "commodity form" of illicit activity emerges: access, a malicious module, a bypass scheme, a concealment service, a distribution channel, a digital identity, an asset, or a data fragment.

At the *meso-level*, which is structurally dominant, the division of labor and the organization of collaboration occur simultaneously. It is here that access providers, developers, operators, intermediaries, call centers, consultants, infrastructure providers, trust actors, and financial executors transform individual functions into a coordinated service economy. In this environment, tasks are broken down and passed between specialized participants, while the platform or marketplace serves as the assembly point for the operation.

At the *macro level*, stability mechanisms are taking shape: trust, arbitration, quasi-market rules, reputation standards, platform governance, principles of inclusion and exclusion, and, in the long term, unique forms of digital governance. It is precisely here that Metacrime ceases to be a strictly organizational and technical environment and begins to manifest itself as an institutionally rich system.

IV. RESULTS AND DISCUSSION

Based on the results of their research, the authors propose, for the sake of analytical clarity and transparency, to consolidate the models listed above and reduce them to nine broad archetypes of criminal business models. This approach avoids the need to create a voluminous catalog of dozens of disparate services and instead focuses on describing the underlying structural logic. Each archetype will be represented by two data sets: the key function and the dominant revenue logic. Let us examine them in the following order.

1. R&D and optimization: vulnerability research, testing, tool refinement; service and consulting revenue.
2. Access and access brokering: acquiring, verifying, and reselling access; access revenue, revenue-sharing model.
3. Infrastructure, evasion, and resilience: hosting, anonymization, obfuscation, resilience; infrastructure and rental revenue.
4. Payload and malicious execution: infection, drainage, sabotage, encryption; subscription and performance-based revenue.
5. Operational outsourcing: call centers, solver functions, consulting, support; fee-based and service rent.
6. Markets, trust, and governance: escrow, ratings, arbitration, market-making; commission and intermediary rent.
7. Monetization, cash-out, and laundering: conversion, routing, mixing, drops; financial-routing rent.
8. Influence, deception, and reputation: deepfakes, bot farms, disinformation, review manipulation; information and reputation rent.

9. Meta-strategies and systemic reproduction: dual-use, digital reincarnation, adaptation, parasitic models; strategic and investment rent.

The most important feature of the proposed architecture is that the same solution can simultaneously function as a technical module, a service, and an element of a broader business model. For example, access can be the product of a direct transaction (sale), an entry point into a more complex operation, or part of a revenue-sharing scheme. Infrastructure can be a standalone entity—a service for sale, a hidden support circuit, or a node through which rent is captured. Consequently, Metacrime can be viewed as a construction set where individual modules are combined into new configurations, and economic sustainability is achieved through their reusability and interoperability.

V. CONCLUSIONS

The Metacrime architecture shows what the system consists of, but does not explain how it operates. This requires an analysis of the life cycle of destructive digital value. In the proposed model, this cycle includes the following interconnected phases: idea—research—development—testing—productization—service packaging—market coordination—monetization—profit distribution—reinvestment.

But this is not merely an abstract intention on the part of the offender; rather, it is the identification of a technological or organizational opportunity that can be economically rationalized as a source of future profit. In this sense, a Metacrime participant acts not only as a technical actor but also as an entrepreneur: they assess whether there is demand, whether they have sufficient resources of their own, whether they can rent the necessary functionality, acquire an intermediate asset, or integrate into an existing service chain.

The research phase transforms fragmented knowledge into a designable function. This stage involves analyzing vulnerabilities, competitor practices, existing services, technical constraints, market niches, and monetization options. Development then gives the idea a technical, organizational, or infrastructural form. This could be code, an access scenario, an obfuscation scheme, a financial roadmap, a consulting package, or a service module. Testing serves as a filter and initial validation of the business model: can the feature be scaled, is there sufficient demand, and how sustainable and compatible is it with other modules.

Productization refers to the process of transforming a project solution into a marketable product. As soon as a feature becomes transferable, rentable, updatable, and maintainable, it ceases to be a one-off initiative and becomes a marketable product. This is where the service layer comes into play: support, updates, training, consulting, customization, help desk, and sometimes—a guarantee of results. It is precisely in this phase that Metacrime definitively transcends the scope of individual criminal activity and becomes a service-oriented platform environment.

Market coordination integrates the service into a broader exchange ecosystem. At this stage, suppliers, intermediaries, operators, buyers, trusted parties, financial service providers, and infrastructure nodes come together. Intermediate assets—such as initial access—become a distinct liquid commodity. The better the mechanisms for trust, rating, and arbitration are established, the lower the transaction costs of illicit exchange. Specific markets for semi-finished products also emerge here: not for an unfinished attack, but for access, a route, a spoofed identity, a consulting service, a tool, or a monetization channel.

Monetization is the conversion of destructive digital value into a liquid form. Revenue can be generated through subscriptions, rentals, pay-per-use models, commissions, revenue shares, premium

services, consulting fees, or hybrid schemes. It is important to note that a significant portion of revenue is generated not at the level of the final malicious action, but at the level of control over the intermediate conditions that enable it: access, infrastructure, anonymization, trusted intermediation, routing, and cash-out.

