

Digital Transformation for Smart and Resilient Communities

Transformare digitală pentru comunități
inteligente și reziliente



Smart-EDU Hub

Coordonator
Cătălin Vrabie

Guest Editor
Lasse Berntzen

2026

SCRD Book Series



**Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică
Smart-EDU Hub**

Digital Transformation for Smart and Resilient Communities

Transformare digitală pentru comunități inteligente și reziliente

Coordonator:

Conf. univ. dr. **Catalin VRABIE**

Guest Editor

Prof. univ. dr. **Lasse BERNTZEN**



COMITETUL ȘTIINȚIFIC

Prof. univ. dr. **Vasile BALTAC**

Școala Națională de Studii Politice și Administrative, București;

Prof. univ. dr. **Lasse BERNTZEN**

University of South-Eastern Norway, Norvegia;

Prof. univ. dr. **Robert MÜLLER-TÖRÖK**

University of Public Administration and Finance Ludwigsburg, Germany;

Prof. univ. dr. **Florina PÎNZARU**

Școala Națională de Studii Politice și Administrative, București;

Prof. univ. dr. **Alexander PROSSER**

Vienna University of Economics and Business, Vienna, Austria;

Prof. univ. dr. **Christian SCHACHTNER**

RheinMain University of Applied Sciences, Wiesbaden, Germany;

Prof. univ. dr. **Nicoleta CORBU**

Școala Națională de Studii Politice și Administrative, București;

Prof. univ. dr. **Adrian FLOREA**

Universitatea "Lucian Blaga", Sibiu;

Prof. univ. dr. **Marta-Christina SUCIU**

Academia de Studii Economice, București;

Prof. univ. dr. **Ana-Maria BERCU**

Alexandru Ioan Cuza University of Iasi, Romania;

Prof. univ. dr. **Attila BARTA**

University of Debrecen, Hungary;

Prof. univ. dr. **Mălina CIOCEA**

Școala Națională de Studii Politice și Administrative, București;

Conf. univ. dr. **Jacek MAŚLANKOWSKI**

University of Gdańsk, Polonia;

Conf. univ. dr. **Florin Codruț NEMȚANU**

Universitatea Politehnica, București;

Conf. univ. dr. **Mauro ROMANELLI**

University of Naples Parthenope, Naples, Italia;

Conf. univ. dr. **Milena YORDANOVA-KRUMOVA**

Technical University-Sofia, Bulgaria

Conf. univ. dr. **Tamás KAISER**

University of Public Service, Budapest, Hungary

Conf. univ. dr. **Cătălin VRABIE**

Școala Națională de Studii Politice și Administrative, București;

Asist. univ. dr. **Nikola VANGELOV**

St. Kliment Ohridski Sofia University, Bulgaria;

Researcher, PhD. **Daniela LICA**

Carol I National Defence University, Bucharest;

Andrea BECCALLI

Internet Corporation for Assigned Names and Numbers (ICANN).

Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică
Smart-EDU Hub

Digital Transformation for Smart and Resilient Communities

Transformare digitală pentru comunități inteligente și reziliente

Coordonator:

Conf. univ. dr. **Catalin VRABIE**

Guest Editor

Prof. univ. dr. **Lasse BERNTZEN**



Copyright © 2026,
Toate drepturile asupra prezentei ediții aparțin Smart-EDU Hub.

Nicio parte din acest volum (fragment sau componentă grafică) nu poate fi copiată
fără acordul scris al Smart-EDU Hub.

COLEGIU EDITORIAL

PREȘEDINTE

Conf. univ. dr. **Catalin VRABIE**

GUEST EDITOR

Prof. univ. dr. **Lasse BERNTZEN**

ASSOCIATE EDITORS

Raluca Andreea BURTICEL

Denisa-Violeta ENE

Andreea Cristina FLOREA

Ionela Diana GÎLCĂ

Amelia-Elena GÎRCOVEANU

Bianca-Ștefania IONIȚĂ

Elena Emilia NĂSTASE

Alexandra-Elena TĂNĂȘESCU

Diana Andreea TOTOLICI

Editura Tritonic. ISBN: 978-606-749-937-7

Smart-EDU Hub
Faculty of Public Administration, SNSPA
Expozitiei blvd. no. 30A, 6th floor,
Bucharest, Romania, 012104
e-mail: catalin.vrabie@snsa.ro
www.administratiepublica.eu

CUPRINS

Editorial. Digital Transformation for Smart and Resilient Communities	7
Lasse BERNTZEN, Catalin VRABIE	
INNO-CULT: Digitization of Cultural Heritage as a Tool for Sustainable Development and Social Inclusion	13
Elena PRUS, Anatoly BABIN, Ion BARABULA	
Utilizarea IA în sistemele judiciare: De la asistență documentară la managementul jurisdicțional	31
Sebastian AVĂCĂRIȚEI, Mihaela TOFAN	
The use of AI in judicial systems: From documentary assistance to jurisdictional management	49
Sebastian AVĂCĂRIȚEI, Mihaela TOFAN	
Bridging the Digital Divide: Monitoring Smart Specialization and Digital Transformation in Regions of Moldova	67
Anatolie Babin, Sergiu Tutunaru, Ion Covalenco	
Digital Twins and MIS Integration for Urban Resilience: A Strategic Approach to Smart City Evolution	83
Frida Zisko, Beșjana Mema	
Smart Technologies and Rural Cultural Heritage – Perspectives for Sustainable Development	99
Anatoly BABIN, Rafael CILOCI, Andrei MIRZA	
Designing Climate-Smart Edible Gardens through Geospatial Ecological Profiling: A Case Study of Măgurele, Ilfov	119
Miruna-Elena Iliescu-Vasile	
Work–Life Balance for Female Employees in the Advertising–Marketing Sector: The Influence of AI Use	127
Cristina Leovaridis, Camelia-Georgiana Gheorghe, Gabriela V. Popescu	

Structuring and Activation of Knowledge for Intelligent Legal Systems in Smart Cities: Towards Transparent and Fair	147
Nicolae Pelin	
Structurarea și activarea cunoștințelor pentru sisteme juridice inteligente în orașe inteligente: către o justiție transparentă și echitabilă	159
Nicolae Pelin	
AI-driven disinformation and IoT weaknesses: operational cyber management, legal compliance and resilience strategies	171
Sebastian Avăcăriței, Mihaela Tofan	
Voluntary IT Specialist Involvement in Romanian City Digital Strategies	191
Elena CIGU, Doru-Constantin MOCANU	
Enhancing Decision-Making Transparency through E-Participation	203
Florentina Pană-Micu	
The role of artificial intelligence in ensuring cyber security in the concept of smart cities of Ukraine	211
Olha Naumenko	
Ethical governance, compliance and systemic performance in public health services in Romania	219
Doina – Monica Agheorghiesei, Ana-Maria Bercu	
Digital product passport for the textile industry: ensuring transparency, circularity, and cyber resilience	231
Anatolie Babin, Andrey Mirza, Sergiu Tutunaru, Ion Covalenco	
A trust-aware explainable AI framework for cyber-resilient smart transportation infrastructure systems	249
Mohammad Farhad Ayazi, Maninder Singh, Rajiv Kumar	

Editorial. Digital Transformation for smart and Resilient Communities

Lasse BERNTZEN

University of South-Eastern Norway, Norvegia;

Catalin VRABIE

Școala Națională de Studii Politice și Administrative, București

Digital transformation should be judged by its contribution to the life of a community: the reliability of its public services, the accessibility of its institutions, the preservation of its cultural memory, and its capacity to respond to disruption. This is the central editorial proposition of Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente. The contributions assembled here examine how digital tools can support these purposes across cultural heritage, regional development, justice, public participation, healthcare, working life, and infrastructure. Read together, they suggest that community resilience depends on the relationship between technological capability and institutional responsibility. Better information can inform action, but its value depends on who can use it, how its quality is established, and how decisions remain open to scrutiny.

The volume brings these questions into settings with distinct histories and capacities, including Romania, the Republic of Moldova, Albania, Ukraine, and an Indian research context. Its breadth allows us to consider the smart community beyond the boundaries of a metropolitan technology programme. Rural heritage, peri-urban food production, textile supply chains, and employees' personal time all belong within an inquiry into the consequences of digital change. The Romanian and English versions of two legal contributions also extend the readership of this discussion. Their inclusion encourages exchange across linguistic communities while retaining the specificity of the legal and administrative problems under examination.

Cultural heritage provides a compelling starting point because it connects innovation with obligations inherited from the past. Elena Prus, Anatoly Babin, and Ion Barabula, in "INNO-CULT: Digitization of Cultural Heritage as a Tool for Sustainable Development and Social Inclusion," present the Inno4Cult platform as an ecosystem for documentation, education, participation, and cross-border cooperation [1]. Their account links digital preservation to environmental and social objectives through a triple-transition framework. The importance of this proposal lies in its attention to the institutions and communities that give cultural resources meaning. Digitisation can widen access to collections and traditions, but continued stewardship requires local expertise, accessible interpretation, and sustained maintenance. Since the project is described as being at an early stage, its anticipated cultural and territorial effects should guide evaluation rather than be treated as established long-term outcomes.

Anatoly Babin, Rafael Ciloci, and Andrei Mirza develop a related territorial argument in “Smart Technologies and Rural Cultural Heritage – Perspectives for Sustainable Development” [2]. Drawing on the Precucuteni–Cucuteni–Tripolye cultural complex, they explore connections between heritage, smart villages, circular bioeconomy, and cooperation across Moldova, Romania, and Ukraine. The contribution invites renewed attention to local materials, settlement patterns, and inherited knowledge when designing contemporary development strategies. Such historical resources deserve careful study on their own terms. Their translation into present-day building, agricultural, or energy systems requires evidence of technical suitability and contemporary feasibility. Heritage can inform innovation without making historical analogy a substitute for testing.

The capacity to pursue these ambitions is unevenly distributed. In “Bridging the Digital Divide: Monitoring Smart Specialization and Digital Transformation in Regions of Moldova,” Anatolie Babin, Sergiu Tutunaru, and Ion Covalenco connect regional development to data governance, digital maturity assessment, and institutional skills [3]. Their use of LORDIMAS, Joint Research Centre frameworks, and regional data tools points towards a recurring administrative problem: authorities need comparable information to identify priorities, yet often lack the infrastructure and competencies required to produce it. The proposed monitoring approach makes territorial inequality visible and connects diagnosis with capacity building. Its policy value will depend on whether assessment leads to sustained changes in access, skills, and the ability of smaller administrations to participate in innovation networks.

Urban resilience introduces a further question: how does information become a coordinated public response? Frida Zisko and Besjana Mema address this in “Digital Twins and MIS Integration for Urban Resilience: A Strategic Approach to Smart City Evolution” [4]. Their conceptual architecture connects sensing, data integration, simulation, management information systems, and decision intelligence. An illustrative flood scenario shows how technical outputs could enter municipal workflows and support early warning and resource allocation. The contribution is especially useful in placing administrative coordination within the architecture itself. A simulation has limited public value if its warnings do not reach responsible officials or cannot be translated into authorised action. The proposed benefits remain to be evaluated in deployed municipal systems, including the quality of their data, the performance of their forecasts, and the practical response to uncertain predictions.

Miruna-Elena Iliescu-Vasile brings the resilience discussion to a more local scale in “Designing Climate-Smart Edible Gardens through Geospatial Ecological Profiling: A Case Study of Măgurele, Ilfov” [5]. Satellite-derived environmental indicators and a plant suitability assessment inform the design of small-scale edible gardens adapted to local conditions. This approach shows how accessible spatial information can support decisions about underused peri-urban spaces. It also connects digital analysis with activities that require continuing physical care. Suitability modelling offers a basis for plant selection; field trials, cultivation experience, and community participation are needed to establish

actual productivity and maintenance requirements. The study therefore opens a practical research route linking ecological evidence, garden design, and local food resilience.

Justice places particularly demanding conditions on the use of intelligent systems. Sebastian Avăcăriței and Mihaela Tofan, in the Romanian “Utilizarea IA în sistemele judiciare: De la asistență documentară la managementul jurisdicțional” and its English counterpart, “The use of AI in judicial systems: From documentary assistance to jurisdictional management,” propose a framework for governing judicial AI [6], [7]. They distinguish documentary support from uses that may influence the assessment of evidence or judicial outcomes, and discuss risk classification, impact assessment, logging, literacy, contestation, and human oversight. Their contribution centres on verifiable responsibility: oversight must be supported by procedures and records through which the exercise of human judgment can be examined. For court administrations, this means defining permitted tasks and review duties before allowing efficiency objectives to reshape established procedural safeguards.

Nicolae Pelin’s English “Structuring and Activation of Knowledge for Intelligent Legal Systems in Smart Cities: Towards Transparent and Fair Justice” and Romanian “Structurarea și activarea cunoștințelor pentru sisteme juridice inteligente în orașe inteligente: către o justiție transparentă și echitabilă” examine the technical organisation of such assistance [8], [9]. The proposed hybrid architecture combines formal rules and knowledge representations with language-model capabilities for processing text and supporting dialogue. Its modular functions make fact extraction, inference, explanation, and auditability explicit. The manuscript also carefully distinguishes digital judicial infrastructure from automated adjudication and acknowledges that it reports no working prototype or measured judicial effects. Read alongside Avăcăriței and Tofan, this contribution shows why a traceable reasoning process needs both technical evaluation and institutional safeguards. Formal consistency alone cannot establish the fairness of a decision when facts are disputed or legal interpretation remains open.

Digital dependence also changes the conditions under which communities can trust information and maintain essential services. In “AI-driven disinformation and IoT weaknesses: operational cyber management, legal compliance and resilience strategies,” Sebastian Avăcăriței and Mihaela Tofan examine the convergence of synthetic content, connected-device vulnerabilities, and organisational responsibility [10]. Their integrated approach connects technical controls with leadership duties, incident procedures, and regulatory analysis. Olha Naumenko’s “The role of artificial intelligence in ensuring cyber security in the concept of smart cities of Ukraine” places these concerns in the context of Ukrainian smart-city development, wartime pressures, and recovery [11]. Together, the articles direct attention to continuity and preparedness. They also make it necessary to distinguish the potential of AI-assisted protection from the evidence required to establish that a particular security intervention works under operational conditions.

Mohammad Farhad Ayazi, Maninder Singh, and Rajiv Kumar examine this evidentiary question through modelling in “A trust-aware explainable AI framework for cyber-resilient

smart transportation infrastructure systems” [12]. Their framework combines Random Forest regression, SHAP explanations, and cyber-related perturbations. The reported evaluation uses 3,000 synthetic observations and controlled disturbance scenarios, providing a bounded setting for examining prediction, interpretability, and robustness. This is a useful methodological contribution, but simulation results do not establish resilience against the full range of attacks or operating conditions encountered on transport networks. Independent data, representative threat models, and field evaluation would strengthen the connection between the reported performance and decisions about infrastructure deployment. Explanations of model behaviour can support inspection; they do not by themselves certify security.

Anatolie Babin, Andrey Mirza, Sergiu Tutunaru, and Ion Covalenco extend the discussion of trusted information into industrial supply chains in “Digital product passport for the textile industry: ensuring transparency, circularity, and cyber resilience” [13]. Their proposed architecture links product-level traceability, lifecycle information, differentiated access, and the SORINTEX textile cluster. It brings the environmental purposes of digital transformation into direct contact with commercial confidentiality and information security. For this editorial, the key implication is that useful transparency requires governance of the underlying records. A durable ledger or a scannable product identifier can support traceability, but neither establishes that the original data are accurate. Responsibility for verification, correction, access, and continuing interoperability remains central to the credibility of product information.

Public participation supplies another measure of whether digital transformation creates shared value. Elena Cigu and Doru-Constantin Mocanu, in “Voluntary IT Specialist Involvement in Romanian City Digital Strategies,” examine expertise transfer and civic collaboration in Bucharest, Cluj-Napoca, Iași, and Timișoara [14]. Their document-based analysis identifies routes through which volunteer technical communities can contribute to local digital strategies, while recognising the limits of generalising from four urban centres. Florentina Pană-Micu’s “Enhancing Decision-Making Transparency through E-Participation” addresses the relationship between digital engagement and transparent administration [15]. These contributions complement one another: access to external expertise can improve an administration’s ability to develop services, while citizen participation can inform their purposes and priorities. Both require clear institutional arrangements. Volunteer support needs continuity and defined responsibilities; consultation needs accessible channels, meaningful consideration of submissions, and visible feedback on decisions.

The distinction between formal arrangements and lived outcomes becomes particularly clear in “Ethical governance, compliance and systemic performance in public health services in Romania,” by Doina-Monica Agheorghiesei and Ana-Maria Bercu [16]. Their qualitative synthesis examines the limitations of compliance when communication, reporting culture, and accountability remain weak. The editorial lesson extends beyond healthcare: digital reporting and expanded procedural requirements need an organisational environment in which problems can be disclosed and addressed. The article’s argument

supports closer attention to ethical governance and patient interests, while its integrative methodology calls for caution about causal claims. Assessing reform requires evidence about care, access, safety, and institutional behaviour alongside the existence of rules or information systems.

Cristina Leovaridis, Camelia-Georgiana Gheorghe, and Gabriela V. Popescu examine another lived outcome in “Work–Life Balance for Female Employees in the Advertising–Marketing Sector: The Influence of AI Use” [17]. Interviews with ten non-managerial female employees and five female managers reveal the importance of workload, flexibility, caring responsibilities, and boundaries around personal time. Their findings complicate the assumption that faster task completion necessarily improves work–life balance: reviewing generated outputs, learning new tools, and responding to heightened expectations may absorb anticipated savings. The qualitative sample provides situated insight rather than population-wide estimates. Its relevance to this volume lies in making working conditions part of the evaluation of digital progress. A community’s ability to benefit from innovation depends partly on whether the people implementing and using it can sustain their professional and personal lives.

Across these contributions, we see a research agenda grounded in public value and proportionate evidence. Conceptual architectures should identify testable propositions and implementation conditions. Local case studies should specify which contextual features affect transferability. Simulated evaluations should describe the limits of their data and threat assumptions. Governance proposals should identify who is responsible, how decisions can be challenged, and which outcomes will demonstrate improvement. For the subjects examined here, meaningful evaluation includes regional access and institutional capacity [3], preparedness and ecological performance [4], [5], judicial safeguards [6]–[9], service continuity and data integrity [10]–[13], effective participation [14], [15], healthcare outcomes [16], and working conditions [17]. These different measures preserve the specific purposes of each field while enabling a shared discussion of responsible digital transformation.

As editors and guest editors, we offer this volume as an invitation to pursue that discussion through careful research and sustained collaboration. We thank the contributing authors and the scientific and editorial colleagues who support this exchange. The papers identify promising directions, unresolved questions, and practical responsibilities for researchers, public authorities, practitioners, and communities. Their collective significance lies in bringing technological choices into conversation with cultural stewardship, professional judgment, and democratic accountability. Smart and resilient communities will be strengthened when innovation is evaluated against these enduring obligations and supported by evidence of improvements in everyday life.

References

- [1] E. Prus, A. Babin, and I. Barabula, “INNO-CULT: Digitization of Cultural Heritage as a Tool for Sustainable Development and Social Inclusion,” in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.

- [2] A. Babin, R. Ciloci, and A. Mirza, "Smart Technologies and Rural Cultural Heritage – Perspectives for Sustainable Development," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [3] A. Babin, S. Tutunaru, and I. Covalenco, "Bridging the Digital Divide: Monitoring Smart Specialization and Digital Transformation in Regions of Moldova," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [4] F. Zisko and B. Mema, "Digital Twins and MIS Integration for Urban Resilience: A Strategic Approach to Smart City Evolution," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [5] M.-E. Iliescu-Vasile, "Designing Climate-Smart Edible Gardens through Geospatial Ecological Profiling: A Case Study of Măgurele, Ilfov," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [6] S. Avăcăriței and M. Tofan, "Utilizarea IA în sistemele judiciare: De la asistență documentară la managementul jurisdicțional," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [7] S. Avăcăriței and M. Tofan, "The use of AI in judicial systems: From documentary assistance to jurisdicțional management," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [8] N. Pelin, "Structuring and Activation of Knowledge for Intelligent Legal Systems in Smart Cities: Towards Transparent and Fair Justice," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [9] N. Pelin, "Structurarea și activarea cunoștințelor pentru sisteme juridice inteligente în orașe inteligente: către o justiție transparentă și echitabilă," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [10] S. Avăcăriței and M. Tofan, "AI-driven disinformation and IoT weaknesses: operational cyber management, legal compliance and resilience strategies," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [11] O. Naumenko, "The role of artificial intelligence in ensuring cyber security in the concept of smart cities of Ukraine," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [12] M. F. Ayazi, M. Singh, and R. Kumar, "A trust-aware explainable AI framework for cyber-resilient smart transportation infrastructure systems," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [13] A. Babin, A. Mirza, S. Tutunaru, and I. Covalenco, "Digital product passport for the textile industry: ensuring transparency, circularity, and cyber resilience," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [14] E. Cigu and D.-C. Mocanu, "Voluntary IT Specialist Involvement in Romanian City Digital Strategies," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [15] F. Pană-Micu, "Enhancing Decision-Making Transparency through E-Participation," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [16] D.-M. Agheorghiesei and A.-M. Bercu, "Ethical governance, compliance and systemic performance in public health services in Romania," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.
- [17] C. Leovaridis, C.-G. Gheorghe, and G. V. Popescu, "Work–Life Balance for Female Employees in the Advertising–Marketing Sector: The Influence of AI Use," in *Digital Transformation for Smart and Resilient Communities / Transformare digitală pentru comunități inteligente și reziliente*, forthcoming.

INNO-CULT: Digitization of Cultural Heritage as a Tool for Sustainable Development and Social Inclusion

Elena PRUS

*Qualified Doctor, University Professor
Free International University of Moldova, Chişinău, Republic of Moldova
eprus@ulim.md*

Anatoly BABIN

*Institutional PhD researcher, MBA
Academy of Economic Studies of Moldova, Chişinău, Republic of Moldova
anatolii.babin@ase.md*

Ion BARABULA

*Researcher, President of AO “Be Up”
Academy of Music, Theatre and Fine Arts (AMTAP), Chişinău, Republic of Moldova
beup.org@gmail.com*

Abstract

Objectives: This paper examines the role of digital transformation in ensuring sustainable development of cultural heritage amidst global challenges such as climate change, demographic shifts and social inequality. The study aims to demonstrate how the INNO-CULT project integrates advanced digital tools to enhance the conservation, mediation and promotion of cultural resources, contributing to the implementation of the Council of Europe’s Strategy 21. **Prior work:** The research builds on contemporary discussions on digitalisation of cultural heritage, participatory cultural ecosystems and sustainable territorial development, particularly drawing from recent studies published in SCRD addressing interoperable platforms, community engagement and the use of immersive technologies for cultural preservation. **Approach:** The study employs a mixed methodological framework combining analysis of digital platform design, case-based observations of regional heritage initiatives and evaluation of participatory formats such as digital laboratories, seminars and innovative events. Special attention is paid to multilingual accessibility, open data principles and the integration of AR, 3D visualization and automated text processing. **Results:** The findings demonstrate that the creation of a sustainable, interoperable digital platform significantly enhances access to cultural artefacts and educational resources, stimulates community participation and supports the formation of cultural and tourist routes. These outcomes contribute to the development of resilient regional cultural ecosystems and promote social inclusion by strengthening cultural identity and accessibility for diverse audiences. **Implications:** The study offers insights for researchers, policymakers and cultural practitioners seeking to implement digital heritage strategies that reinforce sustainability, openness and transnational cooperation. **Value:** The paper’s contribution lies in presenting a comprehensive model of digital transformation of cultural heritage that not only advances technological innovation but also addresses broader socio-economic objectives, offering a replicable framework aligned with European cultural policy priorities.

Keywords: interoperable platforms; community engagement; cultural ecosystems; transnational cooperation; digital humanities

1. Introduction

In recent decades, European countries have faced a series of new challenges that have not only changed political and economic priorities, but also imposed a different perspective on the role of cultural heritage in society. Climate change, demographic transformations, uneven territorial development, increased migration and social inequality, as well as the accelerated digital revolution have created a new reality in which traditional models of

conservation and use of cultural heritage are no longer effective. In these circumstances, cultural heritage is increasingly considered a strategic asset capable not only of strengthening identity and social solidarity, but also of stimulating innovation, expanding educational opportunities and supporting sustainable territorial development. However, for heritage to fulfill these functions, it must be integrated into the modern digital and socioeconomic ecosystem.