Profit distribution within Metacrime is determined not only by participation but also by control over a critical node in the chain. The scarcity of a function, the supplier's reputation, the exclusivity of access, the degree of risk, and the ability to retain customers within the service loop define the revenue hierarchy. Therefore, a stable position in the ecosystem is not necessarily held by those who carry out the most "visible" attacks, but by those who control a recurring and scarce segment of the circulation of destructive digital value.

REFERENCES

Alexandrou, A., 2021. Cybercrime and information technology: The computer network infrastructure and computer security, cybersecurity laws, Internet of Things (IoT), and mobile devices.: CRC Press.

Baker, D. J. &. Robinson. P. H., 2020. Artificial intelligence and the law: Cybercrime and criminal liability.: Routledge.

Bovenzi, G. M., 2023. MetaCrimes: Criminal accountability for conducts in the Metaverse. In: Companion Proceedings of the ACM Web Conference 2023, April, pp. 565-567.

Gómez-Quintero, J., Johnson, S. D., Borrion, H., & Lundrigan, S., 2024. A scoping study of crime facilitated by the metaverse. Futures, Volume 157, p. 103338.

Haber, E., 2024. The Criminal Metaverse. Indiana Law Journal, Vol 99. (Iss 3).

Karapatakis, A. 2025. Metaverse crimes in virtual (Un) reality: Fraud and sexual offences under English law. Journal of Economic Criminology, 7, 100118.

Kshetri, N., 2010. The global cybercrime industry: economic, institutional and strategic perspectives.: Springer Science & Business Media.

Marion, N. E., & Twede, J., 2020. Cybercrime: An encyclopedia of digital crime.: Bloomsbury Publishing USA.

Ohrimenco, S., Orlova, D., & Cernei, V., 2026. The Shadow Digital Economy: Threats and Challenges for the Information Ecosystems. In: Value Creation in Digital Platforms and Business Ecosystems.: Routledge., pp. 50-72.

Ohrimenco, S., Orlova, D., & Cernei, V., 2023. Cyber threats modeling: An empirical study. Business Management/Biznes Upravlenie., 33(3), pp. 90-106.

Schneider, F., & Enste, D. H., 2013. The shadow economy: An international survey.: Cambridge University Press.

Skorich, P., & Manning, M., 2024. Insider Threat: A Systemic Approach.: Routledge.

Steinmetz, K. F., 2023. Against cybercrime: Toward a realist criminology of computer crime.: Routledge.

Tiwari, M., Zhou, Y., Gilmour, P., & Bernot, A., 2025. Confronting metacrime: complexities, enforcement challenges, and regulatory pathways. Law, Innovation and Technology., Vol 17. (1), pp. 159-176.

Watters, P. A., 2023. Cybercrime and cybersecurity.: CRC Press.

Zhou, Y., Tiwari, M., Bernot, A., & Lin, K., 2024. Metacrime and cybercrime: Exploring the convergence and divergence in digital criminality. Asian Journal of Criminology., Vol. 19(3), p. 419–439.

CHALLENGES OF ARTIFICIAL INTELLIGENCE IMPLEMENTATION IN CYBERSECURITY OF SMES FROM THE REPUBLIC OF MOLDOVA IN THE CONTEXT OF ACCELERATED DIGITALISATION

CZU: 004.8:[004.056:334.72.012.63/.64](478)
DOI: https://doi.org/10.53486/tids2026.36

LUCIA GUJUMAN
Associate Professor, Academy of Economic Studies of Moldova
e-mail: gujuman.lucia@ase.md
ORCID ID: 0000-0001-7940-4291

EMILIA GOGU
Associate Professor, Academy of Economic Studies of Bucarest
e-mail: emilia.gogu@csie.ase.ro
ORCID ID: 0000-0002-7333-7128

ZINOVIA TOACĂ
Associate Professor, Academy of Economic Studies of Moldova
e-mail: toaca@ase.md
ORCID ID: 000-0002-8304-1961

VITALIE URSACHI
Academy of Economic Studies of Moldova
e-mail: ursachi.vitalie@ase.md
ORCID ID: 0009-0008-9206-1324

Abstract. The accelerated digital transformation of small and medium-sized enterprises (SMEs) generates new cybersecurity vulnerabilities, while artificial intelligence (AI) offers advanced tools for threat detection and prevention. This study examines the challenges of AI adoption in cybersecurity for SMEs in the Republic of Moldova, employing a mixed methodology combining scientific literature analysis, national statistical data analysis, and comparison with the European regulatory framework. Results indicate that Moldovan SMEs are predominantly exposed to phishing attacks (60–70%), ransomware (50–60%), and account compromise (45–60%), with a low level of cybersecurity maturity and significant deficits in competencies and resources for AI-based solution adoption. The study proposes an implementation framework adapted to the local context, aligned with NIS2 Directive (EU 2022/2555), the AI Act (EU 2024/1689), and GDPR (EU 2016/679) requirements. The authors' contribution consists in adapting the NIST framework augmented with AI to the specificities of Moldovan SMEs and formulating recommendations for strengthening cybersecurity resilience.