Here arises the need for a theoretical and practical rethinking of cultural heritage: not as a static collection of artifacts, but as a living resource capable of generating new forms of participation, economic activity, knowledge and intercultural interaction. The European Strategy for Cultural Heritage in the 21st Century (Strategy 21) [1], adopted by the Council of Europe, emphasizes the need to move from a model of “conservation” to one of integration and development, in which innovation, digitalization, local participation and sustainability play a key role. This strategy is particularly relevant for Moldova, which is simultaneously facing demographic pressure, territorial imbalances, the loss of traditional crafts and practices and the rapid migration of young people, leading to gaps in the transmission of cultural traditions.

Despite its rich tangible and intangible heritage – from ancient archaeological sites to a complex system of folk rituals, visual arts and musical traditions – Moldova lacks a coherent infrastructure for digital documentation, preservation and promotion of cultural heritage. As a result, a significant part of cultural resources remains hidden, unused or at risk of disappearing. Moreover, the country’s regions are developing unevenly: many rural areas are losing population and youth, which is testing the capacity of communities to maintain and transmit their cultural traditions. In this context, the need to modernize approaches to the cultural sector – a modernization that combines digital technologies, educational programs, regional development and local participation – is particularly urgent.

The INNO-CULT project was developed specifically to address these challenges. It proposes a new model for digitization and integration of cultural heritage into public life, oriented towards the principles of sustainable development, social equality, interregional cooperation and innovation. The central element of the project is the creation of the Inno4Cult platform, which aims to become more than a simple digital archive or visualization tool, but a complete ecosystem for research, education, communication and cross-border collaboration. The platform will operate in six development regions of the Republic of Moldova and will integrate with neighboring regions of Romania and Ukraine - countries with which the Republic of Moldova has historical, cultural and linguistic ties.

The developed model is based on the concept of the Triple Transition [2], which has become a key element in European development policy in recent years. This concept integrates the green (environmental), digital and social transitions into a single system, allowing sustainability to be viewed as a comprehensive process, rather than as a set of separate areas. Within the Triple Transition approach, cultural heritage ceases to be an object of protection and becomes a tool for sustainable development: the green transition ensures the conservation of natural and cultural landscapes and the rational management of

resources; the digital transition creates new forms of access, research, interpretation and promotion of heritage; and the social transition strengthens citizens' participation, expands inclusion and promotes cohesive and solidary communities.

It is important to emphasize that the relevance of digitizing cultural heritage is confirmed by an analysis of the national and regional strategies of the Republic of Moldova. The strategic document “Moldova 2030” emphasizes the need to improve the digital literacy of the population, modernize public services and develop an innovative economy. Although cultural heritage is only indirectly mentioned in the strategy, the idea of digitizing the cultural sector is fully consistent with the general paradigm of modernization. Moreover, the new “Strategy for Culture and Cultural Heritage 2025–2035” [3] introduces for the first time the concepts of digital archives, digital tourist routes, virtual museums and digital platforms as mandatory elements of the state’s cultural policy. The regional development strategies of the Republic of Moldova do not yet have a similarly developed digital component, but increasingly emphasize the role of cultural resources as a factor of tourism and regional attractiveness. These documents highlight the need to create a digital infrastructure and form cultural institutions, but implementation mechanisms are still lacking. Therefore, the Inno4Cult project can play an integrative role, connecting regional development plans and national strategic documents with European programs. It is important to note that the development of the digitization of cultural heritage in Europe is accompanied by strong support from transnational programs: Horizon Europe funds research in digital humanities, projects to create digital twins of historical sites and platforms for analyzing cultural data. The Creative Europe program [4] supports digital storytelling, artists’ mobility and innovative cultural platforms. The Interreg NEXT Romania–Republic of Moldova programme [5] create opportunities for the development of cross-border routes, virtual museums and digital laboratories. The S3 (Smart Specialization) thematic platforms form interregional clusters focused on innovation in culture, education and tourism.

Currently, the Republic of Moldova is only partially involved in these ecosystems, but the Inno4Cult platform has the potential to become a tool for the country’s integration into the European innovation space. Thanks to its interoperability, multilingualism, open data and sustainable architecture, the platform will be compatible with European systems, allowing access to Europeana [6], Cultural Gems [7], Heritage Innovation [8] and other EU initiatives. Thus, the current stage of development of the Republic of Moldova requires the creation of a tool capable of integrating national strategies, regional plans, international programmes and local initiatives into a unified ecosystem for the digitalisation and sustainable development of cultural heritage. The Inno4Cult project, based on the Triple Transition methodology, offers just such a model - one that combines technological innovation, social inclusion and environmental sustainability, transforming cultural heritage into a resource for territorial development and strengthening social solidarity.

2. National and regional strategies, European programmes and best practices in cultural heritage digitization

To understand how the Inno4Cult project can be integrated into the strategic development priorities of the Republic of Moldova and the European space, it is necessary to analyze the national strategies, regional plans and transnational programs that shape the modern architecture of cultural and digital initiatives. This analysis reveals that the digitization of cultural heritage is already present in policy documents, but often remains fragmented and not integrated into a unified systemic model. INNO-CULT addresses precisely this institutional disconnect.

The first key document defining the country's development directions is the "National Development Strategy "European Moldova 2030"" [9]. This document defines digital transformation as a key mechanism for modernizing the economy and the social sphere. However, culture and cultural heritage occupy a relatively modest place in the strategy, mainly in the context of tourism development and strengthening cultural identity. The problem is not a lack of interest in heritage, but in the absence of a clear understanding of how it can be integrated into the modern digital economy. However, the strategy sets important conditions for the digitization of heritage: the development of Internet access infrastructure, the creation of public digital services, increasing digital literacy among the population and improving the education system - all of which create a favorable environment for the emergence of projects focused on digital cultural production. Moreover, the strategy proposes to strengthen the role of regional centers in innovation, which is directly related to the idea of creating digital laboratories in six development regions of the country. The recently developed and adopted "Strategy for Culture and Cultural Heritage of the Republic of Moldova for the period 2025-2035" represents a significant step forward. Unlike previous strategic documents, it provides for the first time a holistic understanding of the importance of digital infrastructure for the cultural sector. Priorities include digitizing collections, creating publicly accessible digital heritage platforms, implementing virtual and augmented reality technologies in museums, developing digital literacy among the staff of cultural institutions, and integrating local communities into the processes of documenting and promoting heritage.

A key feature of the strategy is the shift from perceiving culture as a "Financed Sector" to understanding it as a dynamic ecosystem, where cultural heritage becomes part of the knowledge economy, and digital technologies are the basis for innovative development. This logic is fully consistent with the objectives of Inno4Cult: the platform not only creates digital tools for heritage preservation, but also transforms it into a resource for education, science, tourism and social participation. A look at the strategic documents of the regions of the Republic of Moldova reveals a less structured approach compared to national strategies, but a more clearly articulated need to support cultural heritage as a factor of tourism and territorial attractiveness. Most regional plans consider the development of cultural infrastructure as a prerequisite for shaping local identity and improving the quality of life. However, digitalization is rarely presented as an independent objective. Some strategies mention digital tourist routes, modernization of museums and creation of information resources, but they lack a systematic approach to the development of a digital

cultural ecosystem. This means that regional development plans require tools and mechanisms that link heritage digitization to education, innovation, tourism and socio-cultural activities. In this context, Inno4Cult serves not only as a technological platform, but as an "Institutional Bridge" between strategic objectives and their implementation at community and regional level.

The next important level of analysis is represented by the European transnational and interregional programs, which form the framework for cooperation and funding in cultural and digital initiatives. For several decades, the European space has been constantly developing programs to support cultural projects focused on digitization, interoperability and cross-border integration. One of the central programs is Horizon Europe [10], a major research initiative focused on innovation, interdisciplinary research and the creation of digital technologies for areas of social significance. Horizon Europe has created a number of clusters related to digital humanities, visualization of cultural heritage, creation of digital twins of historical sites, big data analysis in culture and sustainable cultural landscapes. These areas align with the objectives of Inno4Cult, as the platform provides for the creation of digital archives, multimodal data, 3D models and the involvement of researchers in the analysis of cultural resources. Thus, INNO-CULT could become the basis for the participation of the Republic of Moldova in Horizon Europe consortia. The second key programme is Creative Europe, an initiative aimed at supporting the cultural and creative industries. It actively funds digital storytelling projects, artistic mobility platforms, digital museums, virtual art labs, educational resources and cross-sectoral initiatives that combine art and technology. The Inno4Cult platform can also be used for applications under the Creative Europe programme, as its architecture integrates cultural, educational and digital components.

Cross-border programmes, such as the Interreg NEXT Romania–Republic of Moldova programme, also play a key role. These programmes focus on the shared use of cultural resources, the creation of cross-border tourist routes and the development of cultural infrastructure and digital services. The regions of Moldova, Ukraine and Romania have common historical and cultural roots, as well as similar challenges in heritage preservation. Therefore, the creation of a common digital space that would unite cultural objects, routes, archives, research and practices is a logical direction for regional cooperation. Inno4Cult, thanks to its multilingualism and interoperability, provides a platform for this interaction. Another important tool is the infrastructure of thematic platforms Smart Specialisation (S3), which form European innovation clusters. Among them, the Innovation in Heritage, Virtual and Smart Cultural Tourism and Education and Digital Skills S3 [11] platforms are particularly important. These platforms allow regions with common interests in innovation to come together and develop joint projects. For Moldova, joining these platforms could mean:

- access to partnerships and European funding,
- participation in innovative pilot projects,
- skills development,
- exchange of technologies,
- building sustainable educational and research networks.

Inno4Cult can become a tool for integrating the regions of the Republic of Moldova into these international clusters, offering common data formats, digital resources, educational programs and visualization capabilities. Finally, an analysis of European best practices in the digitization of cultural heritage demonstrates the importance of creating digital platforms that combine technology, education and citizen participation. Among the most successful initiatives are:

- Europeana - the largest digital library in Europe,
- Cultural Gems – a map of cultural spaces,
- Bologna's digital twin project [12],
- Northern Dimension Partnership on Culture,
- SmartCulture (FP7),
- NUMERIC and others.

All these initiatives demonstrate that digitization does not replace physical assets, but rather enhances their value, creating opportunities for education, tourism, intercultural dialogue and research. Moldova can adapt these models, and Inno4Cult provides the institutional and technical foundation for this process. Thus, an analysis of the strategic and policy framework shows that the Inno4Cult project not only aligns with national and regional priorities, but also fits perfectly with European trends in the digital transformation of cultural heritage. It creates links between strategic documents and practical initiatives, integrating digital, social and environmental objectives into a unified development model.

3. The triple transition as a methodological basis for the digital transformation of cultural heritage

The concept of the "Triple Transition" [13] has become a key element in the strategic thinking of the European Union and the Council of Europe in recent years. It defines a new logic for sustainable development, in which the environmental, digital and social components are viewed not in isolation, but as interconnected elements of a single system. This logic is particularly important in the field of cultural heritage, which has traditionally been on the margins of strategic innovation processes and has only in recent years begun to be viewed as a resource for integrated development. Applying the Triple Transition to cultural heritage allows us to rethink its role in society - from a static object of protection to an active platform for innovation, education, tourism, social integration and environmentally responsible territorial management. For the Republic of Moldova, where culture is often relegated to the role of a symbolic resource or a soft power tool, but its potential in the knowledge economy is rarely taken into account, the Triple Transition concept opens up new horizons. It proposes an approach that integrates cultural heritage into the country's modernization processes, becoming a bridge between innovation and social development. In the context of INNO-CULT and the Inno4Cult platform, the "triple transition" becomes more than a simple theoretical framework, but a practical tool for transforming regions, developing human capital and strengthening international cooperation.

3.1. Green transition: Cultural heritage and environmental sustainability

A green transition is not just about reducing the carbon footprint or developing renewable energy. In a broader sense, it involves promoting an environmentally conscious mindset, connecting natural and cultural heritage, and creating sustainable models of territorial management. Moldova possesses a unique natural and cultural landscape: archaeological sites coexist with nature reserves, rural ethnocultural traditions are closely linked to local ecosystems, and historical settlements were formed with natural resources in mind. However, the collapse of traditional economic models, population migration, unplanned development, and climate change are breaking these links. In this situation, a green transition offers tools to restore the resilience of cultural landscapes. An example is the creation of ecologically sustainable cultural and tourist routes, based on a combination of natural and historical-cultural sites. Such routes can become not only a source of tourist attraction, but also a tool for ecological education, youth involvement, craft preservation and sustainable land use. Within Inno4Cult, a green transition manifests itself through:

- documentation of natural and cultural complexes using digital tools;
- creating virtual reconstructions of objects in danger or under threat;
- development of interactive maps of ecologically sensitive areas;
- training educational modules on environmental practices of traditional communities;
- stimulating cross-border green routes (Moldova-Romania-Ukraine).

Such initiatives help not only to preserve heritage, but also to integrate environmental values into the daily lives of citizens.

3.2. Digital transition: Technologies as infrastructure for a new cultural policy

Digitization has become a key factor in the transformation of society, economy and education. However, in the field of cultural heritage, it has long been perceived as an additional tool: digitizing a collection, creating a museum website or preparing a virtual tour. Modern approaches, however, consider digitization as the foundation for creating new forms of interpretation, research, interregional cooperation and citizen participation. As part of the digital transition, cultural heritage becomes part of big data, interactive platforms, educational systems and algorithmic analysis tools. This transition is particularly important for Moldova, where most collections are either not digitized or are only partially digitized, and access to them is limited. The Inno4Cult platform integrates digital transformation on multiple levels. Firstly, it creates a multilingual and interoperable digital infrastructure, capable of integrating archival materials, 3D models, multimedia content, geodata, texts, ethnographic records and educational programs. Secondly, it uses modern visualization tools - augmented and virtual reality, digital twins, interactive maps and cultural routes. This makes access to heritage more visual, emotional and engaging, especially for young people. Thirdly, digitization allows for automatic text analysis, image recognition, and ethnographic data processing, which strengthens the scientific component of the project and creates conditions for international research. Finally, the digital transition facilitates the technological modernization of cultural institutions - museums, libraries, archives and cultural centers. This requires new skills, new educational programs and

collaboration between universities, NGOs and regional administrations. This modernization becomes one of the long-term goals of INNO-CULT.

3.3. Social transition: Inclusion, participation and local identity

The third component of the triple transition – social transition – is essential for understanding the role of cultural heritage in society. Traditionally, social transition is conceptualized in terms of equal access to services, reducing social gaps and supporting vulnerable groups. However, in the context of cultural heritage, social transition means not only inclusion, but also the active participation of citizens in the creation, interpretation and conservation of heritage. This is a shift from “heritage as an object” to “heritage as a living practice”, in which local communities become co-authors of digital content. It is precisely social transition that allows us to overcome the passive approach characteristic of institutional models of heritage protection. Instead of considering citizens as spectators, it transforms them into participants. In the context of INNO-CULT, social transition manifests itself in several ways:

1. Digital heritage laboratories, where residents of the region – schoolchildren, students, tradition bearers and museum staff – can participate in digitization, storytelling, trail creation, video production and multimedia creation.
2. Inclusive educational programs aimed at different age and social groups, including people with disabilities, migrants and representatives of ethnocultural minorities. The Inno4Cult platform creates special access formats, such as audio guides, interactive maps and adapted interfaces.
3. Strengthening local communities, for whom cultural heritage becomes a way to restore identity, increase self-esteem and develop cultural entrepreneurship – crafts, gastronomy and thematic tourism.
4. Cross-border participation, allowing residents of the Republic of Moldova, Romania and Ukraine to exchange cultural practices, educational resources and jointly create digital collections.

Therefore, social transition in the context of Inno4Cult is not limited to expanding access – it transforms cultural heritage into a tool for social development, communication and solidarity.

3.4. The relationship between three transitions: The INNO-CULT integrative model

The main advantage of the Triple Transition is that it considers changes not in individual spheres, but in their interconnection. This is especially important for cultural heritage, since heritage inherently integrates natural, social and cultural components, and digital technologies allow them to be connected into a functional system. Within INNO-CULT, the Triple Transition becomes the platform architecture:

- the green component ensures the sustainability of landscapes, routes and traditional practices;
- the digital component creates tools for documentation, analysis and visualization;
- the social component forms human and institutional connections that transform digital products into sustainable practices.

This model allows for the expansion of the role of cultural heritage, transforming it from an object of conservation into an active resource for territorial development.

3.5. The importance of the triple transition for Moldova and the region

For Moldova, the triple transition is of strategic importance:

- promotes the modernization of cultural institutions;
- forms new skills and educational programs;
- strengthens regional communities;
- creates incentives for tourism and creative industries;
- forms a bridge with European innovation structures.

For the Moldova-Romania-Ukraine region, the application of the Triple Transition in the field of cultural heritage creates a platform for transnational cooperation, uniting ecological routes, common historical traditions and modern digital practices.

4. Inno4Cult platform as an integration ecosystem: Architecture, mechanisms, regional and transnational cooperation

The development of the Inno4Cult platform represents one of the most ambitious and promising elements of the INNO-CULT project. Unlike traditional digital platforms focused on simply providing access to digital objects or information, Inno4Cult is built as a holistic ecosystem designed to support research, education, cultural and tourism initiatives and regional development. It becomes a tool that connects various spheres of society - culture, education, municipal governance, creative industries, science and civic engagement. In this context, it is important to consider how the project transforms from a technological platform into a multi-level interaction system that unites six development regions of the Republic of Moldova and neighboring regions of Romania and Ukraine. Inno4Cult follows the logic of the Triple Transition, integrating digital, social and environmental aspects into a single methodological model.

4.1. Platform architecture: Structure, principles and key components

The architecture of the Inno4Cult platform is built on four basic principles: multilingualism, interoperability, sustainability and openness. These principles define not only the technical features, but also the conceptual logic of the platform. Multilingualism ensures access to cultural heritage for the inhabitants of Moldova, Romania and Ukraine, as well as for a wider international audience. The platform aims to integrate at least three languages: Romanian, Russian and English, allowing it to encompass the country's main cultural groups and expand beyond its borders. Future plans include the inclusion of Ukrainian and regional dialects, especially in the sections dedicated to oral and intangible heritage. Interoperability refers to the platform's ability to interact with other digital systems - from local museum databases to international platforms such as Europeana, Cultural Gems and Heritage Data Repositories, as well as with regional information resources (e.g. tourism portals). This ensures the platform's flexibility and its ability to be part of an international digital heritage infrastructure.

The openness reflects the FAIR (Findable, Accessible, Interoperable, Reusable) [14] principles and open data. This allows researchers, educators, and NGO representatives to use the platform's materials for their projects, research, and educational programs. Sustainability means that the platform will not be a one-off project. It must have a long-term development strategy, support from partner institutions, technical flexibility and regular content updates. This ensures its long-term value for the regions. Structurally, Inno4Cult includes several key modules:

1. The Digital Archive of Cultural Heritage is a centralized repository of data that includes images, 3D models, audio recordings, ethnographic descriptions, interviews, maps, and interactive elements. This archive is created as a living system, with new materials added as objects are digitized and local communities get involved.
2. Educational module – a set of resources for schools, universities and informal education: lessons, homework, online courses, interactive scenarios, virtual tours and multimedia materials. This module helps educators integrate cultural heritage into the school curriculum.
3. Digital cultural and tourist routes based on GIS technologies and augmented reality. These routes connect heritage sites within regions and across borders, facilitating the development of sustainable cultural tourism.
4. Research tools module, including automatic text analysis, data classification tools, visualization tools, and API sets for scientific projects.
5. A citizen participation platform that allows local residents to create digital stories, upload photos, record traditions, participate in thematic challenges and verified crowdsourcing activities.

Together, these modules create a complex ecosystem, capable of supporting both the "hard" part of cultural heritage (architecture, museum collections) and the "Soft" part (traditions, rituals, oral histories, crafts).

4.2. Integration of the Inno4Cult platform in six development regions of the Republic of Moldova

One of the project's innovations is its focus on regional development. The platform is not designed exclusively for capitals or large cities; instead, it aims to restore the cultural potential of those territories most affected by migration, infrastructure degradation and the loss of local traditions. Each of the six regions will receive:

- a Digital Heritage Lab [15], which functions as a space for learning, research, digitization and social activity;
- local multimedia teams - groups of students, teachers, museum workers and activists who participated in training courses;
- an interactive digital map of the region with historical sites, trails and virtual excursions;
- integrated educational projects in local schools and colleges;
- cultural and tourist products based on digital data - from virtual exhibitions to geolocated audio guides.

This approach sets a precedent for the transition from a centralized model of cultural management to one in which regions become active participants in the process.

Of particular importance is the fact that each digital lab includes equipment for 3D scanning, video and audio recording, data storage and training. This creates the conditions for the professionalization of local staff and the strengthening of the skills necessary for the development of creative industries.

4.3. Cross-border cooperation: Moldova, Romania and Ukraine

The historical and cultural similarities between the three countries create favorable conditions for the development of transnational projects. These territories share a significant overlapping heritage: common historical periods, trade routes, ethnocultural groups and archaeological sites. The Inno4Cult platform envisages the development of cross-border cooperation in three areas:

Collaborative digital collections

Museums, universities and research centres from the three countries will be able to create common databases, linking objects by theme, period or cultural tradition. This is important because many heritage items are scattered between countries due to historical events or migrations.

Cross-border cultural and tourist itineraries

For example, routes along the Dniester River, routes through medieval fortresses, wine, crafts and ancient monasteries. These are created using digital maps, animation and AR technology, being accessible to young people and international tourists.

Educational and research programs

Universities from Moldova, Romania and Ukraine have the opportunity to jointly develop courses on digital heritage, organize summer schools, internships and online courses. This strengthens academic ties and improves the qualifications of specialists.

Thus, the cross-border component of the project transforms the platform into a tool for cultural diplomacy and regional cooperation.

4.4. Support for research, education and infrastructure projects

Inno4Cult is particularly important as an institutional support tool. Unlike isolated initiatives, the platform creates a systematic basis for project development:

Research projects [16]

Open data and analytical tools allow scientists to study:

- historical links between regions;
- transformation of intangible heritage;
- cultural landscapes and their changes;
- social practices of local communities.

Inno4Cult becomes a data source for grants from Horizon Europe, COST, Erasmus+ and national research foundations.

Educational projects [17]

Schools and universities receive:

- digital educational materials,
- online courses,
- virtual tours,
- a platform for project-based learning.

Teachers can use the platform's materials for history, culture, geography, and art lessons.

Infrastructure projects

The digitization of heritage sites contributes to the development of:

- restoration plans,
- museum modernization programs,
- tourist routes,
- interpretation centers,
- cultural centers.

This approach allows regions to develop projects for INTERREG and Creative Europe and connect with youth heritage initiatives such as the European Heritage Youth Ambassadors Programme [18].

4.5. Inno4Cult as a tool for sustainable territorial development

The main function of the platform is not just digitalization, but regional transformation. It stimulates:

- development of local tourism,
- cultural entrepreneurship,
- preservation of intangible traditions,
- increasing cultural literacy,
- youth involvement,
- intercultural dialogue

A dynamic ecosystem is created in which data, people, traditions and technology interact and reinforce each other. Inno4Cult thus sets a new direction for the development of the cultural policy of the Republic of Moldova – from static preservation to active digital and social development.

5. Expected effects and impact assessment: Cultural, social, economic and territorial dimensions

The impact assessment of the INNO-CULT project and the Inno4Cult platform is essential for understanding how the digitisation of cultural heritage can stimulate sustainable development, social inclusion, regional integration and economic modernisation. Although

the project is still in the early stages of development and implementation, it is already possible to identify the areas where its impact will be most visible, as well as to foresee long-term changes at societal and regional level. Unlike traditional projects, where the digitisation of cultural heritage is limited to the creation of online archives or virtual tours, INNO-CULT emphasizes comprehensiveness and interdisciplinary approaches. This allows assessing its impact not only in terms of the volume of digitised objects, but also in terms of regional dynamics, cross-border cooperation, citizen participation, educational potential and innovative development. It is important to note that the Inno4Cult platform is integrated within the Triple Transition framework and is therefore considered a tool for the ecological, digital and social transformation of regions. This approach allows for the analysis of the impact at multiple levels: cultural, social, economic, technological, institutional and international.

5.1. Cultural impact: Conservation, interpretation and accessibility of heritage

The first and most obvious area of impact concerns cultural heritage itself. Digital platforms have long been considered an effective tool for the preservation of cultural assets, but Inno4Cult takes this process to a new level with its multifunctional components.

Conservation and loss prevention

Digitization of heritage sites - architectural monuments, ethnographic collections, texts, audio recordings and household items - helps to stabilize cultural memory, especially in regions facing depopulation or infrastructure degradation. For Moldova, this aspect is of strategic importance: many unique sites are located in rural areas and risk being lost due to lack of resources for restoration. The creation of 3D models, digital twins and high-quality archival materials ensures their preservation and makes future restoration possible even in the event of the physical loss of the original.

Interpreting and changing the approach to heritage

One of the main achievements of digitalization is the opportunity to rethink traditional ways of interpreting cultural heritage. Virtual reconstructions, multimedia routes, augmented reality and interactive maps contribute to the creation of new narratives and the enhancement of the emotional impact of cultural sites. In this sense, the Inno4Cult platform not only documents heritage, but also promotes new ways of understanding it.

Accessibility and democratization of heritage

Given that many museums, archives and cultural sites are located far from population centers, digitization becomes a powerful tool for equal access. The platform makes cultural resources accessible to schoolchildren, people with reduced mobility, seniors, diaspora and international researchers. This democratization of access strengthens cultural identity and promotes the integration of diverse social groups.

5.2. Social impact: Citizen participation, inclusion and community strengthening

The social effects of the project are perhaps the most transformative.

INNO-CULT sees the region's inhabitants not as consumers of cultural products, but as active participants and creators of content. Through digital labs, educational programs, and crowdsourcing initiatives, it promotes a culture of participation - a key feature of social transition.

Involving local communities

Digital Heritage Labs provide a space where schools, NGOs, cultural workers, researchers and local residents can collaborate to create a digital history of their communities. This encourages a sense of responsibility, strengthens intergenerational ties, promotes the transmission of oral traditions and preserves local memory.

Social inclusion and support for vulnerable groups

The use of multimedia formats, audio guides, adaptive interfaces and specialized educational modules makes the platform accessible to a wide range of audiences:

- people with disabilities,
- ethnocultural minorities,
- migrants and returnees,
- young people from rural areas.

This focus on inclusion is in line with the EU's strategic objectives to expand access to cultural resources.

Strengthening local identity and social capital

Citizen involvement in the process of heritage documentation and interpretation promotes social cohesion. Communities that have lost their traditions due to migration and economic instability are given the tools to rebuild cultural ties. This is particularly important for rural areas of Moldova, where cultural practices are often at risk of extinction.

5.3. Economic impact: Boosting tourism and cultural industries

The INNO-CULT project has significant economic prospects, mainly related to the development of sustainable cultural tourism and the stimulation of creative industries.

Sustainable cultural and tourist growth

Digital trails, virtual tours, AR maps, multilingual guides and interactive exhibitions are transforming traditional tourism into a modern, high-quality service. Regional tourist routes that combine natural and cultural attractions create new travel experiences that attract both local and international tourists. This can lead to local economic growth, especially in small towns and rural communities, where tourism is often one of the few sources of income.

Development of creative industries

The digitization of cultural heritage creates opportunities for:

- multimedia content creation;
- development of educational products;
- craft entrepreneurship;
- gastronomic tourism;
- digital animation;
- creating VR games and applications.

This creates a new labor market for young people and supports the development of small businesses.

Increasing the investment attractiveness of regions

Digitization of heritage, especially when combined with ecological and social components, increases the attractiveness of territories for investors and international funds. The Inno4Cult platform simplifies the development of applications for infrastructure projects, allowing regions to participate more actively in EU programs.

5.4. Territorial impact: Regional development and cross-border cooperation

INNO-CULT strengthens territorial connectivity within the Republic of Moldova and between the Republic of Moldova, Romania and Ukraine.

Development of six regions of Moldova

The platform contributes to equalizing territorial disparities by offering regions:

- digital infrastructure,
- educational resources,
- advisory assistance,
- the ability to connect to transnational networks.

Thus, cultural heritage becomes a factor of territorial development, and not just a cultural resource.

Cross-border integration

European cooperation formats, such as INTERREG and Creative Europe, support initiatives aimed at creating transnational routes and shared digital collections. Inno4Cult provides the technical basis for such projects, strengthening cultural ties and stimulating international tourism.

5.5. Institutional and scientific impact

The project contributes to the renewal of the entire cultural heritage management system, forming new standards and models of cooperation.

Strengthening research links

Inno4Cult provides data and tools for research, creates conditions for international projects, and improves the quality of academic publications.

Modernization of cultural institutions

Museums, libraries, archives receive:

- new formats for working with visitors,
- digitization tools,
- projects with social significance.

This increases their sustainability and attractiveness.

5.6. Risks and barriers

Despite the positive effects, the project faces a number of challenges:

- lack of specialists,
- lack of stable financing,
- low digital literacy in some regions,
- personnel migration,
- institutional fragmentation.

However, the experience of European countries shows that these barriers can be overcome with a sustainable platform model and continuous partnerships between the state, universities and NGOs [19].

6. Conclusion and recommendations

The INNO-CULT project and the Inno4Cult platform developed within it represent a unique tool that unites cultural heritage, digital technologies and sustainable development goals. Their significance extends far beyond the simple creation of virtual collections: they become a mechanism for a comprehensive social, economic and territorial transformation, particularly relevant for Moldova and the neighboring regions of Romania and Ukraine. An analysis of national strategies, regional plans and European best practices has shown that the digitization of cultural heritage is a powerful factor of innovative development. European experience with thematic smart specialization platforms demonstrates that the integration of digital technologies with educational and research initiatives contributes to the formation of sustainable cultural and economic ecosystems, which is fully consistent with the concept of the Triple Transition - green, digital and social transformation.

The cultural dimension of the project involves the creation of digital repositories and virtual routes, which ensure the conservation of objects, expand access to them and stimulate the development of cultural identity. The social impact is achieved by involving citizens in the processes of digitization and interpretation of heritage, the creation of digital laboratories, educational programs and crowdsourcing initiatives. This strengthens social cohesion and promotes the inclusion of vulnerable groups.

The economic dimension of the project is achieved through the development of cultural tourism and creative industries, job creation and opening of new markets. The Inno4Cult platform, integrated with transnational programs, provides access to financing and increases the investment attractiveness of the regions. From a geographical point of view, the project contributes to equalizing regional differences and strengthening cross-border

ties, creating the foundation for cultural and economic cooperation. Based on the analysis of international experience, the following key recommendations can be identified:

1. Integrating the Triple Transition approach - developing green tourism, expanding the digital functionality of the platform and actively engaging the public.
2. Development of educational and research components – online courses, digital laboratories, advanced training for cultural and scientific workers, joint projects with EU universities.
3. Support for transnational cooperation – common cultural itineraries, participation in INTERREG and Creative Europe programs, creation of common databases and repositories.
4. Development of digital infrastructure and sustainable financing – cloud solutions, open standards, attracting public and private investments.
5. Performance evaluation and monitoring – quantitative and qualitative indicators of platform usage, economic and social effects.
6. Principles of openness and inclusion - multilingual support, taking into account the needs of different social groups, the possibility of integrating future technologies.

In the long term, the Inno4Cult platform has the potential to become a central infrastructure for cultural, educational and research initiatives in six regions of the Republic of Moldova and neighboring countries, strengthening social cohesion, stimulating economic development and facilitating regional transformation in accordance with the principles of sustainable development. Thus, INNO-CULT is not just a technological project, but a strategic tool for comprehensive development. If all recommendations are implemented, the project is able to create a long-term impact on cultural, social and economic transformation, serving as a model for regions with similar specificities and demonstrating how the digitization of cultural heritage [20] contributes to sustainable development in the 21st century.

References

- [1] Council of Europe, “European Cultural Heritage Strategy for the 21st Century (Strategy 21),” 2017. [Online]. Available: <https://www.coe.int/en/web/culture-and-heritage/strategy-21>
- [2] OECD, Towards a Triple Transition: Strategies for Transformational European Development Action. Paris, France: OECD Publishing, 2023, doi: 10.1787/094322ba-en.
- [3] Ministry of Culture of the Republic of Moldova, “Guvernul Republicii Moldova a aprobat Strategia Națională pentru Cultură și Patrimoniu 2025–2035,” Sep. 24, 2025. [Online]. Available: <https://mc.gov.md/ro/content/guvernul-republicii-moldova-aprobat-strategia-nationala-pentru-cultura-si-patrimoniu-2025>
- [4] Council of the European Union, “Creative Europe programme 2021–2027.” [Online]. Available: <https://www.consilium.europa.eu/ro/policies/creative-europe-2021-2027/>
- [5] Interreg NEXT Romania–Republic of Moldova, “Programme 2021–2027.” [Online]. Available: <https://ro-md.net/en/about-us>
- [6] European Commission, “Europeana platform.” [Online]. Available: <https://digital-strategy.ec.europa.eu/ro/policies/europeana>
- [7] European Commission, Joint Research Centre, “Cultural Gems,” Knowledge4Policy, 2025. [Online]. Available: https://knowledge4policy.ec.europa.eu/projects-activities/cultural-gems_en
- [8] Heritage Innovation, “Digital meets heritage meets innovation.” [Online]. Available: <https://heritageinnovation.eu/>

- [9] Parliament of the Republic of Moldova, Law No. 315, “Strategia națională de dezvoltare «Moldova Europeană 2030»,” Nov. 17, 2022. [Online]. Available: https://anpcv.gov.md/sites/default/files/2024-10/Legea%20315_Moldova%20europeana%202030.pdf
- [10] European Commission, “Cluster 2: Culture, creativity and inclusive society,” Horizon Europe. [Online]. Available: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-2-culture-creativity-and-inclusive-society_en
- [11] European Commission, Directorate-General for Regional and Urban Policy, “Cultural and creative regional ecosystems,” Smart Specialisation. [Online]. Available: https://ec.europa.eu/regional_policy/policy/communities-and-networks/s3-community-of-practice/partnership_industrial_mod_cultural_and_creative_regional_ecosystems_en
- [12] European Commission, Interoperable Europe Portal, “Bologna’s digital twin: Enhancing decisions and citizen engagement.” [Online]. Available: <https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/bolognas-digital-twin-enhancing-decisions-and-citizen-engagement>
- [13] L. Schmerber, “Triple transition and corporate responsibility – a new framework for businesses,” Interreg Europe, 2024. [Online]. Available: <https://www.interregeurope.eu/policy-learning-platform/news/triple-transition-and-corporate-responsibility-a-new-framework-for-businesses>
- [14] H. Lowenthal et al., JRC FAIR Data Guidelines. Luxembourg: Publications Office of the European Union, 2025, JRC140764, doi: 10.2760/5646214.
- [15] Digital Heritage Research Laboratory, Cyprus University of Technology, “Mnemosyne.” [Online]. Available: <https://erachair-dch.eu/>
- [16] Heritage Research Hub, “Heritage projects.” [Online]. Available: <https://www.heritageresearch-hub.eu/heritage-projects/>
- [17] Heritage Innovation, “C4Education.” [Online]. Available: <https://heritageinnovation.eu/c4education/>
- [18] Europa Nostra, ESACH, and European Heritage Tribune, “European Heritage Youth Ambassadors Programme.” [Online]. Available: <https://www.youth-heritage-europe.org/ehya.html>
- [19] AO “Be Up,” “Public Association.” [Online]. Available: <https://aobeup.org/>
- [20] A. Babin, E. Prus, and E. Margineanu, “Access to the European cultural heritage of settlements and towns in the Danube macro-region through interoperable strategies digital transformation,” *Smart Cities and Regional Development*, vol. 8, no. 3, pp. 79–95, 2024, doi: 10.25019/14fmmn81.

Utilizarea IA în sistemele judiciare: De la asistență documentară la managementul jurisdicțional

Sebastian AVĂCĂRIȚEI

*Alexandru Ioan Cuza University of Iași, Faculty of Economics and Business Administration
Iași, Romania
sebastian.avacaritei24.07@gmail.com*

Mihaela TOFAN

*Alexandru Ioan Cuza University of Iași, Faculty of Economics and Business Administration
Iași, Romania
mtofan@uaic.ro*

Abstract

Transformarea digitală aduce instrumente de inteligență artificială (IA) în ecosistemul judiciar cu o gamă largă de utilizări: de la asistență documentară (căutare, clasificare, rezumatizare, anonimizare) până la sprijin pentru managementul jurisdicțional (planificare, alocare a resurselor, sortare administrativă) și, la limită, la analize care pot influența evaluarea probelor și rezultatul cazurilor. În acest context, articolul propune un cadru integrat pentru guvernarea judiciară a IA, aliniat cu Regulamentul (UE) 2024/1689 (AI Act), care combină clasificarea riscurilor, alfabetizarea personalului în IA, auditul (înregistrare, trasabilitate) și explicabilitatea deciziilor automate, cu scopul explicit de a menține legitimitatea luării deciziilor umane. Din perspectivă metodologică, articolul cartografiază utilizările judiciare ale IA în raport cu clasificarea riscurilor din Legea AI și extrage obligațiile aferente (transparență, supraveghere umană, evaluare și atenuare a riscului, jurnale de evenimente), cu accent pe primele prevederi deja operaționale (alfabetizarea IA și practicile interzise). Contribuția centrală este un model de "guvernare judiciară a inteligenței artificiale" care include: registrul utilizărilor IA și matricea de risc; evaluări algoritmice ale impactului; politici de jurnalizare și explicabilitate adecvate publicului țintă (judecători/grefieri/părți); mecanisme de contestare și remediere; comitetul mixt juridic-tehnic-etic; programe de alfabetizare în IA adaptate rolurilor profesionale. Articolul derivă seturi de indicatori (rata intervențiilor umane, calitatea motivației, incidentele de părtinire și contestare) și elaborează ghiduri pentru integrarea AI fără a compromite garanțiile procedurale (principiul contradictorialității, publicitatea și dreptul la apărare). Modelul urmărește integrarea etapizată, documentată și auditabilă a acestor instrumente în instanțe. Concluzia este că legitimitatea deciziei umane nu rezultă din absența inteligenței artificiale, ci din proiectarea și guvernarea acesteia astfel încât controlul și responsabilitatea să revină, în mod verificabil, judecătorului.

Cuvinte cheie: guvernare judiciară; transparență; evaluarea impactului; supraveghere umană

1. Introducere

1.1. Context și motivație

Tehnologiile AI se regăsesc deja în asistența documentară (căutare juridică, clasificare a documentelor, rezumare automată), în managementul administrativ al fluxurilor de cazuri și în anumite proiecte pilot în instrumente care pot influența evaluarea probelor sau recomandarea soluțiilor. Firească din perspectiva eficienței, introducerea IA ridică totuși întrebări esențiale: cum să se păstreze principiul adversarialității, publicității și dreptul la un proces echitabil? Cum revine responsabilitatea finală judecătorului, dacă algoritmi contribuie la decizie? Aceste preocupări sunt împărtășite de literatura specializată recentă, care subliniază necesitatea de a echilibra eficiența cu respectul drepturilor fundamentale. [1], [2], [3], [4]

Regulamentul (UE) 2024/1689 (așa-numita Lege a IA) impune o arhitectură de reglementare bazată pe risc; anumite utilizări ale inteligenței artificiale în domeniul justiției pot fi încadrate ca "cu risc ridicat" și sunt supuse unor obligații specifice. Carta etică CEPEJ (2018) subliniază, la rândul său, principalele principii care trebuie respectate atunci când se folosește IA în justiție: respectarea drepturilor fundamentale, transparența, nediscriminarea și controlul uman asupra deciziei. De asemenea, GDPR (Reg. 2016/679) rămâne relevant în ceea ce privește protecția datelor personale și drepturile persoanei, deoarece prevede, printre altele, dreptul de a nu fi supusă unei decizii bazate exclusiv pe prelucrare automată, care produce efecte legale asupra persoanei sau o afectează semnificativ (art. 22). [5], [6], [7], [8], [9], [10]

2. Metodologie

Studiul de față folosește o abordare doctrinară-normativă combinată a reglementărilor relevante (Legea AI și Carta CEPEJ), combinată cu o cartografiere a utilizărilor IA în justiție. Riscurile asociate fiecărui tip de utilizare au fost identificate, iar obligațiile legale aplicabile au fost extrase. Pe această bază, a fost dezvoltat un model de guvernanta judiciară a IA, compus din elemente operaționale concrete și indicatori măsurabili ai conformității.

Abordarea are un caracter predominant conceptual și normativ. Recomandările propuse trebuie validate și calibrate prin teste empirice, în cadrul proiectelor pilot și adaptate în funcție de resursele instituționale disponibile. De asemenea, analiza nu abordează în detaliu diferențele de implementare la nivelul fiecărei jurisdicții naționale, ci propune un cadru general aplicabil în contextul sistemului judiciar român, în conformitate cu reglementările europene.

3. Reglementarea Europeană: Extrase relevante din Legea AI

3.1. Lista utilizărilor considerate cu risc ridicat (Extras din AI Act, rezumat EUR-Lex)

"Regulamentul definește utilizarea IA în următoarele domenii ca fiind cu risc ridicat, din cauza impactului potențial asupra drepturilor fundamentale, siguranței și bunăstării: ... Legii... administrarea justiției și procesele democratice, sisteme AI folosite de autoritățile judiciare pentru cercetare și interpretare juridică sau sisteme care ar putea influența rezultatele alegerilor." [5]

Conform Legii AI, sistemele IA utilizate în administrarea justiției (de exemplu, de către instanțe, pentru documentație juridică, interpretarea legii sau aplicarea legii la fapte) se încadrează în categoria "cu risc ridicat", la fel ca și cele utilizate în procesele democratice (de exemplu, pentru a influența rezultatul alegerilor). Acest fapt necesită respectarea cerințelor stricte prevăzute de reglementarea pentru astfel de sisteme. [5]

3.2. Practici interzise ale IA (Risc inacceptabil - Extras din Legea AI, Rezumatul EUR-Lex)

"Regulamentul interzice următoarele practici AI cu un nivel inacceptabil de risc: Tehnici subliminale sau înșelătoare pentru manipularea comportamentului individual sau de grup; Exploatarea vulnerabilităților bazate pe vârstă, dizabilitate sau situații socioeconomice;

Punctaj social; Evaluarea riscului penal, care prezice probabilitatea de a comite o infracțiune doar pe baza profilării sau a trăsăturilor de personalitate; Colectarea bazei de date cu recunoaștere facială ... Deducerea emoțiilor în domenii sensibile (locuri de muncă, instituții de învățământ)." [5]

Cu alte cuvinte, Legea AI interzice comercializarea sau utilizarea sistemelor AI care recurg la: (a) tehnici subliminale sau înșelătoare pentru manipularea comportamentului, (b) exploatarea vulnerabilităților legate de vârstă, dizabilitate sau statut socioeconomic, (c) evaluarea socială a indivizilor, (d) evaluarea riscului criminalității (predicția recidivei) bazată pe profilarea automată a individului, (e) extinderea neîntită a bazelor de date de recunoaștere facială prin extragerea imaginilor de pe Internet, și (f) detectarea emoțiilor în contexte sensibile (la locul de muncă, la școală etc.). Toate aceste practici sunt considerate a avea un nivel inacceptabil de risc și, prin urmare, sunt complet interzise de reglementare. [5]

3.3. Obligații pentru sistemele AI cu risc ridicat

Pentru sistemele AI clasificate ca risc ridicat, Legea AI prevede o serie de obligații specifice, menite să asigure utilizarea lor în condiții legale și etice de siguranță. În esență, trebuie implementate următoarele: (i) un sistem de management al riscului pe tot parcursul ciclului de viață al sistemului, de natură iterativă și actualizat periodic; (ii) garanții privind calitatea datelor utilizate și evitarea discriminării – de exemplu, seturile de date de antrenament trebuie să fie relevante, reprezentative și cât mai complete și fără erori posibil, pentru a reduce biasurile algoritmice; (iii) mecanisme de păstrare a evidențelor (jurnale) pentru auditarea evenimentelor și trasabilitatea deciziilor AI; (iv) asigurarea unei supravegheri umane eficiente, adică sistemul este proiectat astfel încât operatorul uman să poată monitoriza și corecta eficient funcționarea acestuia; (v) transparență față de utilizatori (implementatori) și, după caz, față de persoanele afectate de deciziile luate cu ajutorul AI. De exemplu, sistemele AI cu risc ridicat ar trebui să fie însoțite de instrucțiuni clare de utilizare și informații despre capabilitățile și limitările lor, pentru a permite utilizatorilor să interpreteze corect rezultatele. În anumite situații, persoanele afectate de deciziile automate trebuie să fie informate despre rolul AI. Toate aceste cerințe sunt menite să mențină controlul și responsabilitatea față de actorii umani, chiar și atunci când folosesc instrumente automate. [5], [5], [5], [5], [11], [5], [12], [13]

4. Cartografierea utilizărilor IA în justiție și evaluarea riscurilor

4.1. Utilizări și riscuri

Pentru a înțelege impactul IA în sistemul judiciar, am cartografiat principalele tipuri de utilizări posibile și nivelurile lor de risc asociate, în concordanță cu categoriile din Legea AI și din literatura de specialitate: [2]

Suport pentru documente (de exemplu, căutare în jurisprudență, rezumare automată, anonimizare a documentelor): risc scăzut spre mediu. Beneficiile sunt legate de eficiența procesării informațiilor, dar există riscul unor erori de acuratețe (de exemplu, omisiunea surselor relevante sau a rezumatelor inexacte) și a posibilei opacități în modul în care se

obțin rezultatele. Este necesară verificarea umană a informațiilor furnizate de sistem. Suport administrativ (de exemplu, sortare automată a cazurilor, randomizare a cazurilor, gestionarea agendei): risc mediu, care poate deveni ridicat dacă sistemul are un grad ridicat de automatizare fără intervenție umană. Impactul negativ poate fi asupra accesului egal la justiție (dacă, de exemplu, sortarea favorizează sau dezavantajează anumite categorii de cazuri sau persoane) și asupra principiului atribuirii aleatorii. [6]

Sprijin în luarea deciziilor judiciare (de exemplu, instrumente de evaluare a probelor, sisteme pentru prezicerea rezultatului proceselor sau recomandarea sancțiunilor): risc ridicat. Aceste utilizări se încadrează clar în sfera cu risc ridicat definită de Legea AI și necesită respectarea tuturor obligațiilor legale – evaluarea riscurilor, înregistrarea, supravegherea umană strictă etc. Anumite utilizări de acest tip pot fi chiar considerate inacceptabile sau interzise, dacă tind să înlocuiască rolul decizional al judecătorului (de exemplu, un algoritm care decide sentința ar încălca principiul independenței judecătorului). [14], [15], [16], [6], [17]

Per ansamblu, gradul de risc crește pe măsură ce AI trece de la roluri de suport (documentație, administrație) la roluri jurisdicționale directe. Prin urmare, nivelul de reglementare și supraveghere trebuie să crească proporțional.

5. Modelul de guvernare propus pentru AI în justiție

5.1. Principii Călăuzitoare (Normative-Etice)

Având în vedere riscurile și cerințele identificate, propunem un model de guvernare care combină principiile normative cu proceduri operaționale concrete. Scopul este integrarea responsabilă a IA în actul judiciar, fără a compromite garanțiile procedurale și păstrând întotdeauna decizia finală în mâinile judecătorului.

Modelul se bazează pe următoarele principii, aliniate atât cu cerințele legale, cât și cu cele etice:

- Conformitate cu Legea IA – Orice sistem AI folosit în justiție trebuie să respecte pe deplin Regulamentul (UE) 2024/1689 și categoria de risc aferente. [5]
- Respectul pentru drepturile fundamentale și principiile CEPEJ – Fiecare implementare AI trebuie evaluată în raport cu Carta CEPEJ (2018), care pune accent: pe respectul drepturilor omului, nediscriminarea, imparțialitatea și controlul utilizatorilor umani asupra deciziei. [6]
- Proportionalitate și transparență – Introducerea unui instrument bazat pe IA trebuie să fie proporțională cu problema pe care o rezolvă și să fie însoțită de transparență. Orice intervenție a IA în procesul judiciar va fi cunoscută părților și justificată prin eficiența sau acuratețea pe care o aduce, fără a afecta drepturile procedurale.
- Control uman eficient – În toate cazurile, un judecător (sau personalul uman desemnat) trebuie să aibă o oportunitate reală de a supraveghea, valida sau infirma rezultatul oferit de AI. Responsabilitatea deciziei judiciare revine întotdeauna omului, AI-ul având doar un rol consultativ sau auxiliar.