Keywords: *artificial intelligence; cybersecurity; SMEs; Republic of Moldova; NIS2; AI Act; digitalization.*

JEL Classification: O33; L86; K24; M15; D81

INTRODUCTION

Small and medium-sized enterprises (SMEs) constitute the backbone of the Republic of Moldova's economy, representing 99.2% of all registered enterprises and providing over 65% of the national workforce.(Biroul Național de Statistică al Republicii Moldova, 2025) In the context of the national accelerated digitalization program, reflected in the Digital Transformation Strategy of the Republic of Moldova 2023–2030, approved by the Government of the Republic of Moldova in

September 2023, SMEs have registered an increasing dependence on IT infrastructure and digital services.(Carayannis et al., 2024)

This positive development, however, is accompanied by a proportional increase in exposure to cyber threats. According to the World Economic Forum Global Cybersecurity Outlook 2026 (WEF, 2026), over 77% of organizations are already using artificial intelligence (AI) to detect threats and automate response to cybersecurity incidents. However, AI adoption in SMEs remains significantly lower than in large corporations, due to specific economic, technological and organizational barriers.

The Republic of Moldova faces a double challenge: on the one hand, accelerating digitalization in the context of the European integration process (Law No. 315/2022 on the National Development Strategy "European Moldova 2030"), and on the other hand, the need to align with the European regulatory framework in the field of cybersecurity and artificial intelligence, including the NIS2 Directive (EU 2022/2555), the Artificial Intelligence Regulation (AI Act, EU Regulation 2024/1689) and the General Data Protection Regulation (GDPR, EU 2016/679).

The main objective of this paper is to analyze the challenges of implementing AI in cybersecurity for SMEs in the Republic of Moldova and to propose an implementation framework adapted to the local context, in correlation with the applicable European regulations. The study aims to fill a gap identified in the specialized literature: the absence of AI adoption models in cybersecurity specifically adapted for SMEs in EU associated states with limited institutional capacity.

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY – GLOBAL TRENDS

The use of artificial intelligence in cybersecurity has seen exponential growth in recent years, reflecting both the sophistication of cyber threats and the technical advancement of machine learning algorithms. According to the World Economic Forum Global Cybersecurity Outlook 2026(World Economic Forum, 2026), over 77% of organizations globally are using AI for anomaly detection, incident response automation, and user behavioral analysis.

Research in the literature confirms the effectiveness of AI-based solutions in reducing the time to detect cyber incidents. The Cost of a Data Breach Report 2024 published by IBM Security demonstrates that organizations that use AI and automation in cybersecurity identify and contain security breaches 98 days faster than those that do not use such technologies, generating average savings of $2.22 million per incident (IBM, 2024a).

The Data Breach Investigations Report 2025 shows that credential misuse (22%), vulnerability exploitation (20%), and phishing (16%) are the main vectors through which attackers gained initial access to the breaches analyzed, excluding those caused by errors or internal misuse (Verizon, 2025). For SMBs, these findings highlight the importance of taking concrete steps: protecting accounts, regularly updating systems, and training employees to recognize phishing attempts.

The study published by Rombaldo Junior, Becker and Johnson (2023) in arXiv – entitled “Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity” – conducts a systematic review of the literature on cybersecurity in SMEs for the period 2017–2023. The authors analyze 77 relevant studies, identifying 44 unique themes, and conclude that SMEs face difficulties in ensuring cybersecurity, related to insufficient risk awareness, limited knowledge and restricted financial resources.(Rombaldo Junior Carlos and Johnson Shane, 2023)

A recent contribution is the study by Awan et al. (Awan *et al.*, 2026), published in the journal Scientific Reports, which proposes a cybersecurity framework for SMEs in the field of software development. It combines generative artificial intelligence practices with artificial neural networks

(ANN) and interpretive structural modeling (ISM) to identify threats and organize risk reduction measures. The results suggest the potential of this approach, but its evaluation in other enterprises and in the long term requires further research.

BARRIERS TO AI ADOPTION BY SMES

The study published in PLOS ONE (2025) by Rasdi and Baki – "Navigating the AI landscape in SMEs: Overcoming internal challenges and external obstacles for effective integration" – collects primary data through in-depth interviews with representatives of six SMEs from different sectors and identifies major internal obstacles, including resistance to change, fear of job loss and restricted resources, alongside external obstacles such as the dynamic technological landscape and strict regulatory requirements (Mohd Rasdi and Umar Baki, 2025).

Research published in the Journal of Ethics and Emerging Technologies (2026) – "The Role of Information Security in Responsible AI for Digital SMEs: A Systematic Review of Frameworks, Challenges, and Best Practices" – highlights that, although existing studies focus predominantly on technical and public policy solutions, the human factor remains under-represented in the specialized literature, despite its critical role in cybersecurity (Quainoo and Ahad, 2026). The authors emphasize that financial limitations and skills shortages are the main obstacles to the implementation of responsible AI in digital SMEs.