Prin aceste principii ne asigurăm că legitimitatea deciziei judiciare este menținută, IA fiind un instrument subordonat scopului justiției, nu un factor autonom de luare a deciziilor.

5.2. Componente cheie ale Cadrului de Guvernanță

Pentru a pune în aplicare principiile de mai sus, modelul propune următoarele componente instituționale și procedurale:

- Registrul Central al Aplicațiilor AI – O bază de date națională pentru înregistrarea tuturor aplicațiilor AI utilizate în sistemul judiciar. Metadatele esențiale pentru fiecare aplicație vor fi înregistrate: scopul, domeniul de utilizare (documentar/administrativ/judiciar), clasificarea riscului (conform AI Act), versiunea algoritmului, furnizorul, evaluările impactului (dacă sunt realizate) etc. Acest registru central asigură vizibilitate și trasabilitate.
- Evaluări Algoritmice ale Impactului (AIA) – Implementarea standardizată a evaluărilor de impact înainte de punerea în funcțiune a unui sistem AI. Evaluarea Impactului Algoritmice va analiza potențialele părtiniri, riscurile legate de drepturi (de exemplu, nediscriminarea, confidențialitatea), măsurile de atenuare. Se recomandă ca rezumatul non-tehnic al fiecărei evaluări să fie făcut public pentru transparență.
- Politici stricte de jurnalizare – Pentru sistemele cu risc mediu sau ridicat, este necesar să păstreze fișiere de jurnal care să includă date de utilizare: timestamp-uri, date relevante de intrare și ieșire, intervenții umane (dacă există), parametri de sistem. Accesul la aceste jurnale trebuie reglementat: disponibil pentru audit intern, pentru inspecții de către autoritățile competente și, într-o formă adecvată, pentru părțile care contestă soluții generate de AI. [11], [18], [19]
- Cerințe de explicabilitate – Modelul oferă două niveluri de explicabilitate: explicabilitate tehnică (pentru judecători și experți IT, care pot primi documentație detaliată despre funcționarea, performanța și limitele algoritmului) și explicabilitatea accesibilă (pentru părți litigante și public, adică explicații în limbaj comun despre rolul AI în proces și modul în care aceasta a influențat decizia, dacă există).
- Mecanisme de apel și reparare – Stabilirea unei proceduri clare prin care litiganții pot contesta utilizarea sau rezultatul oferit de un sistem AI. De exemplu, o parte care consideră că a fost dezavantajată de o recomandare algoritmică poate depune o cerere pentru revizuire umană a acelei analize. În cazul unei erori demonstrate ale AI, trebuie să fie disponibile mecanisme disciplinare sau remediale (inclusiv rejudicare).
- Comitet central tehnic-juridic-etic – Recomandăm înființarea unui organism colegial (posibil sub auspiciile CSM sau MJ) pentru a supraveghea guvernanța IA. Comitetul ar include judecători, specialiști IT, experți în etică, reprezentanți ai societății civile și, posibil, Autoritatea Națională de Supraveghere a Procesării Datelor (ANSPDCP). Acest comitet ar aproba introducerea noilor sisteme AI, ar revizui rapoartele și incidentele de audit și ar emite recomandări de politici.
- Programe de formare – O componentă fundamentală este alfabetizarea digitală a personalului judiciar. Judecătorii, grefierii, avocații ar trebui să participe la instruire privind elementele de bază ale inteligenței artificiale, interpretarea

rezultatelor algoritmului, potențialele erori și prejudecăți, precum și procedurile de urmat atunci când interacționează cu astfel de instrumente. Aceste programe ar crește încrederea și competența profesională în contextul noilor tehnologii.

- **Audit extern periodic** – Pe lângă monitorizarea internă, modelul prevede audituri independente (efectuate de echipe mixte de profesioniști IT și avocați externi) cel puțin anual, cu publicarea rapoartelor sumare. Auditul va verifica conformitatea sistemelor AI cu obligații legale (de exemplu, dacă un sistem cu risc ridicat are jurnale în ordine, dacă îndeplinește acuratețea declarată etc.) și va oferi recomandări.

Aceste componente, implementate împreună, creează un ecosistem de încredere în utilizarea AI: transparență, control și responsabilitate pe tot parcursul ciclului de viață al algoritmilor în justiție. [20], [21], [22]

5.3. Proceduri operaționale

Pe baza componentelor de mai sus, fluxul procedural pentru introducerea și utilizarea unui sistem AI în instanțe ar putea fi următorul:

1. **Înregistrare inițială:** Orice proiect care implementează un instrument AI este înregistrat în Registrul Central al Aplicațiilor AI, cu o descriere detaliată a scopului și funcționalităților sale.
2. **Evaluare preliminară și opinie:** Se desfășoară o Evaluare Algoritmăică a Impactului (AIA). Raportul AIA este trimis Comitetului Central (CN-GIAJ) pentru opinie. Comitetul poate solicita clarificări, teste suplimentare sau poate impune anumite condiții de utilizare.
3. **Pilot controlat:** Dacă este aprobat, sistemul AI este implementat inițial într-un program pilot (pentru o perioadă limitată într-o instanță sau departament specific), cu monitorizare intensivă. În această fază sunt colectate jurnale și feedback de la utilizatori.
4. **Audit independent:** La finalul fazei pilot, un auditor extern analizează performanța sistemului, conformitatea cu măsurile de reducere a riscului și incidentele.
5. **Aprobarea finală:** Pe baza raportului de audit, Comitetul Central decide dacă sistemul poate fi extins la scară largă. Aprobarea poate fi supusă unor condiții (de exemplu, reevaluarea în 6 luni, îmbunătățiri tehnice necesare etc.).
6. **Implementare operațională:** Sistemul este folosit conform scopului său inițial, în conformitate cu politicile de jurnalizare și transparență. Dacă AI-ul a jucat un rol semnificativ într-un caz (de exemplu, a generat o recomandare de rezolvare), acest lucru ar trebui menționat explicit în hotărârea instanței sau în notele dosarului, inclusiv într-un rezumat al modului în care a fost folosită recomandarea.
7. **Monitorizare continuă:** Indicatorii cheie sunt urmăriți și raportați trimestrial Comitetului Central. Orice incident (eroare, bias raportat, defecțiune) este înregistrat într-un Registru de Incidente AI și declanșează procedura de analiză.
8. **Mecanism de contestare pentru părți:** Dacă o parte implicată într-un proces consideră că a fost nedreptățită sau afectată de utilizarea AI, poate depune o plângere printr-un formular electronic dedicat. Reevaluarea umană a aspectului contestat este asigurată în maximum 30 de zile, iar dacă problema este confirmată, se iau măsuri corective (de

exemplu, excluderea acelei analize AI din raționamentul soluției, reevaluarea dacă este necesar, îmbunătățirea algoritmului pentru viitor).

9. Raportare și revizuire: Anual, se publică un raport sumar (de către CSM sau altă autoritate desemnată) privind utilizarea IA în sistemul judiciar, incluzând statistici, beneficiile observate, problemele întâlnite și planul de acțiune pentru anul următor.

Aceste proceduri creează un ciclu de viață al proiectelor AI, de la idee la evaluare, implementare și feedback, asigurând astfel îmbunătățirea continuă și adaptarea la contextul legal și tehnologic în evoluție.

6. Indicatori de monitorizare

6.1. Indicatori primari

Pentru a evalua eficacitatea și siguranța utilizării IA în justiție, propunem un set de indicatori cheie de performanță și conformitate. Acești indicatori trebuie monitorizați continuu și raportați periodic factorilor de decizie.

- Rata de intervenție umană (RIU): Procentul cazurilor în care operatorul uman (judecător sau personal) a modificat sau respins recomandarea oferită de AI. Un RIU foarte scăzut (de exemplu $< 5\%$ pe o perioadă de 6 luni) ar putea indica fie că AI-ul ia decizii impecabile, fie (mai periculos) că oamenii au devenit excesiv de dependenți de recomandări și nu mai exercită un control critic. Un prag de alertă ar fi $RIU < 5\%$, caz în care ar fi necesară o investigație a Comitetului Central privind calitatea supravegherii umane.
- Rata de transparență în raționament (RTM): Procentul deciziilor instanțelor în care utilizarea unui instrument AI este menționată explicit, când a avut un rol semnificativ în rezolvarea cazului. Ținta trebuie să fie 100% – orice influență a IA asupra luării deciziilor trebuie documentată public. Un RTM sub 100% indică deficiențe de documentație sau transparență care trebuie corectate.
- Incidente AI la 10.000 de cazuri: Numărul incidentelor legate de utilizarea AI (erori majore, părtinire dovedită, breșe de securitate a datelor, plângeri ale părților) raportate pentru fiecare 10.000 de cazuri rezolvate. Atât numărul absolut, cât și tipul incidentelor (tehnice vs. legale sau etice) sunt urmărite. O tendință în creștere impune o reevaluare urgentă a modului în care este utilizată inteligența artificială.
- Timpul mediu de răspuns la sesizările privind IA (TMR): Timpul mediu (în zile) necesar autorităților judiciare pentru a procesa și răspunde la sesizarea unei părți referitoare la utilizarea AI. Ținta propusă este ≤ 30 de zile pentru a asigura remedieri rapide.
- Scorul de calitate al raționamentului (SQM): Un indicator calitativ rezultat din auditurile hotărârilor privind AI, care evaluează coerența juridică a raționamentului, justificarea critică a judecătorului și integrarea adecvată a inputului AI (dacă există). De exemplu, s-ar putea evalua calitatea raționamentului de la 1 la 5, unde 5 înseamnă o decizie excelent argumentată, în care judecătorul folosește informațiile furnizate de AI (dacă au fost folosite) critic, fără a renunța la rolul său.

Acești indicatori trebuie interpretați ca un întreg, nu izolați. Scopul este de a detecta deviațiile timpurii: de exemplu, un RIU foarte scăzut combinat cu un SQM scăzut ar ridica un semnal de alarmă (posibilă dependență excesivă de AI și scăderea calității deliberatiei umane).

6.2. Modul de raportare

Indicatorii vor fi raportați după cum urmează:

- Rapoarte trimestriale interne: către Comitetul Central de Guvernanță a IA (CN-GIAJ), conținând valorile indicatorilor, explicații pentru posibile abateri și măsuri propuse.
- Raport public anual: către Consiliul Superior al Magistraturii (CSM) și publicul larg, incluzând un rezumat al datelor anuale, tendințele, exemple de bune practici și planul de acțiune. Acest raport anual asigură transparența externă și responsabilitatea publică privind modul în care AI este integrată în justiție.
- Notificări către autoritățile europene: Conform Legii AI, în situațiile în care apar incidente grave sau când anumite praguri critice sunt depășite, autoritățile naționale (de exemplu, autoritatea de supraveghere a pieței pentru IA) trebuie să notifice instituțiile europene relevante. Modelul prevede că Comitetul Central este responsabil pentru coordonarea acestor notificări, asigurându-se că România își îndeplinește obligațiile de cooperare la nivelul UE.

Prin monitorizare riguroasă și raportare, învățarea instituțională devine posibilă: sistemul judiciar își poate ajusta continuu politicile de IA, menținând totodată alinierea cu principiul procesului echitabil.

7. Garanții procedurale și considerente etice

7.1. Principiul contradictorialității și explicabilitatea

Integrarea IA în actul judiciar nu trebuie să submineze garanțiile fundamentale ale procesului judiciar. În această secțiune discutăm cum modelul propus se raportează la principiile adversarialității, drepturilor de apărare și publicității, precum și importanța acestor principii în contextul inteligenței artificiale.

Principiul adversarialității impune ca toate probele și argumentele relevante într-un proces să fie cunoscute și accesibile părților, astfel încât să poată fi contestate. Prin urmare, dacă un algoritm AI oferă o analiză sau o recomandare luată în considerare de judecător, concluziile algoritmului trebuie comunicate părților și supuse dezbaterii adversariale. Cu alte cuvinte, părțile au dreptul să știe dacă și cum AI-ul a contribuit la soluția propusă și să aibă oportunitatea de a o contesta sau susține, după caz. Carta CEPEJ subliniază că utilizarea instrumentelor de inteligență artificială nu trebuie să submineze garanțiile dreptului la un proces echitabil – inclusiv egalitatea armelor și adversarialitatea. [6], [6]

În practică, explicabilitatea tehnologiei devine premisa adversarialității: sistemul AI trebuie să ofere o explicație inteligibilă a rezultatului său (sau să permită expertului uman să o explice), astfel încât avocații și judecătorii să poată înțelege raționamentul și să-l discute în

instanță. De exemplu, dacă software-ul sugerează o anumită jurisprudență ca fiind relevantă, partea adversă trebuie să poată verifica acea jurisprudență și să argumenteze împotriva ei. Modelul de guvernare propus stipulează explicit obligația de a menționa utilizarea IA în motivație și de a oferi explicații în înțelegerea părților, tocmai pentru a respecta acest principiu. [23], [24], [6], [8]

7.2. Dreptul la apărare și responsabilitatea judecătorului

Dreptul la apărare al părților presupune că fiecare parte poate contesta efectiv acuzațiile și probele prezentate împotriva sa și că are acces la o decizie rațională luată de un judecător independent. Introducerea AI-ului nu trebuie în niciun fel să creeze o "cutie neagră" inaccesibilă apărării. Prin urmare, orice recomandare a unui AI folosit în fișier trebuie nu doar comunicată, ci și explicată în limbaj juridic. Judecătorul rămâne deținătorul deciziei; Recomandările AI sunt instrumente auxiliare – nu delegarea autorității. Această distincție este crucială: judecătorul poate accepta sau ignora sugestia AI-ului, dar nu poate fi subordonat acesteia.

În situațiile în care utilizarea IA ar duce la o eroare sau o părtinire (de exemplu, dacă un algoritm are o părtinire sistematică împotriva unui grup și influențează negativ o decizie), mecanismele remediale trebuie să permită corectarea deciziei și chiar rejudecarea cauzei, pentru a proteja drepturile părții vătămate. Responsabilitatea finală aparține judecătorului, astfel încât orice eroare a AI-ului integrată în raționament devine o eroare a instanței, care poate fi atacată prin mijloace obișnuite de apel (apel, apel). Modelul propus de guvernare, prin proceduri de apel și intervenție umană, asigură că dreptul la apărare nu este golit de conținut în era digitală.

7.3. Publicitate și încredere publică

Publicitatea audierilor judiciare și transparența actului judiciar sunt pietre de temelie pentru încrederea publică în sistemul judiciar. Dacă instanțele ar folosi AI în secret, fără știrea părților și a publicului, ar crea un risc major de neîncredere și teorii ale conspirației despre "justiția algoritmică". Transparența privind rolul AI în rezolvarea cazurilor este, prin urmare, esențială. Modelul necesită menționarea în hotărâre când un instrument automatizat a contribuit la analiză, precum și publicarea periodică a rapoartelor privind utilizarea AI.

Această abordare proactivă a transparenței urmărește să prevină percepția că IA este un factor de decizie ascuns. Dimpotrivă, folosită corect, IA poate crește încrederea dacă se dovedește că ajută la coerența practicii judiciare, viteza și accesul la informații. Cheia este că utilizarea nu este secretă: doar prin cunoașterea și înțelegerea modului în care AI contribuie la justiție poate publicul (și părțile) să evalueze obiectiv valoarea adăugată sau riscurile posibile. Transparența devine astfel nu doar o obligație legală (conform Legii AI), ci și o strategie de comunicare pentru sistemul judiciar pentru a cultiva încrederea publică.

8. Conformitatea cu Legea AI: Prevederi esențiale explicate

8.1. Practici interzise (Legea AI, art. 5) și relevanță juridică

Legea AI interzice anumite practici IA considerate de risc inacceptabil. Dintre acestea, relevante pentru domeniul judiciar se numără profilarea în scopul "scorului" social și evaluarea automată a riscului penal.

Textul oficial al regulamentului afirmă explicit că este interzisă utilizarea IA pentru a evalua sau clasifica persoane fizice pe baza comportamentului social sau a caracteristicilor personale, atunci când acest lucru conduce la scoruri sociale și tratamente nefavorabile (Parlamentul European & Consiliul, 2024). Prin analogie, orice sistem de "evaluare" al litiganților (de exemplu, un algoritm care ar sugera soluția în funcție de istoricul procedural al părții) ar intra sub această interdicție. Regulamentul interzice, de asemenea, sistemele AI folosite pentru a prezice probabilitatea comiterii unei infracțiuni pe baza profilului unei persoane. Aceasta înseamnă că instrumentele de poliție predictivă sau evaluările automate ale recidivei nu pot fi folosite ca atare în luarea deciziilor penale – ar încălca dreptul la un proces echitabil și prezumția de nevinovăție. [5]

Interpretare: În sistemul judiciar, interdicțiile AI Act impun evitarea oricăror utilizări a IA care ar duce la profilarea punitivă sau evaluarea persoanelor implicate în proces. Orice încercare de a introduce un "indice de pericolitate" automat ar fi împotriva atât a reglementării, cât și a principiilor dreptului penal. De asemenea, inferența emoțiilor oamenilor într-un context judiciar (de exemplu, un AI care "citește" emoțiile unui martor pentru a decide credibilitatea) intră în zona interzisă, interdicția de a deduce emoții în zone sensibile fiind menționată explicit. Astfel, introducerea IA în justiție trebuie să se concentreze pe instrumentele permise (de exemplu: asistență pentru documentare) și să evite clar practicile interzise. [5]

8.2. Cerințe pentru sisteme cu risc ridicat (Legea AI, art. 9–15) – Aplicare

După cum s-a menționat, Legea AI impune sistemelor AI cu risc ridicat o serie de cerințe tehnice și organizaționale: managementul riscului, calitatea datelor, înregistrarea, supravegherea umană, transparență, precum și înregistrarea acestor sisteme într-o bază de date europeană. În domeniul justiției, orice algoritm suficient de avansat pentru a influența o decizie judiciară va fi aproape sigur considerat cu risc ridicat (câmpul "administrarea justiției" este listat ca atare). [5]

În practică, acest lucru se traduce astfel: înainte de implementare, instanța sau Ministerul Justiției (ca furnizor sau implementator al sistemului) trebuie să stabilească un sistem de gestionare a riscurilor pentru acea IA – identificând riscurile posibile pentru drepturile părților și modul de a le atenua (de exemplu, dacă un algoritm de căutare juridică ar putea omite jurisprudența relevantă, este oferită procedura suplimentară de verificare manuală). Calitatea datelor trebuie de asemenea asigurată: dacă un model este antrenat pe baza deciziilor judiciare anterioare, acele date trebuie să fie curate și reprezentative pentru a nu

induce părtinire (de exemplu, dacă într-un anumit caz practica anterioară a fost neuniformă sau părtinitoare, algoritmul antrenat exclusiv pe aceasta ar putea reproduce acea părtinire) [5], [12].

Jurnalizarea este esențială: sistemul trebuie să poată înregistra automat evenimentele de utilizare pentru a permite auditarea. Legea AI prevede, de exemplu, că pentru sistemele de justiție cu risc ridicat jurnalele trebuie să înregistreze cel puțin durata fiecărei utilizări, datele de intrare care au generat un anumit rezultat și identificarea persoanei care a supravegheat rezultatul. Aceasta corespunde măsurilor propuse în modelul nostru, unde am specificat conținutul jurnalelor. [5]

Supravegherea umană trebuie să fie integrată prin design: art. 14 din Legea AI stipulează că sistemele AI cu risc ridicat trebuie proiectate pentru a permite o supraveghere eficientă de către oameni. Aceasta înseamnă interfețe care oferă judecătorului suficientă vizibilitate și control: de exemplu, capacitatea de a vedea justificarea pentru predicția unui algoritm, de a corecta datele de intrare sau de a opri operația automată dacă se observă o problemă.

Nu în ultimul rând, transparența față de utilizatori (judecători/grefieri) implică oferirea de instrucțiuni detaliate pentru utilizatori și informarea clară a celor care folosesc sistemul despre capacitățile și limitările acestuia. Într-un context judiciar, acest lucru ar lua forma unor ghiduri practice pentru magistrați despre cum să folosească (și să nu) o anumită inteligență artificială, ce poate și ce nu poate face acea inteligență artificială etc. [5]

Orice algoritm care poate influența soluția într-un dosar trebuie tratat ca un sistem cu risc ridicat, cu toate măsurile stricte: analiză anterioară, monitorizare atentă și control uman permanent. Numai astfel putem asigura că IA acționează ca un aliat al justiției și nu ca un factor opac sau incontrollabil.

8.3. Menționarea expresă a domeniului justiției în lista utilizărilor cu risc ridicat

Legea AI listează explicit "administrarea justiției" în Anexa III ca o zonă cu risc ridicat a utilizării AI. Această includere are implicații directe: toate aplicațiile AI folosite de autoritățile judiciare intră ipso facto în sfera cu risc ridicat (cu excepția celor pur administrative fără impact asupra drepturilor – dar chiar și acolo, granița este fluidă). [5]

Pentru România, aceasta înseamnă că, odată ce Legea AI va deveni aplicabilă (probabil în 2025-2026, având în vedere că a intrat în vigoare la 1 august 2024, cu o perioadă de grație), instanțele vor fi obligate legal să respecte cerințele menționate mai sus. Nerespectarea acestora ar putea atrage sancțiuni, inclusiv amenzi la nivel UE (Legea AI prevede un regim de conformitate și sancțiuni asemănător GDPR, cu autorități de supraveghere a pieței și mecanisme de audit). Prin urmare, modelul de guvernanță propus se aliniază acestor cerințe pentru a asigura conformitatea încă de la început.

Un alt efect al includerii justiției în lista domeniilor sensibile este că finanțarea proiectelor de IA în domeniul justiției la nivel european poate fi condiționată de existența acestor măsuri de management al riscului. Practic, UE transmite un mesaj clar: "Da, AI în justiție,

dar fă-o cu grijă și responsabilitate." Iar responsabilitatea revine statelor membre să implementeze sisteme de guvernare care să permită beneficiile IA fără a compromite principiile fundamentale ale justiției.

9. Implementare practică: Model de guvernare în România (propunere)

9.1. Structura instituțională propusă

La nivel central (național), propunem înființarea unui Comitet Național pentru Guvernarea IA în Justiție (CN-GIAJ). Ar putea funcționa sub auspiciile CSM sau ca organism interinstituțional (Ministerul Justiției + CSM + alți actori). Componenta ar urma să includă: reprezentanți ai CSM (judecători, procurori), ai Ministerului Justiției, experți tehnici independenți (specialiști în IA), un reprezentant al ANSPDCP (ținând cont de aspectele datelor personale) și reprezentanți ai societății civile sau ai profesiei juridice (cu rol de observatori, pentru transparență). Mandatul comitetului ar fi să coordoneze strategic toate proiectele de IA în justiție: opinii, monitorizare, ghiduri de bune practici.

La nivelul fiecărei instanțe mari (instanțe de apel, tribunale) ar putea fi numit un Manager IA (de exemplu, un grefier sau un specialist IT, sub supravegherea președintelui instanței) pentru a urmări aplicațiile IA utilizate local, pentru a se asigura că procedurile sunt respectate (de exemplu, păstrarea jurnalelor, informația părților când este necesar) și pentru a raporta incidentele sau problemele către CN-GIAJ. Comisii locale de etică tehnologică ar putea fi, de asemenea, înființate în instanțe pentru a evalua feedback-ul utilizatorilor și părților litigante.

Această structură dublă – centrală și locală – asigură atât unitatea națională în abordare (prin Comitetul Central, care oferă linia și standardele), cât și sprijin local acolo unde are loc utilizarea efectivă (prin manageri și comisii locale care pot răspunde rapid problemelor cotidiene).