EUROPEAN REGULATORY FRAMEWORK – NIS2, AI ACT AND GDPR

The European Union has developed in recent years a complex and coherent regulatory framework for cybersecurity and the responsible use of artificial intelligence, with direct implications for SMEs in the Member States and associated countries.

Directive (EU) 2022/2555 (NIS2), adopted on 14 December 2022, set 17 October 2024 as the deadline for Member States to transpose its provisions into national law. It significantly expands the scope of cybersecurity obligations across 18 critical sectors, including energy, transport, healthcare, digital infrastructure and public administration. As a general rule, these obligations apply to medium-sized and large entities in the covered sectors, although certain smaller entities are also included. Article 20 requires management bodies to approve and oversee cybersecurity risk-management measures and provides for their accountability for infringements. Article 16 establishes EU-CyCLONe to support the coordinated management of large-scale cybersecurity incidents and crises (European Parliament and Council of the European Union, 2022). On 20 January 2026, the European Commission proposed targeted amendments to NIS2 to increase legal clarity and simplify compliance. According to the Commission, the proposed changes would ease compliance for 28,700 companies, including 6,200 micro and small-sized enterprises (European Commission, 2026a).

The Artificial Intelligence Act (AI Act), Regulation (EU) 2024/1689 of 13 June 2024, entered into force on 1 August 2024. It sets common rules for AI in the European Union, with requirements that vary according to how a system is used and the risks it poses. For SMEs adopting AI-based cybersecurity tools, an important distinction concerns the classification of high-risk systems. Annex III covers AI used as a safety component in certain critical infrastructure, but recital 55 specifies that components used solely for cybersecurity do not qualify as safety components in this context. A cybersecurity tool is therefore not automatically considered high-risk: its classification depends on its intended use and the relevant legal criteria(European Parliament and Council of the European Union, 2024). The rules take effect in stages. Following the AI Omnibus amendments in 2026, most provisions became applicable on 2 August 2026. The requirements for high-risk systems listed in

Annex III apply from 2 December 2027, while those for high-risk systems embedded in regulated products covered by Annex I apply from 2 August 2028 (European Commission, 2026b).

The interaction between the AI Act and NIS2 is particularly relevant: essential and important entities developing or using AI systems must comply with both the cybersecurity requirements imposed by NIS2 and the specific risk management framework provided for by the AI Act. The overlap is particularly pronounced with regard to incident reporting obligations and supply chain governance (Graux *et al.*, 2025). The European Union Agency for Cybersecurity (ENISA) provides detailed technical guidance for the implementation of Implementing Regulation (EU) 2024/2690, supporting digital infrastructure entities in complying with the requirements of NIS2 (ENISA, 2025).

THE SPECIFIC CONTEXT OF THE REPUBLIC OF MOLDOVA

The Republic of Moldova is advancing its digital transformation through the Digital Transformation Strategy for 2023–2030, developed with UNDP support. At the time of the strategy's approval in 2023, UNDP reported that 44% of public services for entrepreneurs and 34% of those for citizens were available online (UNDP, 2023). Earlier evidence also points to a developed digital infrastructure: an article published on the UNDP website in 2021 reported 4G coverage across 98% of the country's territory, based on 2020 data, and described the ICT sector's contribution to national GDP as approximately 7% (Botezatu Serghei, 2021). These figures provide historical context for Moldova's digital transformation rather than a measure of its current level of digitalisation.

Despite progress in digitalisation, Moldova still needs to strengthen its national cybersecurity capabilities. The ITU Global Cybersecurity Index 2024 places the country in Tier 3 ("Establishing"), indicating that its cybersecurity framework is still developing(ITU, 2024). An important step was the adoption of Law No. 48/2023 on cybersecurity, drafted with support from Estonia and aligned with EU standards (Runde, Kieff and Bryja, 2024; 2024). Institutional development also included the establishment of the Cybersecurity Agency under Government Decision No. 1028/2023 and the National Institute for Cybersecurity Innovation "Cybercor" at the Technical University of Moldova under Government Decision No. 671/2023. These institutions support national cybersecurity governance and the development of specialised skills, respectively (Government of the Republic of Moldova, 2023a; 2023b).

The SME Policy Index: Eastern Partner Countries 2024 identifies challenges affecting the development and digital transformation of SMEs in the Republic of Moldova, including difficulties in accessing finance and gaps in digital skills. The report also recognises progress in strengthening the institutional and regulatory framework, while highlighting the need for further reforms and more targeted support for SME digitalization (OECD., 2024). In 2024, the Ministry of Economic Development and Digitalization developed and published the White Paper on Artificial Intelligence and Data Governance. The document sets out a strategic vision for the responsible use of AI and data to support innovation and economic development. Although it is not a formal policy document, it provides guidance for future national policies, emphasising skills development, resilient infrastructure, responsible AI adoption and alignment with EU standards (MDED, 2024).

RESEARCH METHODOLOGY

This research adopts a mixed-methods approach, which combines qualitative and quantitative dimensions, allowing for a comprehensive analysis of the phenomenon studied from both a theoretical and an applied perspective. This approach is considered appropriate for studies that involve both the

analysis of macroeconomic and technological trends and the assessment of specific institutional contexts (Creswell and Plano Clark, n.d.).