9.2. Proceduri (Flux de lucru)

Fluxul procedural propus în secțiunea 5.3 ar trebui adaptat contextului instituțional românesc. Pe scurt, fluxul cuprinde următoarele etape:

- Inițierea proiectului AI: O instanță sau Ministerul propune un proiect (de exemplu, implementarea unui sistem inteligent de alocare a cazurilor). Proiectul este înregistrat în registrul național al IA.
- Evaluarea Algoritmă a Impactului (AIA): Echipa de proiect pregătește raportul AIA. Este posibil să solicite sprijin de la CN-GIAJ pentru metodologie.
- Opinia CN-GIAJ: Comitetul Național examinează raportul AIA și emite o opinie (favorabilă / nefavorabilă). Fără aprobare pozitivă, proiectul nu poate continua la pilot.
- Pilot controlat: Dacă este aprobat, proiectul este implementat ca pilot în una sau două instanțe. Managerii locali AI sunt implicați pentru monitorizare. La finalul pilotului, se întocmește un raport de evaluare (inclusiv metrice precum RIU, incidente etc.).

- Audit extern: Raportul pilot este auditat independent (de exemplu, de Institutul Național al Magistraților sau de o echipă academică de la o facultate de drept și o facultate de informatică).
- Aprobarea extinderii: CN-GIAJ, pe baza auditului, autorizează extinderea sistemului către alte instanțe, posibil în etape. Registrul central este actualizat cu starea "operațională" a sistemului.
- Utilizare curentă: În faza de utilizare curentă, managerii locali AI monitorizează conformitatea procedurilor (de exemplu, menționează utilizarea AI în decizii, colectează jurnale). Ei lucrează cu departamentele IT pentru mentenanță și cu grefieri/grefieri de instanță pentru suport.
- Raportarea incidentelor: Dacă apar probleme (reclamații tehnice sau de părți), managerul local IA completează formularul Registrului de Incidente IA și alertează imediat CN-GIAJ dacă incidentul este major.
- Analiza incidentelor: CN-GIAJ se întâlnește (sau delegă într-un subcomitet tehnic) pentru a analiza incidentele și a propune măsuri (de exemplu, oprirea sistemului, repararea tehnică, instruire suplimentară a utilizatorilor dacă problema a fost folosită greșit).
- Buclă de feedback: CN-GIAJ emite periodic recomandări sau revizuieste ghiduri de utilizare pe baza lecțiilor învățate. MoJ propune, de asemenea, posibile ajustări legislative (dacă se găsește o nulitate legală sau o contradicție între lege și utilizarea AI).

Acest proces asigură că nimic nu este lăsat la voia întâmplării: fiecare etapă are mecanisme de control și echilibru, implicând atât avocați, cât și tehnologi. România ar deveni astfel conformă Legii AI și, în același timp, o pionieră în dezvoltarea unei justiții îmbunătățite de IA, dar demnă de încredere.

9.3. Resurse și instruire

Implementarea unui astfel de model necesită resurse dedicate:

- Resurse financiare: pentru achiziția sau dezvoltarea sistemelor AI (ideal, open-source sau dezvoltate în parteneriat cu universități, pentru transparență), pentru infrastructură securizată de stocare a logurilor, pentru audituri externe etc. Fondurile europene pot fi accesate (de exemplu, prin programe de digitalizare a justiției) pentru a susține aceste costuri.
- Resurse umane specializate: va fi nevoie de recrutarea sau instruirea specialiștilor IT în sistemul judiciar (dacă nu la fiecare instanță, cel puțin la nivelul instanțelor de apel) pentru a susține tehnic implementarea IA. De asemenea, judecătorii și personalul auxiliar trebuie să fie parțial eliberați de funcții pentru a putea participa la instruirii specializate.
- Programe de educație continuă: Institutul Național de Magistratură (INM) ar trebui să includă module de tehnologie și etică a inteligenței artificiale în curricula sa. În mod similar, Școala Națională a Registrarilor poate introduce module practice despre utilizarea instrumentelor AI (de exemplu, cum să verifici un rezumat generat automat, cum să folosești un motor de căutare pentru jurisprudență bazat

pe IA etc.). Aceste programe pot fi desfășurate în parteneriat cu universități sau cu alte țări care au inițiative similare.

Un aspect important este schimbul de bune practici internaționale: deoarece multe țări ale UE vor implementa Legea AI în sistemul judiciar, România ar trebui să participe activ la rețelele europene (cum ar fi grupurile de lucru CEPEJ sau proiectele pilot coordonate de Comisia Europeană) pentru a învăța din experiența altora și a-și face cunoscute propriile inovații.

În esență, investiția în guvernanta IA este o investiție în viitorul justiției. Pe termen mediu și lung, aceste resurse alocate vor fi compensate de eficiența și calitatea justiției îmbunătățite tehnologic, atâta timp cât este implementată responsabil.

10. Discuții critice și limitări

10.1. Probleme practice anticipate

Una dintre principalele probleme este tensiunea dintre transparență și secretul comercial al furnizorilor de soluții AI. Dacă sistemul judiciar achiziționează o soluție de la un furnizor privat, acel furnizor ar putea invoca secrete comerciale pe algoritm. Pe de altă parte, sistemul judiciar are nevoie de transparență pentru a-și menține credibilitatea. Soluții posibile: includerea în contracte a obligației furnizorului de a oferi acces la un audit independent al algoritmului, utilizarea software-ului open-source atunci când este fezabil sau cel puțin mecanisme controlate de divulgare (de exemplu, codul sursă care să fie pus la dispoziția unei terțe părți de încredere, cum ar fi Institutul Național de Magistratură, în baza clauzelor de confidențialitate). [6], [5], [9], [25]

O altă problemă este capacitatea și resursele tehnice limitate. Multe instanțe din România încă se confruntă cu lipsă de personal IT sau chiar de echipamente învechite. Introducerea IA va necesita investiții simultane în infrastructură (serve, stocare securizată) și întreținere. Dacă aceste investiții nu sunt făcute, există riscul ca proiectele AI să eșueze sau, mai rău, să creeze vulnerabilități (de exemplu, un sistem insuficient securizat ar putea deveni ținta atacurilor cibernetice, punând în pericol datele criminalistice).

Rezistența la schimbare este, de asemenea, ceva de luat în considerare. Unii magistrați sau personal de suport pot fi reticenți să folosească instrumente AI fie din lipsă de încredere, fie din ignoranță. Această barieră culturală trebuie gestionată prin dialog și instruire – dar există riscul ca, dacă implementarea este grăbită sau impusă de sus în jos, să genereze opoziție.

Nu în ultimul rând, cadrul legal național ar putea necesita ajustare. Deși Legea AI va fi aplicabilă direct, pot fi necesare modificări specifice în legislația națională (de exemplu, în Legea Organizării Judiciare, pentru a permite comitetelor de etică tehnologică sau în regulile de ordine internă ale instanțelor să stipuleze explicit obligația de a menționa utilizarea IA în motivație). Fără o astfel de ancorare internă, unele recomandări pot rămâne la nivelul celor mai bune practici aplicate inegal.

10.2. Nevoi suplimentare de cercetare

Cercetarea de față are un caracter exploratoriu și conceptual. Sunt necesare studii empirice viitoare pentru a valida (sau invalida) ipotezele noastre. De exemplu, un proiect pilot într-o instanță cu implementare parțială a modelului de guvernare ar fi util pentru a vedea cum funcționează indicatorii propuși în practică și ce ajustări necesită.

Evaluările comparative ar fi, de asemenea, valoroase: cum abordează alte țări UE introducerea IA în justiție? Există deja proiecte în Franța, Olanda, Estonia etc. – un studiu comparativ ar putea inspira îmbunătățiri ale modelului românesc. De exemplu, Estonia testează un "judecător robot" pentru reclamații mărunte; rezultatele acelui experiment (dacă sunt transparente) ar oferi lecții despre limitările IA în rolul decizional. [17], [18], [14], [16, 24], [26]

O direcție necesară de cercetare este dezvoltarea standardelor tehnice sectoriale. Legea AI prevede standarde armonizate (art. 40), dar ar fi util ca comunitatea judiciară să dezvolte ghiduri specifice: ce înseamnă "părtinire acceptabilă" într-un algoritm juridic? Ce nivel de acuratețe ar trebui să fie folosit un rezumat al hotărârii? Astfel de întrebări pot primi răspuns doar prin colaborare interdisciplinară între avocați, informaticieni și experți în etică, în cadrul unor grupuri de lucru dedicate.

În concluzie, implementarea IA în justiție este un proces continuu care va evolua pe măsură ce tehnologia avansează și societatea își clarifică valorile și așteptările. Această lucrare reprezintă un pas în această conversație, dar mai este mult de explorat.

11. Concluzii

11.1. Rezumatul final

Adoptarea Legii AI a schimbat fundamental peisajul reglementării IA în UE, stabilind obligații clare pentru sistemele de inteligență artificială cu risc ridicat și interzicând anumite utilizări considerate inacceptabile. Pentru sistemul judiciar, acest cadru european reprezintă atât o provocare, cât și o oportunitate: provocarea de a integra tehnologii avansate fără a compromite drepturile și garanțiile procedurale și oportunitatea de a crește eficiența și accesibilitatea justiției prin instrumente moderne.

În această lucrare am susținut că o implementare responsabilă a IA în justiție necesită un cadru de guvernare robust și multidimensional. Am propus un astfel de model, care include: registrul național al aplicațiilor AI (pentru transparență și evidență), evaluări algoritmice ale impactului înainte de comisionare (pentru cartografierea și reducerea riscurilor), politici stricte de înregistrare și audit (pentru trasabilitate și responsabilitate), cerințe de explicabilitate adaptate publicului țintă (judecători vs. părți), mecanisme pentru contestarea și corectarea deciziilor influențate de AI, structuri instituționale dedicate (comitete tehnic-juridice-etice) și programe de formare profesională în domeniul inteligenței artificiale.

În esență, legitimitatea luării deciziilor umane nu se câștigă prin excluderea completă a IA, ci prin proiectarea, documentarea și guvernarea utilizării IA astfel încât responsabilitatea să rămână, verificabil și ireversibil, în aparența judecătorului. IA poate fi un aliat valoros al justiției – de exemplu, pentru a gestiona volume mari de informații, a identifica tipare jurisprudențiale sau a reduce durata proceselor – dar doar atunci când este folosită ca un instrument sub control uman și într-un cadru de încredere.

Munca noastră a evidențiat că o astfel de integrare este posibilă și de dorit, cu condiția să existe un cadru normativ și etic clar, voința instituțională de a o implementa și un proces continuu de evaluare și îmbunătățire. Pe măsură ce tehnologia evoluează, va fi nevoie de adaptare, dar principiile fundamentale prevăzute de Legea AI și CEPEJ oferă o busolă clară: omul și drepturile sale trebuie să rămână în centrul sistemului de justiție, oricât de sofisticate ar deveni instrumentele auxiliare.

11.2. Recomandări

În lumina concluziilor de mai sus, formulăm câteva recomandări concrete pentru acțiune imediată pentru factorii de decizie din România:

- **Înființarea Comitetului Național (CN-GIAJ):** Începerea procedurilor pentru crearea organismului central pentru guvernarea IA în justiție, cu un mandat clar și alocarea resurselor necesare. Ar trebui să înceapă imediat inventarierea oricăror inițiative de IA existente în sistemul judiciar.
- **Implementarea registrului național al aplicațiilor IA:** Chiar înainte de implementarea Legii AI, un astfel de registru poate fi înființat intern, pentru a ști exact ce prototipuri sau software bazat pe IA există deja în instanțe/urmăriri penale (de exemplu, poate unele instanțe folosesc instrumente de traducere automată, instrumente de anonimizare etc.).
- **Evaluarea obligatorie a impactului (AIA):** Prin ordinul ministrului sau decizia CSM, se stabilește cerința ca orice propunere de achiziție/dezvoltare de software de inteligență artificială pentru instanțe să fie însoțită de o evaluare a impactului (cel puțin privind drepturile și libertățile, dacă nu una tehnică foarte detaliată). Acest pas asigură că gândirea în managementul riscului este internalizată încă de la început.
- **Politici de jurnalizare și audit:** În colaborare cu STS sau alte organisme IT guvernamentale, dezvoltați un plan pentru infrastructura de jurnalizare la nivelul întregii instanțe și un protocol periodic de audit. Aceasta implică și alocarea bugetară pentru echipamente și servicii.
- **Programe de Alfabetizare Digitală Juridică:** INM și SNG, posibil împreună cu facultăți de drept și parteneri internaționali, pentru a iniția rapid ateliere/cursuri scurte pentru magistrați despre ce este IA, ce oferă Legea AI și cum ar trebui abordată din perspectivă judiciară. Scopul este ca, până la intrarea în vigoare a reglementării europene, organismul profesional să aibă un bagaj conceptual minim pentru a naviga noile realități.

Prin implementarea acestor măsuri imediate, România s-ar poziționa proactiv în fața valului de schimbare adus de inteligența artificială în justiție, transformând obligația de a

se conforma într-o oportunitate de modernizare și eficiență, fără a compromite legea justiției.

Referințe

- [1] A. Ionescu, “Inteligența artificială în administrația publică: între eficiență și etică,” *Journal of Public Administration*, vol. 7, nr. 1, pp. 15–30, 2023.
- [2] M. Georgescu și A. Popescu, *Guvernanța algoritmilor în justiție: provocări și soluții*. București, România: Editura Universul Juridic, 2024.
- [3] M. Hildebrandt, *Smart Technologies and the End(s) of Law*. Cheltenham, U.K.: Edward Elgar, 2015.
- [4] M. Hildebrandt, *Law for Computer Scientists and Other Folk*. Oxford, U.K.: Oxford University Press, 2020.
- [5] European Parliament and Council, Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), *Official Journal of the European Union*, Jul. 12, 2024. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- [6] European Commission for the Efficiency of Justice (CEPEJ), “European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment,” Council of Europe, Dec. 2018. [Online]. Available: <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>
- [7] European Parliament and Council, Regulation (EU) 2016/679 (General Data Protection Regulation), *Official Journal of the European Union*, vol. L 119, May 4, 2016. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [8] Article 29 Data Protection Working Party, “Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679,” WP251rev.01, Feb. 6, 2018; endorsed by the European Data Protection Board, May 25, 2018. [Online]. Available: https://www.edpb.europa.eu/documents/guideline/automated-decision-making-and-profiling_en
- [9] L. Edwards and M. Veale, “Slave to the algorithm? Why a ‘right to explanation’ is probably not the remedy you are looking for,” *Duke Law & Technology Review*, vol. 16, pp. 18–84, 2017.
- [10] S. Wachter, B. Mittelstadt, and L. Floridi, “Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation,” *International Data Privacy Law*, vol. 7, no. 2, pp. 76–99, 2017.
- [11] E. Tabassi, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023, doi: 10.6028/NIST.AI.100-1.
- [12] S. Barocas, M. Hardt, and A. Narayanan, *Fairness and Machine Learning: Limitations and Opportunities*. Cambridge, MA, USA: MIT Press, 2023. [Online]. Available: <https://fairmlbook.org/>
- [13] S. Barocas and A. D. Selbst, “Big data’s disparate impact,” *California Law Review*, vol. 104, no. 3, pp. 671–732, 2016.
- [14] N. Aletras, D. Tsarapatsanis, D. Preotiuc-Pietro, and V. Lampos, “Predicting judicial decisions of the European Court of Human Rights: A natural language processing perspective,” *PeerJ Computer Science*, vol. 2, Art. no. e93, 2016, doi: 10.7717/peerj-cs.93.
- [15] D. M. Katz, M. J. Bommarito II, and J. Blackman, “A general approach for predicting the behavior of the Supreme Court of the United States,” *PLOS ONE*, vol. 12, no. 4, Art. no. e0174698, 2017, doi: 10.1371/journal.pone.0174698.
- [16] M. Medvedeva, M. Vols, and M. Wieling, “Using machine learning to predict decisions of the European Court of Human Rights,” *Artificial Intelligence and Law*, vol. 28, pp. 237–266, 2020.
- [17] OECD, “Recommendation of the Council on Artificial Intelligence,” OECD/LEGAL/0449, May 22, 2019, amended 2024. [Online]. Available: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
- [18] European Commission, “Coordinated Plan on Artificial Intelligence: 2021 Review,” COM(2021) 205 final, Apr. 21, 2021.
- [19] J. A. Kroll et al., “Accountable algorithms,” *University of Pennsylvania Law Review*, vol. 165, no. 3, pp. 633–705, 2017.
- [20] F. Doshi-Velez and B. Kim, “Towards a rigorous science of interpretable machine learning,” arXiv:1702.08608, 2017.

- [21] R. Guidotti et al., “A survey of methods for explaining black box models,” *ACM Computing Surveys*, vol. 51, no. 5, Art. no. 93, 2018, doi: 10.1145/3236009.
- [22] C. Rudin, “Stop explaining black-box models in high-stakes decisions and use interpretable models instead,” *Nature Machine Intelligence*, vol. 1, pp. 206–215, 2019.
- [23] S. Wachter, B. Mittelstadt, and C. Russell, “Counterfactual explanations without opening the black box: Automated decisions and the GDPR,” *Harvard Journal of Law & Technology*, vol. 31, no. 2, pp. 841–887, Spring 2018.
- [24] A. Barredo Arrieta et al., “Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI,” *Information Fusion*, vol. 58, pp. 82–115, 2020, doi: 10.1016/j.inffus.2019.12.012.
- [25] J. Burrell, “How the machine ‘thinks’: Understanding opacity in machine learning algorithms,” *Big Data & Society*, vol. 3, no. 1, pp. 1–12, 2016.
- [26] C. Molnar, *Interpretable Machine Learning: A Guide for Making Black Box Models Explainable*, 2nd ed. Munich, Germany: Christoph Molnar, 2022.

The use of AI in judicial systems: From documentary assistance to jurisdictional management

Sebastian AVĂCĂRIȚEI

*Alexandru Ioan Cuza University of Iași, Faculty of Economics and Business Administration
Iași, Romania
sebastian.avacaritei24.07@gmail.com*

Mihaela TOFAN

*Alexandru Ioan Cuza University of Iași, Faculty of Economics and Business Administration
Iași, Romania
mtofan@uaic.ro*

Abstract

Digital transformation brings artificial intelligence (AI) tools to the judicial ecosystem with a wide range of uses: from documentary assistance (search, classification, summarization, anonymization) to support for jurisdictional management (planning, resource allocation, administrative sorting) and, at the limit, to analyses that can influence the evaluation of evidence and the outcome of cases. In this context, the article proposes an integrated framework for judicial governance of AI, aligned with the EU Regulation on AI (AI Act), which combines risk classification, AI literacy of staff, audit (logging, traceability) and explainability of automated decisions, with the explicit aim of maintaining the legitimacy of human decision-making. From a methodological perspective, the paper maps the judicial uses of AI on the risk classification of the AI Act and extracts the related obligations (transparency, human oversight, risk assessment and mitigation, event logs), with a focus on the first provisions already operational (AI literacy and prohibited practices). The central contribution is a model of “judicial AI governance” that includes: registry of AI uses and risk matrix; algorithmic impact assessments; policies of journaling and explainability appropriate to the target audience (judges/registrars/parties); mechanisms of challenge and redress; joint legal-technical-ethical committee; role-based AI literacy programs. The article derives sets of indicators (rate of human interventions, quality of motivation, incidents of bias/challenge) and draws guidelines for integrating AI without compromising procedural guarantees (adversarial, publicity, right to defense). The conclusion is that the legitimacy of human decision does not result from the absence of AI, but from its design and governance in such a way that control and responsibility remain, verifiably, with the human judge.

Keywords: judicial governance; transparency; impact assessment; human oversight

1. Introduction

1.1. Background and motivation

AI technologies are already found in document assistance (jurisprudence search, document classification, automatic summarization), in the administrative management of case flows, and in certain pilot projects in tools that can influence the evaluation of evidence or the recommendation of solutions. Natural from the perspective of efficiency, the introduction of AI nevertheless raises essential questions: how to preserve the principle of adversariality, publicity and the right to a fair trial? How does the final responsibility rest with the judge, if algorithms contribute to the decision? These concerns are shared by recent specialized literature, which emphasizes the need to balance efficiency with respect for fundamental rights [1], [2], [3], [4].

Regulation (EU) 2024/1689 (the so-called AI Act) imposes a risk-based regulatory architecture; certain uses of AI in the field of justice can be categorized as "high-risk" and are subject to specific obligations [5]. The CEPEJ ethical charter (2018) underlines, in turn, the main principles that must be respected when using AI in justice: respect for fundamental rights, transparency, non-discrimination and human control over the decision [6]. Also, the GDPR (Reg. 2016/679) remains relevant regarding the protection of personal data and the rights of the person, as it provides, among other things, the right not to be the subject of a decision based exclusively on automatic processing, which produces legal effects on the person or significantly affects him (art. 22) [7], [8], [9], [10].

2. Methodology

The present study uses a combined doctrinal-normative approach to the relevant regulations (AI Act and CEPEJ Charter), combined with a mapping of the uses of AI in justice. The risks associated with each type of use were identified and the applicable legal obligations were extracted. On this basis, a model of judicial governance of AI was developed, composed of concrete operational elements and measurable indicators of compliance.

The approach has a predominantly conceptual and normative character. The proposed recommendations must be validated and calibrated through empirical testing, within pilot projects, and adapted according to available institutional resources. Also, the analysis does not address in detail the differences in implementation at the level of each national jurisdiction, but proposes a general framework applicable in the context of the Romanian judicial system, in accordance with European regulations.

3. European Regulation: Relevant Extracts from the AI Act

3.1. List of Uses Considered High Risk (Extract from the AI Act, EUR-Lex Summary)

“The regulation defines the use of AI in the following areas as high risk, due to the potential impact on fundamental rights, safety and well-being: ... law enforcement ... administration of justice and democratic processes, AI systems used by judicial authorities for legal research and interpretation or systems that could influence election outcomes.” [5]

According to the AI Act, AI systems used in the administration of justice (e.g. by courts, for legal documentation, interpretation of the law or application of the law to facts) fall into the "high-risk" category, as do those used in democratic processes (e.g. to influence the outcome of elections) [5]. This fact requires compliance with the strict requirements provided by the regulation for such systems.

3.2. Prohibited AI Practices (Unacceptable Risk - Extract from the AI Act, EUR-Lex Summary)

“The regulation prohibits the following AI practices with an unacceptable level of risk: Subliminal or deceptive techniques to manipulate individual or group behaviour; Exploiting vulnerabilities based on age, disability, or socioeconomic situations; Social scoring; Criminal risk assessment, predicting the likelihood of committing a crime solely

based on profiling or personality traits; Facial recognition database scraping ... Inferring emotions in sensitive areas (workplaces, educational institutions).” [5]

In other words, the AI Act prohibits the marketing or use of AI systems that resort to: (a) subliminal or deceptive techniques to manipulate behavior, (b) exploitation of vulnerabilities related to age, disability or socioeconomic status, (c) social scoring of individuals, (d) crime risk assessment (prediction of recidivism) based on automatic profiling of the individual, (e) untargeted expansion of facial recognition databases through extracting images from the Internet, and (f) detecting emotions in sensitive contexts (at work, in schools, etc.) [5]. All these practices are considered to have an unacceptable level of risk and are therefore completely prohibited by the regulation.

3.3. Obligations for High-Risk AI Systems

For AI systems classified as high-risk, the AI Act provides a series of specific obligations, aimed at ensuring their use in legal and ethical safety conditions. In essence, the following must be implemented: (i) a risk management system throughout the system's life cycle, of an iterative nature and periodically updated [5]; (ii) guarantees regarding the quality of the data used and the avoidance of discrimination – for example, training datasets must be relevant, representative and as complete and error-free as possible, to reduce algorithmic biases [5]; (iii) record-keeping mechanisms (logs) for auditing events and traceability of AI decisions [5]; (iv) ensuring effective human supervision, i.e. the system is designed so that a human operator can effectively monitor and correct its operation [5]; (v) transparency towards users (implementers) and, as the case may be, towards the persons affected by the decisions made with the help of AI [11]. For example, high-risk AI systems should be accompanied by clear instructions for use and information on their capabilities and limitations, to enable users to correctly interpret their results [5]. In certain situations, people affected by automated decisions must be informed about the role of AI. All of these requirements are intended to maintain control and accountability with human actors, even when using automated tools. [12], [13]

4. Mapping AI Uses in Justice and Risk Assessment

4.1. Uses and Risks

To understand the impact of AI in the judicial system, we have mapped the main types of possible uses and their associated risk levels, consistent with the categories in the AI Act and the literature [2]:

Document support (e.g., case law search, automatic summarization, document anonymization): low to medium risk. The benefits are related to efficiency in information processing, but there is a risk of accuracy errors (e.g. omission of relevant sources or inaccurate summaries) and possible opacity in the way results are obtained. Human verification of the information provided by the system is required [6]. Administrative support (e.g., automated case sorting, case randomization, agenda management): medium risk, which can become high if the system has a high degree of automation without human intervention. The negative impact may be on equal access to justice (if, for example, sorting

favors or disfavors certain categories of cases or persons) and on the principle of random assignment.