The methodology includes the following main components:

• Systematic analysis of scientific literature indexed in Scopus and Web of Science databases, with a focus on publications from 2020–2026, on the use of AI in SME cybersecurity, adoption barriers and implementation frameworks;

• Analysis of relevant European regulatory documents: NIS2 Directive (EU 2022/2555), AI Act Regulation (EU 2024/1689), GDPR (EU 2016/679) and Cyber Resilience Act (CRA, 2024);

• Statistical analysis of secondary data on the structure of SMEs and the level of digitalization in the Republic of Moldova, using official sources: National Bureau of Statistics (NBS, 2025), Ministry of Economy and Digitalization (MED, 2023, 2024), UNDP Moldova (2023, 2024);

• Analysis of empirical data on the typology and prevalence of cyberattacks on SMEs, based on international reports Verizon DBIR (2025), IBM Security (2024) and ENISA Threat Landscape (2024);

• Comparative analysis between the European Union and the Republic of Moldova on cyber maturity, AI adoption and regulatory framework;

• Original conceptual approach for developing an adapted framework for implementing AI in the cybersecurity of SMEs in the Republic of Moldova, based on the NIST Cybersecurity Framework standard (NIST, 2024) and augmented with AI components.

Methodological limitations include the absence of primary data collected directly from SMEs in the Republic of Moldova due to access and availability constraints, which also constitutes a direction for future research. The data used are representative at the macro trend level, not at the individual organization level.

CYBER THREAT PROFILE OF SMES

Analysis of available data reveals that SMEs in the Republic of Moldova and comparable regions are exposed to a wide range of cyber threats, with different prevalences depending on the sector and level of digital maturity. Table 1 presents the distribution of the main types of attacks, correlated with international data:

Table 1. Distribution of types of cyberattacks in SMEs

Attack type	Estimated share (%)	Main reference source
Phishing and social engineering	60–70	Verizon DBIR (2025); ENISA (2024)
Ransomware	50–60	IBM Security (2024); WEF (2026)
Credential Compromise	45–60	Verizon DBIR (2025)
Exploitation of technical vulnerabilities	30–45	ENISA Threat Landscape (2024)
Supply chain attacks	20–35	WEF (2026); ENISA (2024)
Insider threats	15–25	IBM Security (2024)

Source: *Prepared by the authors based on Verizon DBIR (2025), IBM Security (2024), ENISA (2024), WEF (2026)*

Phishing remains one of the main initial access vectors in data breaches, although the 2025 Verizon Data Breach Investigations Report places it behind credential abuse and vulnerability exploitation. The report also finds that approximately 60% of the breaches analysed involved a human

element, highlighting the continuing importance of employee awareness and secure working practices (Verizon, 2025). These findings suggest that an AI-supported cybersecurity framework for SMEs should combine technical protection with regular staff training.

Ransomware is a particular concern for smaller organisations. In the Verizon dataset, it was involved in 88% of breaches affecting small and medium-sized businesses, compared with 39% of breaches affecting large organisations (Verizon, 2025). The financial consequences of data breaches are also substantial: IBM's Cost of a Data Breach Report 2024 estimates an average global cost of USD 4.88 million across the organisations studied (IBM, 2024a). This figure covers data breaches generally, rather than ransomware incidents or SMEs alone, and provides broader context for the economic importance of cybersecurity.

Implementing AI solutions in cybersecurity offers measurable advantages, extensively documented in the literature. The main benefits identified are:

- AI in cybersecurity: artificial intelligence and machine learning can help organisations analyse cyber threats, but attackers can also use these technologies to develop more sophisticated attacks. Understanding both sides of this development can guide the design of cybersecurity measures in Industry 4.0 environments (De Azambuja et al., 2023).
- Faster identification and containment of breaches: AI and automation can support security teams in identifying and containing data breaches more quickly. IBM's 2024 report found that organisations using these technologies extensively identified and contained breaches an average of 98 days faster than those that did not use them (IBM, 2024b).
- Lower breach costs: AI and automation can help organisations reduce the financial impact of data breaches. IBM's 2024 report found that organisations using these technologies extensively had average breach costs USD 1.88 million lower than those that did not use them (IBM, 2024b).

THE CHALLENGES OF ADOPTING AI IN SMES IN THE REPUBLIC OF MOLDOVA

Although artificial intelligence offers important opportunities for strengthening cybersecurity, its use in SMEs is still limited, including in the Republic of Moldova. The analysis of the specialized literature and available data allowed the identification of six main categories of challenges that hinder the adoption of these solutions:

Table 2. Barriers to AI adoption in SME cybersecurity

Category	Specific Challenges	Relevance for Moldova
Financial	High licensing and implementation costs; ROI difficult to quantify in the short term	High – limited access to financing
Technical	Depreciated IT infrastructure; lack of interoperability; insufficient volume of data to train AI models	High – heterogeneous infrastructure
Human Resources	Shortage of AI and cybersecurity specialists; organizational resistance to change	Very high – brain drain
Regulatory	The complexity of compliance with NIS2, AI Act and GDPR; auditability and transparency requirements	Environment – national legislation in alignment
Organizational	Absence of a security culture; lack of integrated security strategy	High – low level of maturity
Financial	Risks regarding the protection of personal data processed by AI systems; GDPR requirements	Average – GDPR framework partially implemented

Source: *Authors' compilation based on Management Review Quarterly (2024), Rasdi & Baki (2025), ENISA (2024), and OECD/EBRD (2024).*

The lack of advanced digital skills is a challenge for the digital transformation of SMEs in the Republic of Moldova. The OECD/EBRD report (OECD and European Bank for Reconstruction and Development, 2023) highlights the persistent nature of the deficit of advanced ICT skills and the need to strengthen digital readiness in small enterprises. In the context of the present research, these findings suggest that the availability of the necessary skills may also limit the adoption of AI solutions for cybersecurity.

The complexity of the European regulatory framework represents an additional challenge for SMEs falling within the scope of these acts. The study carried out at the request of the European Parliament(Graux *et al.*, 2025) highlights overlaps and difficulties in correlating the AI Act with other European digital regulations. For enterprises with limited resources, identifying applicable obligations and organizing the compliance process may require additional effort. In the case of SMEs from the Republic of Moldova, the relevance of the requirements of NIS2, AI Act, GDPR and CRA should be analyzed according to the activities carried out and the relations with the European Union market.

PROFILE OF SMES IN THE REPUBLIC OF MOLDOVA

SMEs occupy an important place in the economy of the Republic of Moldova, both in terms of their number and their contribution to job creation. In 2023, they constituted 99.2% of all reporting enterprises and had 65.3% of their average number of employees. Most SMEs were active in trade (33.1%), followed by professional, scientific and technical activities (9.2%), agriculture, forestry and fishing (8.9%) and manufacturing (7.9%). Enterprises in the field of information and communications represented 5.9% of all SMEs (Biroul Național de Statistică al Republicii Moldova, 2025).

The level of cyber maturity of Moldovan SMEs is generally low, characterized by:

- ✓ Mixed IT infrastructures, combined with depreciated equipment and outdated applications;
- ✓ Formal cybersecurity policies absent or insufficiently implemented in most organizations;
- ✓ Budget dedicated to cybersecurity below 2% of total IT spending;
- ✓ Generalist IT staff without specialization in cybersecurity or artificial intelligence;
- ✓ Lack of tested disaster recovery and business continuity plans.

In the case of industrial SMEs, the use of operational technology (OT) equipment and IoT devices requires increased attention to cybersecurity. Their integration into networks can introduce additional vulnerabilities, especially when existing systems have limited protection mechanisms. Therefore, security measures need to be adapted to the specificities of the equipment and production processes (ENISA, 2018).

In the financial services sector, stricter regulatory requirements do not eliminate cyber risks, as access to financial resources and sensitive data can attract attackers. In traditional trade and agriculture, digitalization must be accompanied by the development of protective capabilities. Businesses with limited digital resources and skills may face difficulties in preventing and managing cyber incidents.

AI implementation framework in cybersecurity proposed for SMEs

The analysis of the specialized literature, European regulations and the particularities of SMEs in the Republic of Moldova formed the basis for the development of a framework for implementing AI in cybersecurity, called AI-NIST-SME-MD Framework. The proposed framework is based on the five functions of the NIST Cybersecurity Framework, version 1.1 (National Institute of Standards and

Technology, 2018), and integrates artificial intelligence components adapted to the needs and resources of these enterprises:

Table 3. AI-NIST-SME-MD Framework for Implementing AI in Cybersecurity

NIST Function	Proposed AI Component	Recommended Tooling R	Related Requirement
Identification	Automated risk assessment with ML algorithms; IT asset mapping	Vulnerability scanners cu ML; Asset management tools	NIS2 Art. 21; AI Act Art. 9
Protection	Adaptive behavior-based controls; advanced authentication (MFA + biometrics)	Zero Trust Architecture; AI-enhanced IAM	GDPR Art. 32; NIS2 Art. 21
Detection	IDS/IPS with ML; behavioral analysis (UEBA); real-time anomaly detection	SIEM cu ML; NDR tools	NIS2 Art. 23; AI Act Art. 15
Response	SOAR automation; automatic alert triage; automatic isolation of compromised systems	SOAR platforms; AI-driven playbooks	NIS2 Art. 23; AI Act Art. 13
Recovery	Planuri de continuitate generate și testate cu IA; analiză post-incident automata	BCP/DRP tools; AI forensics	NIS2 Art. 21(f); ISO 22301

Source: *Original contribution by the authors, adapted from NIST CSF (2018), NIS2 (EU 2022/2555) and AI Act (EU 2024/1689)*

The author's contribution consists in adapting the NIST framework to the needs and possibilities of SMEs in the Republic of Moldova. The model takes into account the limited financial resources, the diversity of the IT infrastructure and the lack of personnel with specialized skills, as well as the relevant European requirements, including NIS2 and the AI Act, to the extent that they are applicable. The modular structure allows for the gradual introduction of the proposed measures and their expansion as the enterprise develops its capabilities and has additional resources.