Support in judicial decision-making (e.g., evidence evaluation tools, systems for predicting the outcome of trials or recommending sanctions): high risk. These uses clearly fall within the high-risk sphere defined by the AI Act and require compliance with all legal obligations [14], [15], [16] – risk assessment, logging, strict human supervision, etc. [6], [17] Certain uses of this type may even be considered unacceptable or prohibited, if they tend to substitute the decision-making role of the judge (for example, an algorithm that decides the sentence would violate the principle of independence of the judge).

Overall, the degree of risk increases as AI moves from support roles (documentation, administration) to direct jurisdictional roles. Accordingly, the level of regulation and supervision must also increase proportionately.

5. The Governance Model Proposed for AI in Justice

5.1. Guiding Principles (Normative-Ethical)

Considering the identified risks and requirements, we propose a governance model that combines normative principles with concrete operational procedures. The goal is the responsible integration of AI into the judicial act, without compromising procedural guarantees and always keeping the final decision in the hands of the judge.

The model is based on the following principles, aligned with both legal and ethical requirements:

- AI Act Compliance – Any AI system used in justice must fully comply with Regulation (EU) 2024/1689 and related risk category [5].
- Respect for fundamental rights and CEPEJ principles – Every AI implementation must be evaluated against the CEPEJ Charter (2018), which emphasizes: respect for human rights, non-discrimination, impartiality and human user control over the decision [6].
- Proportionality and transparency – The introduction of an AI-based tool must be proportionate to the problem it solves and accompanied by transparency. Any AI intervention in the judicial process will be known to the parties and justified by the efficiency or accuracy it brings, without affecting procedural rights.
- Effective human control – In all cases, a judge (or designated human staff) must have a real opportunity to supervise, validate or refute the result provided by the AI. The responsibility of the judicial decision always remains with the human, the AI having only an advisory or auxiliary role.

Through these principles we ensure that the legitimacy of the judicial decision is maintained, AI being a tool subordinate to the goal of justice, not an autonomous decision-making factor.

5.2. Key Components of the Governance Framework

To operationalize the above principles, the model proposes the following institutional and procedural components:

- **Central Registry of AI Applications** – A national database to register all AI applications used in the judicial system. Essential metadata will be recorded for each application: purpose, field of use (documentary/administrative/judicial), risk classification (according to AI Act), algorithm version, vendor, impact assessments (if performed), etc. This central registry ensures visibility and traceability.
- **Algorithmic Impact Assessments (AIAs)** – Standardized implementation of impact assessments prior to commissioning an AI system. The Algorithmic Impact Assessment will analyze potential bias, rights risks (e.g. non-discrimination, privacy), mitigation measures. It is recommended that the non-technical summary of each evaluation be made public for transparency.
- **Strict logging policies** – For medium or high risk systems, it is required to keep log files that include usage data: timestamps, relevant input and output data, human interventions (if any), system parameters [11], [18]. Access to these logs must be regulated: available for internal audit, for inspections by competent authorities and, in an appropriate form, for parties contesting AI-generated solutions. [19]
- **Explainability requirements** – The model provides two levels of explainability: technical explainability (for judges and IT experts, who can receive detailed documentation about the algorithm's operation, performance, limits) and accessible explainability (for litigants and the public, i.e. explanations in common language about the role of AI in the process and how it influenced the decision, if any).
- **Appeal and redress mechanisms** – Establishing a clear procedure by which litigants can challenge the use or output provided by an AI system. For example, a party that believes it has been disadvantaged by an algorithmic recommendation may file a request for human review of that analysis. In the event of demonstrated AI error, disciplinary or remedial mechanisms (including retrial) must be available.
- **Technical-legal-ethical central committee** – We recommend the establishment of a collegial body (possibly under the auspices of the CSM or MJ) to oversee the governance of AI. The committee would include judges, IT specialists, ethics experts, civil society representatives and possibly the National Data Processing Supervisory Authority (ANSPDCP). This committee would approve the introduction of new AI systems, review audit reports and incidents, and issue policy recommendations.
- **Training programs** – A fundamental component is the digital literacy of judicial staff. Judges, clerks, lawyers should participate in training on the basics of AI, the interpretation of algorithm results, potential errors and biases, and the procedures to follow when interacting with such tools. These programs would increase confidence and professional competence in the context of new technologies.
- **Periodic external audit** – In addition to internal monitoring, the model provides for independent audits (performed by mixed teams of IT professionals and external lawyers) at least annually, with the publication of summary reports. The audit will verify compliance of AI systems with legal obligations (e.g., whether a high-risk

system has logs in order, whether it meets the stated accuracy, etc.) and provide recommendations.

These components, implemented together, create an ecosystem of trust in the use of AI: transparency, control and accountability throughout the lifecycle of algorithms in justice. [20], [21], [22]

5.3. Operational Procedures

Based on the above components, the procedural flow for introducing and using an AI system in the courts could be as follows:

1. Initial registration: Any project implementing an AI tool is registered in the Central Registry of AI Applications, with a detailed description of its purpose and functionalities.
2. Preliminary assessment & opinion: An Algorithmic Impact Assessment (AIA) is being conducted. The AIA report is sent to the Central Committee (CN-GIAJ) for opinion. The committee may request clarifications, additional tests, or may impose certain conditions of use.
3. Controlled pilot: If approved, the AI system is initially implemented in a pilot program (for a limited time in a specific court or department) with intensive monitoring. In this phase logs and feedback from users are collected.
4. Independent audit: At the end of the pilot phase, an external auditor analyzes system performance, compliance with risk reduction measures and incidents.
5. Final approval: Based on the audit report, the Central Committee decides whether the system can be expanded on a large scale. Approval may be subject to conditions (e.g., re-evaluation in 6 months, technical improvements required, etc.).
6. Operational implementation: The system is used according to its intended purpose, in compliance with the logging and transparency policies. If the AI played a significant role in a case (e.g. generated a resolution recommendation), this should be explicitly stated in the court order or case notes, including a summary of how the recommendation was used.
7. Ongoing monitoring: Key indicators are tracked and reported quarterly to the Central Committee. Any incident (error, reported bias, malfunction) is registered in an AI Incident Register and triggers the analysis procedure.
8. Party Complaint Mechanism: If a party to a lawsuit believes it has been wronged or affected by the use of AI, it can file a complaint through a dedicated electronic form. Human re-evaluation of the challenged aspect is ensured within 30 days maximum, and if the problem is confirmed, corrective measures are taken (e.g. exclude that AI analysis from the solution reasoning, re-judge if necessary, improve the algorithm for the future).
9. Reporting and review: Annually, a summary report is published (by the CSM or other designated authority) on the use of AI in the judiciary, including statistics, benefits observed, problems encountered and the action plan for the following year.

These procedures create a lifecycle of AI projects, from idea to evaluation, implementation and feedback, thereby ensuring continuous improvement and adaptation to the evolving legal and technological context.

6. Monitoring Indicators

6.1. Primary Indicators

To assess the effectiveness and safety of the use of AI in justice, we propose a set of key performance and compliance indicators. These indicators must be continuously monitored and periodically reported to decision makers.

- **Human Intervention Rate (RIU):** The percentage of cases in which the human operator (judge or staff) modified or rejected the recommendation provided by the AI. A very low RIU (e.g. < 5% over a 6-month period) could indicate either that the AI is making flawless decisions, or (more dangerously) that humans have become overly dependent on recommendations and are no longer exercising critical control. An alert threshold would be $RIU < 5\%$, in which case a Central Committee investigation into the quality of human supervision would be required.
- **The rate of transparency in reasoning (RTM):** The percentage of court decisions in which the use of an AI tool is explicitly mentioned, when it had a significant role in the resolution of the case. The target must be 100% – any influence of AI on decision-making to be publicly documented. An RTM below 100% indicates documentation or transparency deficiencies that need to be corrected.
- **AI incidents per 10,000 cases:** The number of incidents related to the use of AI (major errors, proven bias, data security breach, party complaints) reported for every 10,000 cases resolved. Both the absolute number and the type of incidents (technical vs. legal or ethical) are tracked. A growing trend calls for an urgent reassessment of how AI is used.
- **Average Response Time to AI Referrals (TMR):** The average time (in days) it takes for judicial authorities to process and respond to a party's referral regarding the use of AI. The proposed target is ≤ 30 days to ensure prompt remedies
- **Reasoning Quality Score (SQM):** A qualitative indicator resulting from audits of judgments involving AI, which assesses the legal coherence of the reasoning, the judge's critical justification and the appropriate integration of AI input (if any). For example, one could rate the quality of reasoning from 1 to 5, where 5 means an excellently reasoned decision, where the judge uses the information provided by the AI (if it was used) critically, without abdicating his role.

These indicators should be interpreted as a whole, not in isolation. The goal is to detect early deviations: for example, a very low RIU combined with a low SQM would raise a red flag (possible over-reliance on AI and decreased quality of human deliberation).

6.2. Mode of Reporting

Indicators will be reported as follows:

- **Internal quarterly reports:** to the Central AI Governance Committee (CN-GIAJ), containing the values of the indicators, explanations for possible deviations and proposed measures.
- **Annual public report:** to the Superior Council of Magistracy (CSM) and the general public, including a summary of annual data, trends, examples of good practice and

the action plan. This annual report ensures external transparency and public accountability on how AI is being integrated into justice.

- Notifications to European authorities: According to the AI Act, in situations where serious incidents occur or when certain critical thresholds are exceeded, national authorities (e.g. market surveillance authority for AI) must notify the relevant European institutions. The model stipulates that the Central Committee is responsible for coordinating these notifications, ensuring that Romania fulfills its cooperation obligations at the EU level.

Through rigorous monitoring and reporting, institutional learning becomes possible: the judiciary can continually adjust its AI policies while maintaining alignment with the principle of due process.

7. Procedural Guarantees and Ethical Considerations

7.1. Adversarial Process and Explainability

The integration of AI into the judicial act must not undermine the fundamental guarantees of the judicial process. In this section we discuss how the proposed model relates to the principles of adversariality, rights of defense and publicity, as well as the importance of these principles in the context of AI.

The principle of adversariality requires that all relevant evidence and arguments in a trial be known and accessible to the parties, so that they can be contested. Consequently, if an AI algorithm provides an analysis or recommendation that is taken into account by the judge, the conclusions of the algorithm must be communicated to the parties and subjected to adversarial debate [6]. In other words, the parties have the right to know whether and how the AI contributed to the proposed solution and to have the opportunity to challenge or support it, as appropriate. The CEPEJ Charter highlights that the use of artificial intelligence tools must not undermine the guarantees of the right to a fair trial – including equality of arms and adversariality [6].

In practice, the explainability of technology becomes the premise of adversariality: the AI system must provide an intelligible explanation of its output [23], [24] (or allow the human expert to explain it) so that lawyers and judges can understand the reasoning and discuss it in court [6], [8]. For example, if software suggests certain case law as relevant, the opposing party must be able to check that case law and argue against it. The proposed governance model explicitly stipulates the obligation to mention the use of AI in the motivation and provide explanations in the understanding of the parties, precisely to respect this principle.

7.2. The Right to Defense and the Responsibility of the Judge

The parties' right to defense presupposes that each party can effectively challenge the allegations and evidence presented against it, and that it has access to a reasoned decision by an independent judge. The introduction of AI must in no way create a "black box" inaccessible to defense. Therefore, any recommendation of an AI used in the file must not only be communicated, but also explained in legal language. The judge remains the owner

of the decision; AI recommendations are ancillary tools – not delegation of authority. This distinction is crucial: the judge can accept or ignore the AI's suggestion, but cannot be subordinated to it.

In situations where the use of AI would lead to an error or bias (for example, if an algorithm has a systematic bias against a group and negatively influences a decision), remedial mechanisms must allow for the correction of the decision and even the retrial of the case, in order to protect the rights of the injured party. The final responsibility belongs to the judge, so that any error of the AI integrated in the reasoning becomes an error of the court, which can be attacked through ordinary means of appeal (appeal, appeal). The proposed governance model, through appeal procedures and human intervention, ensures that the right to defense is not emptied of content in the digital age.

7.3. Publicity and Public Trust

Publicity of court hearings and transparency of the judicial act are cornerstones for public confidence in the judicial system. If the courts used AI in secret, without the knowledge of the parties and the public, it would create a major risk of mistrust and conspiracy theories about "algorithmic justice". Transparency about AI's role in case resolution is therefore essential. The model requires mention in the judgment when an automated tool contributed to the analysis, as well as the periodic publication of reports on the use of AI.

This proactive approach to transparency aims to prevent the perception that AI is a hidden decision-maker. On the contrary, used correctly, AI can increase trust if it is shown to help the consistency of judicial practice, speed and access to information. The key is that the use is not secret: only by knowing and understanding how AI contributes to justice can the public (and the parties) objectively assess the added value or possible risks. Transparency thus becomes not only a legal obligation (according to the AI Act), but also a communication strategy for the judicial system in order to cultivate public trust.

8. Compliance with the AI Act: Essential Provisions Explained

8.1. Prohibited Practices (AI Act, Art. 5) and Legal Relevance

The AI Act prohibits certain AI practices deemed to be of unacceptable risk. Of these, relevant for the judicial field are profiling for the purpose of social "scoring" and the automated assessment of criminal risk.

The official text of the regulation explicitly states that it is prohibited to use AI to evaluate or classify natural persons based on social behavior or personal characteristics, when this leads to social scoring and unfavorable treatments (European Parliament & Council, 2024). By analogy, any litigant "rating" system (e.g. an algorithm that would suggest the solution depending on the party's procedural history) would fall under this prohibition. The regulation also prohibits AI systems used to predict the likelihood of committing a crime based on a person's profile [5]. This means that predictive policing tools or purely automated recidivism assessments cannot be used as such in criminal decision-making – they would violate the right to a fair trial and the presumption of innocence.

Interpretation: In the judicial system, the AI Act prohibitions require the avoidance of any uses of AI that would achieve punitive profiling or scoring of individuals involved in the process. Any attempt to introduce an automatic "dangerousness index" would be against both the regulation and the principles of criminal law. Also, the inference of people's emotions in a judicial context (e.g., an AI to "read" the emotions of a witness to decide credibility) falls into the prohibited area, the prohibition of inferring emotions in sensitive areas being explicitly mentioned [5]. So, the introduction of AI in justice must focus on permissible tools (e.g.: documentation assistance) and clearly avoid prohibited practices.

8.2. Requirements for High-Risk Systems (AI Act, Arts. 9–15) – Enforcement

As mentioned, the AI Act imposes on high-risk AI systems a series of technical and organizational requirements: risk management, data quality, logging, human supervision, transparency, as well as the registration of these systems in a European database. In the field of justice, any algorithm advanced enough to influence a judicial decision will almost certainly be considered high-risk (the "administration of justice" field is listed as such) [5].

In practice, this translates as follows: before implementation, the court or the Ministry of Justice (as the provider or deployer of the system) must establish a risk management system for that AI – identifying the possible risks to the rights of the parties and how to mitigate them (e.g. if a jurisprudence search algorithm could omit relevant jurisprudence, the additional manual verification procedure is provided). The quality of the data must also be ensured: if a model is trained based on previous judicial decisions, those data must be clean and representative in order not to induce bias (for example, if in a certain matter the previous practice was non-uniform or biased, an algorithm trained exclusively on it could reproduce that bias) [5], [12].

Logging is crucial: the system must be able to automatically record usage events to enable auditing. The AI Act provides, for example, that for high-risk justice systems the logs must record at least the duration of each use, the input data that generated a certain result and the identification of the person who supervised the result [5]. This corresponds to the measures proposed in our model, where we specified the content of the logs.

Human supervision must be integrated by-design: AI Act art. 14 stipulates that high-risk AI systems must be designed to allow effective supervision by humans. That means interfaces that give the judge enough visibility and control: for example, the ability to see the justification for an algorithm prediction, correct input data, or stop automatic operation if a problem is noticed.

Last but not least, transparency towards users (judges/registrars) involves providing detailed user instructions and clearly informing those using the system about its capabilities and limitations [5]. In a judicial context, this would take the form of practical guidelines for magistrates on how to use (and not use) a particular AI, what that AI can and cannot do, etc.

Any algorithm that can influence the solution in a file must be treated as a high-risk system, with all the strict measures: prior analysis, careful monitoring and permanent human control. Only in this way can we ensure that AI acts as an ally of justice and not as an opaque or uncontrollable factor.

8.3. Express Mention of the Field of Justice in the List of High-Risk Uses

The AI Act explicitly lists "administration of justice" in Annex III as a high-risk area of AI use [5]. This inclusion has direct implications: all AI applications used by judicial authorities fall ipso facto into the high-risk sphere (except for purely administrative ones with no impact on rights – but even there, the boundary is fluid).

For Romania, this means that once the AI Act becomes applicable (probably in 2025-2026, given that it entered into force on August 1, 2024, with a grace period), the courts will be legally bound to comply with the above-mentioned requirements. Failure to comply with them could attract sanctions, including fines at EU level (the AI Act provides for a GDPR-like compliance and sanctions regime, with market surveillance authorities and audit mechanisms). Therefore, the proposed governance model aligns with these requirements to ensure compliance from the outset.

Another effect of the inclusion of justice in the list of sensitive areas is that the funding of AI projects in justice at European level may be conditional on the existence of these risk management measures. Basically, the EU sends a clear message: "Yes, AI in justice, but do it carefully and responsibly." And the onus is on member states to implement governance systems that enable the benefits of AI without compromising basic principles of justice.

9. Practical Implementation: Governance Model in Romania (Proposal)

9.1. Proposed Institutional Structure

At the central (national) level, we propose the establishment of a National Committee for AI Governance in Justice (CN-GIAJ). It could function under the auspices of the SCM or as an inter-institutional body (Ministry of Justice + SCM + other actors). The composition would include: representatives of the CSM (judges, prosecutors), of the Ministry of Justice, independent technical experts (AI specialists), a representative of the ANSPDCP (taking into account personal data aspects) and representatives of civil society or the legal profession (with the role of observers, for transparency). The mandate of the committee would be to strategically coordinate all AI projects in justice: opinions, monitoring, best practice guides.

At the level of each large court (courts of appeal, tribunals) an AI Manager (for example, a clerk or IT specialist, under the supervision of the court president) could be appointed to keep track of the IA applications used locally, to ensure that procedures are followed (e.g., that logs are kept, that the parties are informed when necessary) and to report incidents or problems to CN-GIAJ. Local technology ethics commissions could also be established within courts to evaluate feedback from users and litigants.

This double structure – central and local – ensures both national unity in approach (through the Central Committee, which gives the line and standards), and local support where the actual use happens (through managers and local commissions that can quickly respond to everyday problems).

9.2. Procedures (Workflow)

The procedural flow proposed in section 5.3 should be adapted to the Romanian institutional context. Briefly summarizing and particularizing:

- **AI project initiation:** A court or the Ministry proposes a project (for example, the implementation of an intelligent case allocation system). The project is registered in the national AI register.
- **Algorithmic Impact Assessment (AIA):** The project team prepares the AIA report. May request support from CN-GIAJ for methodology.
- **CN-GIAJ opinion:** The National Committee examines the AIA report and issues an opinion (favorable / favorable with conditions / unfavorable). Without positive approval, the project cannot proceed to the pilot.
- **Controlled pilot:** If approved, the project is implemented as a pilot in one or two instances. Local AI managers are involved for monitoring. At the end of the pilot, an evaluation report is drawn up (including metrics such as RIU, incidents, etc.).
- **External audit:** The pilot report is independently audited (perhaps by the National Institute of Magistrates or an academic team from a law school and a computer science school, for example).
- **Approval of the extension:** CN-GIAJ, based on the audit, authorizes the extension of the system to other instances, possibly in stages. The central register is updated with the "operational" status of the system.
- **Current use:** In the current use phase, local AI managers monitor compliance with procedures (e.g., mentioning AI use in decisions, collecting logs). They work with IT departments for maintenance and clerks/court clerks for support.
- **Incident reporting:** If problems arise (technical or party complaints), the local IA manager fills out the AI Incident Register form and immediately alerts CN-GIAJ if the incident is major.
- **Incident Analysis:** CN-GIAJ meets (or delegates to a technical sub-committee) to analyze incidents and propose measures (e.g. system shutdown, technical fix, additional user training if the problem was misuse).
- **Feedback loop:** CN-GIAJ periodically issues recommendations or revises user guides based on lessons learned. The MoJ also proposes possible legislative adjustments (if a legal void or a contradiction between the law and the use of AI is found).

This process ensures that nothing is left to chance: each stage has checks and balances, involving both lawyers and technologists. Romania would thus become compliant with the AI Act and, at the same time, a pioneer in the development of a justice augmented by AI, but worthy of trust.

9.3. Resources and Training

The implementation of such a model requires dedicated resources:

- Financial resources: for the acquisition or development of AI systems (ideally, open-source or developed in partnership with universities, for transparency), for secure log storage infrastructure, for external audits, etc. European funds can be accessed (e.g. through justice digitization programs) to support these costs.
- Specialized human resources: there will be a need to recruit or train IT specialists within the judicial system (if not at every court, at least at the level of appeals courts) to technically support AI implementation. Also, judges and auxiliary staff must be partially relieved of their duties in order to be able to participate in specialized trainings.
- Continuing education programs: The National Institute of Magistracy (INM) should include artificial intelligence technology and ethics modules in its curricula. Similarly, the National School of Registrars can introduce practical modules on the use of AI tools (e.g. how to check an automatically generated abstract, how to use an AI-based case law search engine, etc.). These programs can be carried out in partnership with universities or with other countries that have similar initiatives.

An important aspect is the exchange of international best practices: since many EU countries will implement the AI Act in the judiciary, Romania should actively participate in European networks (such as CEPEJ working groups or pilot projects coordinated by the European Commission) to learn from the experience of others and make its own innovations known.

In essence, investing in AI governance is an investment in the future of justice. In the medium to long term, these allocated resources will be offset by the efficiency and quality of technology-augmented justice, as long as it is implemented responsibly.

10. Critical Discussions and Limitations

10.1. Anticipated Practical Problems

One of the main issues is the tension between transparency and trade secrecy of AI solution providers [6], [5], [9], [25]. If the court system purchases a solution from a private vendor, that vendor could invoke trade secrets on the algorithm. On the other hand, the judiciary needs transparency to maintain its credibility. Possible solutions: including in the contracts the supplier's obligation to provide access to independent audit of the algorithm, the use of open-source software when feasible, or at least controlled disclosure mechanisms (e.g. source code to be made available to a trusted third party, such as the National Institute of Magistrature, under confidentiality clauses).

Another issue is limited technical capacity and resources. Many courts in Romania still face a lack of IT staff or even outdated equipment. Introducing AI will require concurrent investments in infrastructure (servers, secure storage) and maintenance. If these investments are not made, there is a risk that AI projects will fail or, worse, create

vulnerabilities (for example, an inadequately secured system could become the target of cyber attacks, putting forensic data at risk).

Resistance to change is also something to consider. Some magistrates or support staff may be reluctant to use AI tools either due to lack of confidence or ignorance. This cultural barrier needs to be managed through dialogue and training – but there is a risk that if implementation is rushed or imposed from the top down, it will generate opposition.

Last but not least, the national legal framework may need to be adjusted. Although the AI Act will be directly applicable, specific changes in national legislation may be required (e.g. in the Judiciary Organization Act, to allow technological ethics committees, or in the rules of internal order of the courts, to explicitly stipulate the obligation to mention the use of AI in the motivation). Without such internal anchoring, some recommendations may remain at the level of unevenly applied best practices.