The use of AI in SME cybersecurity involves both capitalizing on its benefits and examining the applicable legal requirements. Solutions for anomaly detection, user authentication and network monitoring are not automatically classified as high-risk systems. The classification depends on the purpose of use and the conditions set out in the AI Act. For systems falling into this category, the regulation establishes requirements regarding risk management, transparency, human oversight, accuracy, robustness and cybersecurity (European Parliament and Council of the European Union, 2024).

Within the proposed model, these principles are considered benchmarks for the responsible use of AI. Their application aims to support the understanding of the generated results, the intervention of personnel when necessary and the monitoring of risks during use. For SMEs in the Republic of Moldova, legal obligations should be analyzed depending on the activity of the enterprise and the scope of the regulation.

For SMEs to which these requirements apply, documenting compliance and organising human supervision may require additional effort. Meeting the obligations requires time, technical skills and legal knowledge, resources that may be limited in small enterprises. In this context, practical guides, staff training and support measures tailored to the needs of SMEs can facilitate the responsible use of AI and compliance with legal requirements. The AI Act provides for support measures for these enterprises and takes into account their needs in the development of implementation guidelines (European Parliament and Council of the European Union, 2024).

CONCLUSIONS AND RECOMMENDATIONS

The analysis highlights the potential of artificial intelligence to support SMEs' cybersecurity by detecting threats, automating incident response activities, and using available resources more efficiently. However, realizing these benefits depends on the readiness of enterprises and the integration of AI solutions into existing processes. For SMEs in the Republic of Moldova, limited financial resources, lack of specialized skills, and the need to modernize IT infrastructure can make this process difficult.

The study's findings indicate the need for a gradual approach, in which digitalization is accompanied by the development of cyber protection capabilities. Staff training, risk assessment, and access to technical support are important directions for the responsible use of AI. At the same time, European requirements must be analyzed according to the activity of each enterprise and the scope of relevant regulations.

The AI-NIST-SME-MD framework proposed in the paper aims to provide SMEs with a benchmark for the gradual integration of AI into cybersecurity. Its modular structure allows for the selection of measures based on the identified risks, available resources and the level of preparedness of the enterprise. The application of the framework can support the strengthening of protection and the organization of the compliance process, and its practical usefulness is to be assessed through testing in SMEs in the Republic of Moldova.

- Based on the results of the analysis, the following recommendations are proposed to support SMEs in the Republic of Moldova in the adoption and responsible use of AI in cybersecurity:
- Develop a financial support program for SMEs, facilitating investments in cybersecurity, including the adoption of AI solutions appropriate to their needs. The funding could combine national resources with European opportunities, subject to the eligibility conditions of the relevant programs.
- Strengthening assistance services for SMEs in the field of cybersecurity, through a specialized structure or by developing the capacities of existing institutions. These services could include technical consultancy, risk assessment and staff training.
- Develop a practical guide on the requirements of NIS2 and AI Act relevant to SMEs, explaining the conditions of applicability and the necessary measures for compliance. The guide could be developed with the involvement of competent institutions and specialists in the field.
- Examine the opportunity of tax incentives for investments in cybersecurity, including for AI solutions, based on an assessment of the costs and benefits for businesses.
- Develop university and continuing professional training programs in cybersecurity and AI, by strengthening the collaboration between universities, businesses and public institutions. The focus should be on the practical skills needed to implement and use these solutions.

REFERENCES

Awan, M., Alam, A., Khan, R.A., Alwageed, H.S., Ayouni, S. and Almagrabi, A.O., 2026. A generative AI-driven cybersecurity framework for small and medium enterprises software development: an ANN-ISM approach. *Scientific Reports*, 16(1), p.9813. https://doi.org/10.1038/s41598-026-37614-8.

Biroul Național de Statistică al Republicii Moldova, 2025. *Activitatea întreprinderilor mici și mijlocii în anul 2024*. Biroul Național de Statistică al Republicii Moldova. Available at: https://statistica.gov.md/ro/activitatea-intreprinderilor-mici-si-mijlocii-in-anul-2024-9557_61902.html.

Botezatu Serghei, 2021. *Digital Transformation of Moldova: there is no way back*. United Nations Development Programme. Available at: https://www.undp.org/moldova/blog/digital-transformation-moldova-there-no-way-back

Carayannis, E.G., Dumitrescu, R., Falkowski, T. and Zota, N.-R., 2024. Empowering SMEs "Harnessing the Potential of Gen AI for Resilience and Competitiveness". *IEEE Transactions on Engineering Management*, 71, pp.14754–14774. https://doi.org/10.1109/TEM.2024.3456820.

Creswell, J.W. and Plano Clark, V.L., n.d. *Designing and Conducting Mixed Methods Research*. 3rd edn. Thousand Oaks, CA: SAGE Publications.

De Azambuja, A.J.G., Plesker, C., Schützer, K., Anderl, R., Schleich, B. and Almeida, V.R., 2023. Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. *Electronics*, 12(8), p.1920. https://doi.org/10.3390/electronics12081920.

ENISA, 2018. *Good Practices for Security of Internet of Things in the Context of Smart Manufacturing*. European Union Agency for Network and Information Security. Available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot.

ENISA, 2025. *Technical implementation guidance on Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures*. Institution. Available at: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

European Commission, 2026a. *Commission strengthens EU cybersecurity resilience and capabilities*. European Commission. Available at: https://digital-strategy.ec.europa.eu/en/news/commission-strengthens-eu-cybersecurity-resilience-and-capabilities.

European Commission, 2026b. *Timeline for the Implementation of the EU AI Act, 2026*. AI Act Service Desk. Available at: https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act.

European Parliament and Council of the European Union, 2022. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

European Parliament and Council of the European Union, 2024. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

Government of the Republic of Moldova, 2023a. *Hotărârea Guvernului nr. 671 din 13 septembrie 2023 privind dezvoltarea profesională în domeniul securității cibernetice*. Available at: https://www.legis.md/cautare/getResults?doc_id=139187&lang=ro.

Government of the Republic of Moldova, 2023b. *Hotărârea Guvernului nr. 1028 din 21 decembrie 2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică*. Available at: https://www.legis.md/cautare/getResults?doc_id=140895&lang=ro.

Graux, H., Garstka, K., Murali, N. and Cave, J., 2025. *Interplay between the AI Act and the EU digital legislative framework*. [PE 778.575] European Parliament. Available at: https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU%282025%29778575.

IBM, 2024a. *Cost of a Data Breach Report 2024*. IBM. Available at: https://emea.ingrammicro.com/getmedia/6ed5227f-ce0a-445e-98a2-8a2c195df484/IBM-Cost-of-a-Data-Breach-Report-2024.pdf.

IBM, 2024b. *Cost of a Data Breach Report 2024*. IBM. Available at: https://emea.ingrammicro.com/getmedia/6ed5227f-ce0a-445e-98a2-8a2c195df484/IBM-Cost-of-a-Data-Breach-Report-2024.pdf.

ITU, 2024. *Global Cybersecurity Index 2024*. International Telecommunication Union. Available at: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf.

MDED, 2024. *[POLICY PAPER] Cartea Albă privind Inteligența Artificială și Guvernanța Datelor – primul document cadru de politici al MDED*. Ministerul Dezvoltării Economice și Digitalizării. Available at: https://mded.gov.md/ .

Mohd Rasdi, R. and Umar Baki, N., 2025. Navigating the AI landscape in SMEs: Overcoming internal challenges and external obstacles for effective integration. *PLOS One*, 20(5), p.e0323249. https://doi.org/10.1371/journal.pone.0323249.

National Institute of Standards and Technology, 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.6.

OECD., EBRD., 2024. *SME Policy Index: Eastern Partner Countries 2024*. OECD Publishing. Available at: https://www.oecd.org/en/publications/sme-policy-index-eastern-partner-countries-2024_3197420e-en/full-report.html.

OECD and European Bank for Reconstruction and Development, 2023. *SME Policy Index: Eastern Partner Countries 2024: Building Resilience in Challenging Times*. SME Policy Index. OECD Publishing. https://doi.org/10.1787/3197420e-en.

Quainoo, C.R. and Ahad, M.A.R., 2026. The Role of Information Security in Responsible AI for Digital SMEs: A Systematic Review of Frameworks, Challenges, and Best Practices. *Journal of Ethics and Emerging Technologies*, 36(1), pp.1–29. https://doi.org/10.55613/jeet.v36i1.193.

Rombaldo Junior Carlos, B.I. and Johnson Shane, 2023. *Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity*. Available at: https://arxiv.org/abs/2309.17186.

Runde, D.F., Kieff, L. and Bryja, T., 2024. *Strengthening Moldova's Cyber Landscape*. Center for Strategic and International Studies.

UNDP, 2023. *A 100% digital state: The strategy for digital transformation of the Republic of Moldova for 2023-2030, approved by the Executive*. United Nations Development Programme. Available at: https://www.undp.org/moldova/press-releases/100-digital-state-strategy-digital-transformation-republic-moldova-2023-2030-approved-executive .

Verizon, 2025. *2025 Data Breach Investigations Report*. Verizon. Available at: https://www.verizon.com/business/resources/Tc25/reports/2025-dbir-data-breach-investigations-report.pdf.

World Economic Forum, 2026. *Global Cybersecurity Outlook 2026*. World Economic Forum. Available at: https://www.weforum.org/publications/global-cybersecurity-outlook-2026/ [Accessed 30 September 2026].

În redacția autorilor

Bun de tipar 05.11.2026
Coli editoriale 23,25. Coli de autor 23,0. Coli de tipar 38,50.
Comanda nr. 75.

Serviciul Editorial-Poligrafic
al Academiei de Studii Economice din Moldova
Chişinău, MD-2005, str.Bănulescu-Bodoni 59.
Tel.: 022-402-910