10.2. Further Research Needs

The present research has an exploratory and conceptual character. Future empirical studies are needed to validate (or invalidate) our hypotheses. For example, a pilot project in a court with partial implementation of the governance model would be useful to see how the proposed indicators work in practice and what adjustments they require.

Comparative assessments would also be valuable: how are other EU countries approaching the introduction of AI in justice? There are already projects in France, Holland, Estonia, etc. [17], [18], [14], [16, 24], [26] – a comparative study could inspire improvements of the Romanian model. For example, Estonia is testing a "robot judge" for petty claims; the results of that experiment (if transparent) would provide lessons about the limitations of AI in a decision-making role.

A necessary research direction is the development of sectoral technical standards. The AI Act provides for harmonized standards (Art. 40), but it would be useful for the judicial community to develop specific guidelines: what does "acceptable bias" mean in a legal algorithm? What level of accuracy should a judgment summary be to be used? Such questions can only be answered through interdisciplinary collaboration between lawyers, computer scientists and ethics experts, within dedicated working groups.

In conclusion, implementing AI in justice is an ongoing process that will evolve as technology advances and society clarifies its values and expectations. This paper represents a step in this conversation, but much remains to be explored.

11. Conclusions

11.1. Final Summary

The adoption of the AI Act fundamentally changed the landscape of AI regulation in the EU, establishing clear obligations for high-risk artificial intelligence systems and prohibiting certain uses deemed unacceptable. For the judicial system, this European

framework represents both a challenge and an opportunity: the challenge to integrate advanced technologies without compromising procedural rights and guarantees, and the opportunity to increase the efficiency and accessibility of justice through modern tools.

In this paper, we have argued that a responsible implementation of AI in justice requires a robust and multidimensional governance framework. We have proposed such a model, which includes: national registry of AI applications (for transparency and recordkeeping), pre-commissioning algorithmic impact assessments (to map and mitigate risks), strict logging and auditing policies (for traceability and accountability), explainability requirements tailored to the target audience (judges vs. litigants), mechanisms for challenging and redressing AI-influenced decisions, dedicated institutional structures (committees technical-legal-ethical) and professional training programs in the field of AI.

In essence, the legitimacy of human decision-making is not gained by completely excluding AI, but by designing, documenting and governing the use of AI in such a way that the responsibility remains, verifiably and irreversibly, with the judge. AI can be a valuable ally of justice – for example, to manage large volumes of information, identify jurisprudential patterns or reduce the length of trials – but only when it is used as a tool under human control and in a framework of trust.

Our work has highlighted that such integration is possible and desirable, provided there is a clear normative and ethical framework, the institutional will to implement it and a continuous process of evaluation and improvement. As technology evolves, adaptation will be needed, but the fundamental principles outlined by the AI Act and CEPEJ provide a clear compass: the human and his rights must remain at the center of the justice system, however sophisticated the ancillary tools become.

11.2. Recommendations

In the light of the above conclusions, we formulate some concrete recommendations, for immediate action, for decision-makers in Romania:

- Establishment of the National Committee (CN-GIAJ): Starting the procedures for the creation of the central body for the governance of AI in justice, with a clear mandate and the allocation of the necessary resources. It should immediately begin inventorying any existing AI initiatives in the judiciary.
- Implementation of the national registry of AI applications: Even before the implementation of the AI Act, such a registry can be established internally, to know exactly what AI-based prototypes or software already exist in courts/prosecutions (for example, maybe some courts use automatic translation tools, anonymization tools, etc.).
- Mandatory impact assessment (AIA): By order of the minister or decision of the CSM, establish the requirement that any proposal for the acquisition/development of artificial intelligence software for the courts be accompanied by an impact assessment (at least on rights and freedoms, if not a very detailed technical one). This step ensures that risk management thinking is internalized from the very beginning.

- Logging and Audit Policies: In collaboration with STS or other government IT bodies, develop a plan for instance-wide logging infrastructure and a periodic audit protocol. This also involves budgetary allocation for equipment and services.
- Legal Digital Literacy Programs: INM and SNG, possibly together with law schools and international partners, to rapidly initiate workshops/short courses for magistrates on what AI is, what the AI Act provides, and how it should be approached from a judicial perspective. The aim is that, until the entry into force of the European regulation, the professional body has a minimal conceptual baggage to navigate the new realities.

By implementing these immediate measures, Romania would proactively position itself in front of the wave of change brought by artificial intelligence in justice, transforming an obligation to comply into an opportunity for modernization and efficiency, without compromising on the justice act.

References

- [1] A. Ionescu, "Artificial intelligence in public administration: Between efficiency and ethics," *Journal of Public Administration*, vol. 7, no. 1, pp. 15–30, 2023.
- [2] M. Georgescu and A. Popescu, *Governance of Algorithms in Justice: Challenges and Solutions*. Bucharest, Romania: Universul Juridic, 2024.
- [3] M. Hildebrandt, *Smart Technologies and the End(s) of Law*. Cheltenham, U.K.: Edward Elgar, 2015.
- [4] M. Hildebrandt, *Law for Computer Scientists and Other Folk*. Oxford, U.K.: Oxford University Press, 2020.
- [5] European Parliament and Council, Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), *Official Journal of the European Union*, Jul. 12, 2024. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- [6] European Commission for the Efficiency of Justice (CEPEJ), "European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment," Council of Europe, Dec. 2018. [Online]. Available: <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>
- [7] European Parliament and Council, Regulation (EU) 2016/679 (General Data Protection Regulation), *Official Journal of the European Union*, vol. L 119, May 4, 2016. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [8] Article 29 Data Protection Working Party, "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679," WP251rev.01, Feb. 6, 2018; endorsed by the European Data Protection Board, May 25, 2018. [Online]. Available: https://www.edpb.europa.eu/documents/guideline/automated-decision-making-and-profiling_en
- [9] L. Edwards and M. Veale, "Slave to the algorithm? Why a 'right to explanation' is probably not the remedy you are looking for," *Duke Law & Technology Review*, vol. 16, pp. 18–84, 2017.
- [10] S. Wachter, B. Mittelstadt, and L. Floridi, "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation," *International Data Privacy Law*, vol. 7, no. 2, pp. 76–99, 2017.
- [11] E. Tabassi, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023, doi: 10.6028/NIST.AI.100-1.
- [12] S. Barocas, M. Hardt, and A. Narayanan, *Fairness and Machine Learning: Limitations and Opportunities*. Cambridge, MA, USA: MIT Press, 2023. [Online]. Available: <https://fairmlbook.org/>
- [13] S. Barocas and A. D. Selbst, "Big data's disparate impact," *California Law Review*, vol. 104, no. 3, pp. 671–732, 2016.
- [14] N. Aletras, D. Tsarapatsanis, D. Preotiuc-Pietro, and V. Lampos, "Predicting judicial decisions of the European Court of Human Rights: A natural language processing perspective," *PeerJ Computer Science*, vol. 2, Art. no. e93, 2016, doi: 10.7717/peerj-cs.93.

- [15] D. M. Katz, M. J. Bommarito II, and J. Blackman, “A general approach for predicting the behavior of the Supreme Court of the United States,” *PLOS ONE*, vol. 12, no. 4, Art. no. e0174698, 2017, doi: 10.1371/journal.pone.0174698.
- [16] M. Medvedeva, M. Vols, and M. Wieling, “Using machine learning to predict decisions of the European Court of Human Rights,” *Artificial Intelligence and Law*, vol. 28, pp. 237–266, 2020.
- [17] OECD, “Recommendation of the Council on Artificial Intelligence,” OECD/LEGAL/0449, May 22, 2019, amended 2024. [Online]. Available: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
- [18] European Commission, “Coordinated Plan on Artificial Intelligence: 2021 Review,” COM(2021) 205 final, Apr. 21, 2021.
- [19] J. A. Kroll et al., “Accountable algorithms,” *University of Pennsylvania Law Review*, vol. 165, no. 3, pp. 633–705, 2017.
- [20] F. Doshi-Velez and B. Kim, “Towards a rigorous science of interpretable machine learning,” arXiv:1702.08608, 2017.
- [21] R. Guidotti et al., “A survey of methods for explaining black box models,” *ACM Computing Surveys*, vol. 51, no. 5, Art. no. 93, 2018, doi: 10.1145/3236009.
- [22] C. Rudin, “Stop explaining black-box models in high-stakes decisions and use interpretable models instead,” *Nature Machine Intelligence*, vol. 1, pp. 206–215, 2019.
- [23] S. Wachter, B. Mittelstadt, and C. Russell, “Counterfactual explanations without opening the black box: Automated decisions and the GDPR,” *Harvard Journal of Law & Technology*, vol. 31, no. 2, pp. 841–887, Spring 2018.
- [24] A. Barredo Arrieta et al., “Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI,” *Information Fusion*, vol. 58, pp. 82–115, 2020, doi: 10.1016/j.inffus.2019.12.012.
- [25] J. Burrell, “How the machine ‘thinks’: Understanding opacity in machine learning algorithms,” *Big Data & Society*, vol. 3, no. 1, pp. 1–12, 2016.
- [26] C. Molnar, *Interpretable Machine Learning: A Guide for Making Black Box Models Explainable*, 2nd ed. Munich, Germany: Christoph Molnar, 2022.

Bridging the Digital Divide: Monitoring Smart Specialization and Digital Transformation in Regions of Moldova

Anatolie Babin, MBA

Academy of Economic Studies of Moldova, Chişinău, Republic of Moldova
anatolii.babin@ase.md

Sergiu Tutunaru

Academy of Economic Studies of Moldova, Chişinău, Republic of Moldova
tutunaru@ase.md

Ion Covalenco

National Research and Educational Network of Moldova, Chişinău, Republic of Moldova
ion.covalenco@renam.md

Abstract

This paper examines how strategic data governance and digital transformation monitoring can reduce the digital divide and support Smart Specialization Strategies (S3) in Moldova's regions. The study highlights the growing disparities between Chişinău and rural districts, where broadband penetration remains below 55% compared to over 85% in the capital, and innovation activities such as patent registrations are concentrated in less than 10% of localities. Objectives: The study examines how regional administrations can use a systematic process of data collection, analysis, and visualization to support smart specialization and digital transformation to strengthen entrepreneurial potential and innovation capacity. Prior work: Building on contributions in the SCRD Journal and relevant European methodologies, this study adapts EU legal frameworks (Data Governance Act, Data Act, and Open Data Directive) to Moldova's context. Approach: An integrated approach was applied, combining desk research, geostatistical mapping of broadband and patent activity, a multilevel methodology integrating LORDIMAS, JRC frameworks, and the Data Hub. Results: Findings confirm strong territorial asymmetries in infrastructure and institutional capacity. Rural administrations face fragmented data infrastructures and limited digital skills, which hinder effective S3 implementation. The authors introduce a comparative matrix for assessing regional digital readiness and identifying priority gaps. Implications: The paper stresses the need for EU-compliant data collection, sharing, and monitoring, alongside capacity-building for local governments. Concrete recommendations include establishing regional digital observatories, supporting innovation hubs, and promoting open data platforms at the municipal level. Value: This study provides one of the first integrated applications of LORDIMAS, JRC frameworks and Data Hub in an Eastern Partnership country. It offers original evidence and practical recommendations for designing inclusive, data-driven strategies to foster smart regional and rural transformation in Moldova. Additionally, establishing EDIHs initiatives can further accelerate digital innovation and capacity building at the regional level.

Keywords: data governance; LORDIMAS; regional innovation; European Digital Innovation Hubs; interoperability

1. Introduction

The digital transformation of Moldova's regions is a strategic tool for improving governance efficiency, stimulating innovation, and integrating the country into the European digital space. It aims to create a unified digital ecosystem capable of uniting municipalities, educational institutions, businesses, and the population, ensuring equal access to digital services and data. The goal of digital transformation is to ensure sustainable regional development, reduce digital and territorial inequalities, increase the competitiveness of border and rural areas, and prepare the regions for participation in European Union programs such as Digital Europe [1], the European Interoperability Act

[2], and the Smart Specialization (S3) initiative. The implementation of digital technologies in the regions faces a number of key challenges. Firstly, there is a digital divide between the Chisinau metropolitan area and rural or border areas, which manifests itself in limited access to high-speed internet, a lack of modern digital services, and weak infrastructure. Secondly, low levels of digital competence among municipal staff, teachers, and local innovation teams hinder the effective use of digital tools and participation in cross-border projects. Thirdly, limited institutional and organizational support creates difficulties in implementing comprehensive digital strategies, especially in rural and remote areas.

To overcome these challenges, a comprehensive approach is needed, including assessing the digital maturity of regions, developing digital competencies, implementing digital innovation platforms, and building a sustainable monitoring system. In Moldova, such a system is being developed using the LORDIMAS (Local and Regional Digital Maturity Assessment) methodology [3], which assesses the state of infrastructure, organizational readiness, and innovation activity of regions and integrates the results with European Digital Innovation Hubs (EDIHs) [4] and international indices such as the Regional Digital Readiness Indicators (RDRI). European Commission (JRC) methodologies are also being applied to assess the digital competencies of employees, educational institutions, and organizations, enabling the creation of digital capability maps and the development of targeted skills development programs. Thus, the digital transformation of Moldova's regions is not limited to technical solutions. It encompasses social and organizational aspects aimed at increasing municipalities' readiness to implement innovative solutions, activating civic participation, and ensuring sustainable development. The comprehensive implementation of the Moldova 2030 strategy envisions the gradual equalization of digital opportunities, the stimulation of innovation, and the integration of regions into the European digital ecosystem.

2. LORDIMAS Methodology and Digital Maturity

The digital transformation of regions requires a systematic approach to assessing the readiness of territories and municipalities to implement innovative solutions. In this context, the LORDIMAS methodology provides a structured tool for assessing digital maturity, taking into account both the technical infrastructure and the organizational and managerial readiness of regions.

2.1. Basic principles of LORDIMAS

The LORDIMAS methodology is based on several key principles:

- Multi-level assessment: the analysis is conducted at the level of individual municipalities, regional administrations, and inter-municipal cooperation, which allows us to identify both local and regional characteristics of digital maturity;
- Consideration of the socio-economic context: LORDIMAS takes into account population density, education level, infrastructure availability, and economic activity, allowing it to create an accurate picture of a region's readiness for digital transformation;

- Compatibility with European instruments: the methodology integrates with the DESI and RDRI, ensuring comparability of the digital maturity of Moldovan regions with the EU and supporting participation in cross-border initiatives.

LORDIMAS assesses four key dimensions of digital maturity: infrastructure, organizational readiness, staff competencies, and innovation activity. This multifaceted assessment allows for the identification of weaknesses and the prioritization of digital transformation priorities.

2.2. Six-stage model of digital maturity

To systematize differences between regions and set strategic goals, LORDIMAS uses a six-stage digital maturity model. The levels include (Table 1):

Table 1. Six-stage model of digital maturity of regions (adapted to Moldova)

Level	Description	Main disadvantages	Priority measures
1. Digital nascent	Minimum level of digitalization	Insufficient infrastructure, low digital literacy, lack of e-services	Investments in the internet, basic digital literacy, and digitalization of basic government services
2. Reactive (Digital reactivity)	Reacting to digitalization without a strategy	Lack of strategy, weak sustainability	Developing a strategy, improving coordination, and implementing proactive solutions
3. Developing (Digital development)	Partial implementation of technologies	Insufficient infrastructure, incompatible systems, limited funding	Infrastructure expansion, ensuring system compatibility, allocating funds
4. Intentional (Digital intent)	Strategy and active implementation	Lack of competence, weak citizen engagement, poor cybersecurity	Continuous education, citizen engagement, and improved cybersecurity
5. Optimized (Digitally optimized)	High level of integration	The need for innovation and personalization	Supporting innovation, adapting services to the needs of citizens, and scalability
6. Digital leader (Digital natives)	Best digital practices	Issues of sustainability, digital inclusion, data protection	Ensuring sustainability, promoting inclusivity, and high levels of data protection

Source: Author's development

This classification allows regional administrations to formulate differentiated digital transformation strategies, set priority areas, and compare Moldova's position with European regions.

2.3. Adaptation of LORDIMAS to Moldova and integration with EDIHs Network

Adapting the LORDIMAS methodology to the Moldovan context requires taking into account the specific characteristics of border and rural areas. High population migration, limited access to educational resources and infrastructure, low digital literacy, and weak support for innovation create unique challenges. The adaptation process is being implemented in several stages:

- Data collection: information on the state of infrastructure, access to broadband internet, the number of specialists, the availability of e-government services, and the level of digitalization of municipalities;
- Localization of the methodology: adjustment of categories, indicators and assessment scales taking into account the characteristics of regions and border areas;
- Piloting: testing the methodology in different regions with varying levels of digital maturity, identifying problem areas, and training municipal employees;
- Integration with EDIHs: connection to European Digital Innovation Hubs ensures continuous data updates, support for innovation platforms and monitoring of personnel competencies.

The resulting Regional Digital Readiness Index assesses municipalities' readiness to implement digital solutions across four dimensions: infrastructure, organizational readiness, competencies, and innovation. This index is used for comparative analysis, investment planning, and monitoring digital transformation progress.

The digital maturity of regions is determined not only by the availability of technical infrastructure, but also by the organizational and managerial readiness of local authorities. According to the National Bureau of Statistics (NBS) [5], six NUTS 3 administrative-territorial units demonstrate significant differences in internet access, digital device availability, and the level of digital competencies of the population. Figure 1 illustrates the level of internet penetration and digital infrastructure by region in Moldova.

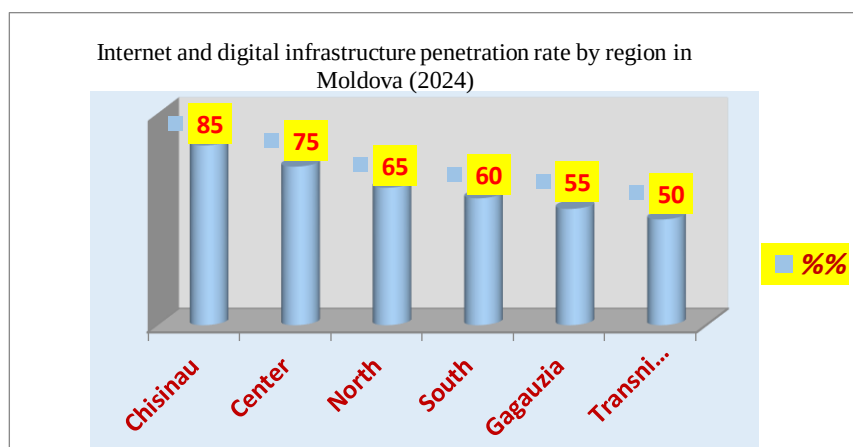


Fig. 1. Internet and digital infrastructure penetration by region.
Source: Authors' drawing based on NBS Moldova [5]

The figure demonstrates the differences between the capital region, where infrastructure is well-developed, and rural and border areas, where access to digital resources is limited. These differences have a direct impact on the ability to implement digital services and the

The National Development Strategy “European Moldova 2030” [6] is relevant to this effort. Adapting LORDIMAS also helps identify the specific needs of remote and border areas,

formulate measures to increase digital inclusion, and stimulate the local economy. Integration with EDIHs makes the system dynamic and ensures continuous data updates, which is critical for supporting long-term strategies and implementing Smart Specialization projects.

3. Developing digital competencies: JRC and EDIHs Network

The digital transformation of Moldova's regions is impossible without the systematic development of human capital. In this context, the digital competencies of municipal employees, teachers at educational institutions, and innovation sector organizations play a key role. A lack of skills in working with digital platforms and data management, a weak cybersecurity culture, and limited organizational capacity hinder the effective implementation of digital projects and the Smart Specialization (S3) strategy.

3.1. Assessing digital competencies using JRC

The methodologies of the European Commission's Joint Research Centre (JRC) – DigComp [7], DigCompEdu [8] and DigCompOrg [9] – provide a standardized tool for assessing competencies at the individual and institutional levels:

- DigComp - assesses individual employee skills: information search and analysis, communication, digital content creation, cybersecurity, and problem solving. It is used by municipal workers, librarians, social service providers, and NGOs;
- DigCompEdu - aimed at teachers and educational institutions; assesses educational organizations' readiness to implement digital technologies and their level of digital pedagogical competence;
- DigCompOrg - a tool for assessing organizational maturity: data management, digital leadership, ICT infrastructure, process digitalization, employee support, and interaction with external partners.

These tools provide a comprehensive picture of a region's level of digital maturity, identify gaps, and determine priority areas for training and development. To translate these diagnostic results into actionable capacity-building measures, the development of digital competencies is organized as a structured, six-step cycle. This framework links assessment, training design, piloting, scaling, and integration with European initiatives into a coherent process. Following the initial assessment stage, the next component of the competency development cycle focuses on planning and delivering targeted training programs. The steps are outlined below.

Step 1: Digital Competence Development Framework (Six-Step Model).

At the first stage, a systemic assessment is carried out using a combination of quantitative and qualitative methods:

- Standardized JRC questionnaires;
- Test tasks on information processing, content creation and solving typical problems;
- Digital portfolios of employees and teachers;
- Interviews and focus groups;

- Audit of organizational processes through DigCompOrg.

The diagnostic results are classified by level, from basic to advanced. Initial data shows that many municipalities possess basic skills (office applications, electronic communications), but struggle with data management, digital process organization, cybersecurity, and the integration of digital tools into project management. As shown in Figure 2, the LORDIMAS methodology [10] covers a wide range of digital maturity aspects: from service management and design to data management, technology, and connectivity. This approach provides a comprehensive assessment of the state of digital transformation and helps identify the strengths and weaknesses of regional administrations. In the Moldovan context, the application of LORDIMAS can contribute to the formation of a holistic picture of the digital development of territories and their comparison with EU regions using common assessment criteria. At the same time, the tool identifies existing gaps in local communities: insufficient digital competencies of local government employees and teachers, limited access to digital services for marginalized groups, and low citizen participation in digital initiatives. These factors directly impact the ability of regions to implement the “Republic of Moldova 2030 digital transformation strategy” [11] and participate in the “Digital Europe” program. These findings make it possible to move from diagnosing digital competencies to designing structured capacity-building programs.

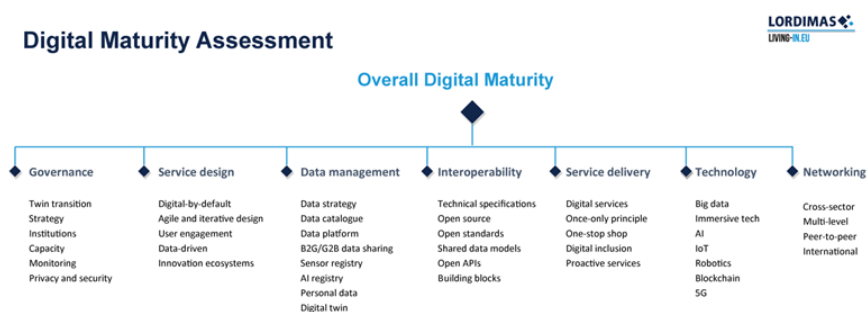


Fig. 2. Digital maturity assessment.

Source: [10]

Step 2: Designing Regional Digital Skills Development Programs (development of targeted courses for different categories of specialists).

Following the assessment of competencies, targeted professional development programs are developed, targeting specific categories of specialists:

- Municipal employees - courses on digital literacy, working with administrative information systems, data analysis and cybersecurity;
- Teachers and educational institutions - DigCompEdu trainings, practical classes on the implementation of digital tools in the educational process;
- Participants of local innovation ecosystems - seminars and workshops on digital project management, working with analytics, and preparing reports based on digital indicators.

Training programs are designed using an adaptive model that takes into account participants' initial skill levels, the specifics of their organizations, and regional circumstances. Individual and group development paths are created, simultaneously enhancing basic skills and preparing specialists for complex digital challenges. After designing the programs, the next stage is piloting them in selected municipalities and institutions, supported by the EDIHs Network.

Step 3: Piloting and Scaling with EDIH (program testing, data collection, scaling up successful practices). The effectiveness of the programs is assessed through pilot projects in selected municipalities and educational institutions. This is facilitated by the European Digital Innovation Hubs Network, which provides:

- Integration of online courses, digital laboratories and physical competence centers;
- Testing modules and interactive trainings with adaptation to local conditions;
- Conducting joint workshops to identify organizational and technical barriers;
- Collecting data on training results, including participant progress, implementation of new tools, and the effectiveness of digitalization of processes.

Based on pilot results, scaling strategies are developed, including the transfer of successful practices to other municipalities and educational institutions. Particular attention is paid to adapting to the infrastructural, personnel, and organizational characteristics of the regions. After successfully piloting and scaling digital learning programs, it is important to continue to build on these achievements. To ensure sustainable impact, it is necessary to regularly monitor the progress of participants and organizations, evaluate the implementation of new digital tools, and adjust educational and organizational measures according to identified needs. Monitoring allows us to identify weaknesses and build an evidence base for further improvement of the digital transformation of regions. Following the piloting phase, continuous monitoring and evaluation are required to measure progress and guide further improvements.

Step 4: Monitoring and evaluating program effectiveness, including:

- Analysis of progress of participants and organizations in digital competencies;
- Evaluation of the implementation of digital tools in municipal and educational processes;
- Adjusting training programs based on results.

As programs mature, the next priority is establishing mechanisms that ensure long-term continuity and sustainability of digital skills development.

Step 5: Institutionalization and sustainable development of competencies, including:

- Implementation of continuous training and certification systems;
- Creation of local centers of competence and exchange of experience;
- Formation of a strategy to support digital initiatives at the regional level.

Finally, to maximize impact and ensure alignment with broader strategic goals, regional initiatives must be connected to national and European digital transformation frameworks.

Step 6: Integration with national and European programs, including:

- Connection with the Digital Europe programme;
- Support for the “Republic of Moldova 2030 digital transformation strategy” [11];
- Comparison of regions with European practices and exchange of successful cases

Completing the digital transformation cycle at the regional level requires the creation of a sustainable competency development system capable of adapting to future challenges and innovations. Integration with national strategies and European programs opens up opportunities for sharing experiences, attracting resources, and building a unified roadmap for the country's digital development. This approach ensures the long-term effectiveness of initiatives and facilitates the emergence of digitally leading regions.

3.2. Integration of the EDIHs Network in Regional Digital Skills Development

After establishing the six-step model for developing digital competencies, it is important to identify the institutional mechanisms that ensure its practical implementation and scaling. In this context, the European Digital Innovation Hubs (EDIHs) network plays a key role. It provides access to specialized services, infrastructure, methodological support, and experimental platforms that enable municipalities and educational institutions to effectively implement digital transformation programs, develop human capital, and enhance the digital maturity of regions. To systematize the assessment of regional actors' digital competencies, JRC methodologies-DigComp, DigCompEdu, and DigCompOrg-are used. These approaches assess both the individual skills of staff and teachers and the organizational readiness of municipalities and educational institutions for digital transformation. Table 2 shows the main categories of digital competencies and the corresponding assessment methods, providing a basis for planning targeted training programs and creating roadmaps for human capital development in the regions.

Table 2. Main categories of digital competencies and methods of their assessment according to JRC

Category	Description	Assessment methods
Information literacy	Search, filter and analyze digital information	Tests, analytical tasks
Communication and cooperation	Using digital tools for interaction	Online projects, group work
Digital content creation	Creation of multimedia, texts and program code	Practical assignments, portfolio
Safety	Data protection, risk management	Threat simulations, tests
Problem solving	Application of digital tools for analysis	Cases, practical tasks
Organizational competencies	Digital Process Management	Audits, DigCompOrg

Source: Author's development

The digital competency assessment results presented in Table 2 serve as a starting point for developing individual and institutional professional development programs. They enable prioritization of training areas, identification of the needs of various categories of specialists, and planning of consistent skills development. Integration of this data with the EDIHs Network enables continuous monitoring of progress and the ability to tailor training programs to the actual needs of municipalities and educational institutions. To structure regional differences and prioritize digital transformation, a six-stage digital maturity model is used, allowing for classification of territories from the initial stage of digitalization to full digital leadership. The model covers the following levels (Fig.3):



Fig. 3. Levels of digital maturity.

Source: [12]

- Digital nascent – minimal infrastructure, low digital literacy, lack of electronic services;
- Digital reactivity – digital measures are taken in a fragmented manner, without a strategy;
- Digital development – the importance of digitalization is recognized, but the technologies are being implemented in a limited way;
- Digital intent – the presence of a strategy and active implementation of digital solutions;
- Digitally optimized – developed infrastructure, integrated processes;
- Digital native – leadership in digitalization, high degree of maturity and innovation.

A six-stage digital maturity model helps systematize differences between regions and identify key gaps in digital transformation. Each level reflects the degree of development of infrastructure, competencies, organizational readiness, and the implementation of innovative solutions. This classification facilitates comparison of Moldovan regions with European practices; helps prioritize strategic initiatives, and develop targeted measures to improve digital maturity at the municipal and regional levels. Together, these steps form an integrated framework that links skills assessment, training, experimentation, and long-term institutionalization. This ensures that digital competency development becomes a continuous and adaptive process aligned with regional and European priorities.

4. Bridging the Digital Divide and EDIHs Network

The digital divide between urban and rural areas in Moldova remains a key challenge to achieving a comprehensive digital transformation. In the capital and large municipal areas, such as Chisinau, the infrastructure and level of digital skills are sufficiently high, allowing for the effective use of electronic services and participation in innovative projects. However, rural and border areas face limited access to high-speed internet, low levels of digital literacy among the population and local administration staff, and insufficient support for innovation.

To overcome these challenges, a comprehensive strategy combining infrastructure development, user training and support, the implementation of modern technologies, and the creation of a sustainable monitoring system is critical. European Digital Innovation Hubs [13] act as centers of competence and coordination, providing technical support, educational modules, and platforms for interaction between municipal administrations, educational institutions, businesses, and the civil society.

One of the key tools for bridging the digital divide [14] is the creation of digital and physical access points providing residents with access to the internet, educational resources, and government services. These points can be located in schools, libraries, municipal centers, and other public spaces. They provide not only technical access but also support staff capable of consulting users, assisting with online services, and conducting training sessions. A key component is the implementation of targeted training and courses on digital literacy. These programs aim to enhance the competencies of municipal employees, teachers, students, and representatives of local innovation ecosystems. Training covers information systems, basic and advanced digital skills, data security, information processing, and the use of collaboration platforms. Partnerships with businesses and startups are also an effective tool, integrating practical training, internships, and joint projects within regional initiatives. This collaboration stimulates the development of an innovation ecosystem, strengthens ties between educational institutions and businesses, and supports the development of entrepreneurial skills among young people and aspiring professionals.

An equally important aspect is the use of online platforms and educational portals, which allow residents, regardless of geographic location, to access educational materials, distance learning courses, and interactive tools. These platforms facilitate remote learning, collaborative project work, and knowledge sharing across regions. Below is a table listing the main EDIHs tools, their target audience, expected impact, and examples of successful practice in EU countries.

Table 3. EDIHs tools for reducing the digital divide

Tool	Target audience	Effect	The EU example
Digital + Physical Access Points	Marginalized groups	Access to the Internet and education	Smart Villages
DigComp training modules	Teachers, students	Developing digital skills	Living-in.EU
Partnerships with business	Startups, youth	Internships, practical training	EU Smart Hubs
Online platform	Population	Access to services and content	Smart Education Portals

Source: Author's development

The use of these tools allows regional administrations and educational institutions not only to narrow the digital divide but also to develop long-term skills development strategies integrated with the Smart Specialization concept. The combination of digital and physical resources creates conditions for a more equitable distribution of opportunities between urban and rural areas and promotes sustainable digital transformation in the regions. Particular attention is paid to marginalized groups—the elderly, people with disabilities, rural residents, and young people in remote villages. Adapted training programs are being developed for them, including both in-person classes at access points and distance learning courses on online platforms. EDIHs also serve as a coordinating center for monitoring and evaluating the effectiveness of initiatives. Collecting data on access point attendance, learning outcomes, participant engagement, and the level of skills acquired allows for real-time adjustments to programs. This ensures the dynamism and adaptability of the system, minimizes the risks of uneven development, and increases the effectiveness of investments in digital transformation. Thus, the integrated use of digital and physical access points, DigComp educational modules, partnerships with businesses, and online platforms allows for the equalization of digital capabilities across regions, the enhancement of the competencies of employees, teachers, and the general public, and the promotion of participation in cross-border projects and Smart Specialization initiatives

5. Integrated model for digital maturity management

To successfully transform Moldova's regions digitally, it is necessary to combine various approaches to assessing, developing, and monitoring digital maturity into a single, integrated model. Such a model not only systematizes data on competencies, infrastructure, and digital services but also transforms them into a practical strategic management tool.

The integrated model combines three key functions: assessment, development, and monitoring, ensuring the continuous improvement of the regions' digital capabilities. Model functions:

1. Evaluation. Assessing digital maturity is the model's foundational stage and includes a comprehensive assessment of all key components of a region's digital transformation. This process utilizes the following approaches:

- Assessment of the competencies of employees and educational organizations using JRC methods (DigComp, DigCompEdu, DigCompOrg), which allows us to determine the level of knowledge and skills in working with digital tools, organizational readiness and the ability to implement innovations;
- Assessment of infrastructure and digital services using LORDIMAS, including analysis of internet accessibility, equipment, software solutions and the quality of digital services provided;
- Comparative analysis [15] and international reference using RDRI and comparison with practices of European regions through the EDIHs Network.

The assessment results form a map of the region's digital maturity, identifying risk areas, weaknesses, and potential opportunities for development.

2. Development. Based on the diagnostic results, competency and infrastructure development programs are being developed to address identified gaps and improve the effectiveness of digital transformation. Key development areas include:

- Training and professional development for municipal administration employees, teachers, and representatives of the local innovation ecosystem through thematic courses, trainings, and workshops of DigComp and DigCompEdu;
- Infrastructure development, including expanding internet access, creating digital and physical access points, upgrading equipment and introducing modern digital platforms;
- Support for cross-border initiatives of the Border Data Hub [16], which provides for the participation of Moldovan regions in joint projects with neighboring countries, exchange of experience and the use of best EU practices through EDIHs;
- Creating an environment for innovative activity, including partnerships with businesses, start-ups, and scientific institutions, and the formation of educational and laboratory hubs.

3. Monitoring. Monitoring ensures continuous tracking of digital maturity dynamics and the effectiveness of measures taken. Key monitoring mechanisms include:

- Regular collection of data through the EDIHs Network and Data Hub on competencies, infrastructure, use of digital services, and the level of public engagement;
- Analytical panels [17] and dashboards that allow you to visualize the progress of regions compare indicators between municipalities and evaluate the effectiveness of investments;
- Forecasting and development modeling, which helps formulate scenarios for digital maturity growth, plan resources, and adjust strategies based on changes in the region and external environment.

4. Effects of the integrated model. The application of an integrated digital maturity management model has a comprehensive impact on regional development and the formation of an innovation ecosystem:

- Equalization of digital opportunities between metropolitan and rural areas [18], which helps reduce territorial inequality and ensure equal access to digital resources and educational programs;
- Support for cross-border initiatives, including joint projects with neighboring countries, knowledge exchange, and the creation of cross-border innovation clusters;
- Formation of a mature digital ecosystem where competencies, infrastructure, processes and services are interconnected, support innovation and create a sustainable basis for the implementation of Smart Specialization strategies;
- Improving the efficiency of strategic planning through the integration of assessment, monitoring and forecasting data into a single analytical system;
- Stimulating investment and attracting external resources, as the availability of systematized data on the digital maturity of regions increases the transparency and validity of decisions for public and private investors.

The integrated digital maturity management model transforms digital competencies and infrastructure into a strategic resource, ensuring sustainable growth and competitiveness in Moldova's regions. It links diagnostic data with development programs and monitoring, creating a cyclical process of continuous improvement, where each new program iteration enhances the overall digital maturity of the region and promotes the sustainable development of local communities.

6. Conclusions and recommendations

An analysis of the digital maturity of Moldova's regions reveals significant regional disparities. The Chisinau metropolitan area boasts a high degree of digital maturity, developed infrastructure, and a competent workforce, while rural and border areas face limited internet access, low levels of digital competencies, and weak organizational support for innovation. This asymmetry hinders the implementation of Smart Specialization projects and requires targeted measures to equalize opportunities across regions. The strategic role of human capital is particularly important: the competencies of municipal administration employees, educators, and representatives of the local innovation ecosystem are becoming a key resource for the implementation of digital initiatives and innovative projects. A lack of skills [19] in data management, cybersecurity, and digital process management limits effectiveness even when the necessary infrastructure is in place.

The effectiveness of an integrated approach based on the combined application of LORDIMAS [20], JRC (DigComp, DigCompEdu, DigCompOrg [21]) methodologies, and the EDIHs Network is demonstrated by the possibility of comprehensive monitoring, systemic diagnostics, and targeted competency development. This model ensures data comparability across municipalities, integration with international practices, and supports strategic-level digital transformation planning. Based on the analysis, the following specific recommendations are proposed:

1. Human resource development, including:

- Implementation of targeted educational programs and trainings on DigComp and DigCompEdu for municipal employees, teachers, and teams of local innovation ecosystems;
- Creation of digital hubs and competence centers for knowledge sharing and practical training;
- Support for continuous professional development and mentoring, including participation in international projects and cross-border initiatives.

2. Monitoring and analytics, including:

- Using the EDIHs Network to continuously collect and analyze data on digital skills, infrastructure, and regional readiness to implement innovations;
- Regular comparative assessments of municipalities [22] to adjust strategies, identify priority areas and plan investments;
- Implementation of dynamic dashboards and analytical tools to forecast digital maturity development.

3. Bridging the digital divide, including:

- Expanding access to digital infrastructure in rural and marginalized communities;
- Organizing trainings, creating partnerships with businesses and startups, and providing online platforms to improve digital literacy among the population;
- Implementation of digital and physical access points to ensure equal opportunities for learning and receiving services.

4. Integration with Smart Specialization, including:

- Inclusion of data on digital competencies in the process of planning innovative projects and cross-border cooperation;
- Formation of joint clusters and investment priorities based on monitoring and analysis of the digital maturity of regions;
- Using integrated data for strategic planning and long-term development of the regional innovation ecosystem.

Thus, implementing these recommendations will help equalize digital opportunities between urban and rural areas, create a mature digital ecosystem, ensure sustainable integration of Moldova's regions into cross-border initiatives, and improve the effectiveness of Smart Specialization strategies. The integration of competencies, infrastructure, and monitoring creates the foundation for the country's long-term and balanced digital development.

References

- [1] European Commission, “Digital Europe Programme (DIGITAL),” 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>
- [2] European Parliament and Council, Regulation (EU) 2024/903 of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act), Official Journal of the European Union, Mar. 22, 2024. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2024/903/oj>

- [3] ESPON EGTC, “Digital maturity of local and regional governments, 2024,” final report, Dec. 2024. [Online]. Available: <https://www.espon.eu/publications/lordimas-digital-maturity-local-and-regional-governments-2024-final-report>
- [4] G. Rissola and J. Sörvik, *Digital Innovation Hubs in Smart Specialisation Strategies*, EUR 29374 EN. Luxembourg: Publications Office of the European Union, 2018, doi: 10.2760/475335.
- [5] National Bureau of Statistics of the Republic of Moldova, “Regional statistics.” [Online]. Available: https://statistica.gov.md/en/statistic_indicator_details/29
- [6] Government of the Republic of Moldova, “National Development Strategy ‘European Moldova 2030,’” 2022. [Online]. Available: <https://mediu.gov.md/ro/content/4119>
- [7] European Commission, Joint Research Centre, “Digital Competence Framework for Citizens (DigComp).” [Online]. Available: https://joint-research-centre.ec.europa.eu/projects-and-activities/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp_en
- [8] European Commission, Joint Research Centre, “European Framework for the Digital Competence of Educators (DigCompEdu).” [Online]. Available: https://joint-research-centre.ec.europa.eu/digcompedu_en
- [9] P. Kampylis, Y. Punie, and J. Devine, *Promoting Effective Digital-Age Learning: A European Framework for Digitally-Competent Educational Organisations*, EUR 27599 EN. Luxembourg: Publications Office of the European Union, 2015, doi: 10.2791/54070.
- [10] ESPON EGTC, “LORDIMAS: Digital Maturity Assessment for Local and Regional Governments.” [Online]. Available: <https://lordimas.espon.eu/>
- [11] Ministry of Economic Development and Digitalization of the Republic of Moldova, “Digital Transformation Strategy 2023–2030.” [Online]. Available: <https://mded.gov.md/transparency/digital-transformation-strategy-2023-2030/>
- [12] Agência para a Modernização Administrativa, “Framework for Local and Regional Action Plans,” Portugal DigitalGov, Dec. 27, 2024. [Online]. Available: <https://digital.gov.pt/documentos/framework-para-planos-de-acao-local-e-regional>
- [13] European Commission, “European Digital Innovation Hubs in the Digital Europe Programme,” 2019. [Online]. Available: https://errin.eu/system/files/2020-02/European%20Digital%20Innovation%20Hubs%20in%20Digital%20Europe%20Programme_2019-12-02.pdf
- [14] A. Babin, R. Ciloci, and N. Davydenko, “Perspectives of sustainable development of cluster organizations through internationalization and dual use,” *Smart Cities and Regional Development*, vol. 9, no. 3, pp. 99–120, 2025, doi: 10.25019/0hbt367.
- [15] M. Navarro, J. J. Gibaja, S. Franco, A. Murciego, C. Gianelle, F. B. Hegyi, and A. Kleibrink, “Regional benchmarking in the smart specialisation process: Identification of reference regions based on structural similarity,” *S3 Working Paper Series*, no. 03/2014, 2014. [Online]. Available: https://joint-research-centre.ec.europa.eu/reports-and-technical-documentation/regional-benchmarking-smart-specialisation-process-identification-reference-regions-based-structural_en
- [16] European Commission, Joint Research Centre, “Cross-Border Data Hub.” [Online]. Available: <https://territorial.ec.europa.eu/across?lng=en&ctx=ACROSS>
- [17] A. Babin, T. Colesnicova, and S. Tutunaru, “Developing the European Villages in the Republic of Moldova taken into account the Digital Economy Society Index (DESI),” *Smart Cities and Regional Development*, vol. 7, no. 2, pp. 39–47, 2023, doi: 10.25019/eeafre59.
- [18] European Commission, “European Data Governance Act,” 2022. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act>
- [19] European Commission, “Digital Skills Indicator 2.0: Measuring Digital Skills across the EU.” [Online]. Available: <https://digital-skills-jobs.europa.eu/en/learning-space/resources/digital-skills-indicator-20-measuring-digital-skills-across-eu>
- [20] METREX, “Mapping METREX: ESPON LORDIMAS system,” 2025. [Online]. Available: <https://www.eurometrex.org/activities/metrex-expert-groups/mapping-metrex/>
- [21] ALL DIGITAL, “DigComp-related Communities of Practice,” 2024. [Online]. Available: <https://all-digital.org/communities-of-practice/>
- [22] Smart-EDU Hub, “Smart-EDU Hub,” 2025. [Online]. Available: <https://www.smart-edu-hub.eu/>

Digital Twins and MIS Integration for Urban Resilience: A Strategic Approach to Smart City Evolution

Frida Zisko

Mediterranean University of Albania, Tirana, Albania
besjana.mema@umsh.edu.al

Besjana Mema

Mediterranean University of Albania, Tirana, Albania
besjana.mema@umsh.edu.al

Abstract

The evolution of smart cities has accelerated the adoption of real-time digital infrastructures capable of sensing, processing, and simulating urban dynamics. Digital Twin technology, defined as a virtual replica of physical city systems, offers significant potential for predictive scenario modeling and resilience planning. However, most Digital Twin implementations remain fragmented and limited to technical or engineering layers, lacking integration with Management Information Systems (MIS), which are essential for strategic decision-making, interdepartmental coordination, and governance intelligence. This paper proposes a novel MIS–Digital Twin integration framework designed to enhance urban resilience and predictive governance in smart city ecosystems. The study applies a systematic literature synthesis to identify gaps in the current deployment of digital urban platforms and develops a multi-layered architecture that connects Digital Twin data layers with MIS-driven governance dashboards. A scenario-based application in urban resilience management is conceptualized to demonstrate how MIS-enabled Digital Twins can support proactive policy formulation, resource allocation, and risk monitoring. The conceptual analysis suggests that embedding Digital Twin simulations within MIS structures enables a shift from reactive city management towards intelligent, simulation-driven decision systems that improve transparency, preparedness, and adaptive governance. The proposed model contributes academically by positioning MIS as a strategic layer in Digital Twin research and offers municipal authorities a scalable blueprint for implementing data-informed resilience strategies. Drawing on sociotechnical systems theory, the framework distinguishes five linked layers: physical sensing, data integration, Digital Twin computation, MIS governance, and decision intelligence. The illustrative flood scenario follows sensor inputs through simulation, dashboard interpretation, early warning, and coordinated municipal action. Because the study develops a conceptual architecture rather than testing a deployed system, its proposed performance and resilience benefits require empirical validation in municipal settings.

Keywords: predictive governance; decision intelligence; interoperability; flood risk management; municipal information systems

1. Introduction

The rapid evolution of smart cities over the past decade has been driven by an accelerated wave of digital transformation, marked by real-time sensing infrastructures, pervasive connectivity, and advanced computational ecosystems [1], [2]. Cities are increasingly deploying Internet of Things (IoT) networks, edge computing systems, and cyber-physical platforms to monitor environmental and operational conditions as they occur, creating new possibilities for situational awareness and automated urban management [3], [4]. Within this expanding digital landscape, Digital Twin (DT) technology has emerged as one of the most transformative innovations. Defined as a virtual replica of physical systems continuously updated through real-time data streams, Digital Twins enable cities to simulate, predict, and optimize complex urban processes [5], [6], [7].

Despite this potential, most current Digital Twin implementations remain fragmented and confined to technical or engineering domains—such as mobility models, infrastructure monitoring, and energy-flow analyses—while lacking integration with the strategic and administrative layers required for holistic city governance [8], [9]. This limitation constrains the ability of Digital Twins to contribute meaningfully to city-wide coordination, long-term planning, and resilience strategies. Management Information Systems (MIS), traditionally recognized for facilitating data consolidation, organizational coordination, and governance intelligence, offer a complementary capability that has been overlooked within mainstream Digital Twin research [10], [11]. MIS can act as a strategic layer that transforms raw simulation outputs into actionable insights for policymakers, thereby enhancing transparency, interdepartmental alignment, and predictive decision-making.

Growing urban vulnerabilities—ranging from climate-related shocks to infrastructure failures—intensify the need for integrated governance tools that link technical simulations with administrative decision systems [12]. Integrating Digital Twins into MIS platforms would allow cities to shift from reactive management toward proactive, simulation-driven predictive governance. Through such integration, municipalities can test resilience scenarios, anticipate disruptions, allocate resources effectively, and implement adaptive strategies guided by reliable predictive analytics [13], [14].

This paper responds to this emerging need by proposing a novel MIS–Digital Twin integration framework designed to enhance urban resilience and predictive governance within smart city ecosystems. Although digital urbanism is increasingly interdisciplinary, current scholarly discourse offers limited conceptualizations that bridge digital engineering architectures with MIS-driven governance mechanisms. To address this gap, the study poses three research questions: (1) How can MIS enhance the strategic value of Digital Twin ecosystems? (2) What multi-layered architecture supports effective DT–MIS interoperability for resilience planning? and (3) How does MIS-enabled DT integration improve predictive governance and scenario-based urban management?

By exploring these questions, the paper aims to contribute to both theory and practice by positioning MIS as a critical component of next-generation Digital Twin-enabled governance for resilient, data-informed smart cities.

2. Literature Review

2.1. Smart City Evolution and Digital Urban Infrastructures

Smart city development has been shaped by global trends in digital transformation, real-time data acquisition, and urban-scale computational systems. Early smart city models focused primarily on ICT-enabled service efficiency, but contemporary approaches emphasize adaptive, data-driven governance supported by continuous sensing and urban intelligence [2], [1]. Through the deployment of Internet of Things (IoT) devices, edge computing nodes, and high-throughput data pipelines, cities can now collect granular, real-time observations on mobility flows, environmental changes, infrastructure conditions, and citizen behavior [3], [4]. These infrastructures form the backbone of digital urban

ecosystems and enable the integration of advanced simulation technologies—such as predictive modeling, cyber-physical analytics, and automated response systems—into urban management.

However, despite these advancements, many cities struggle with fragmented data environments where sensing infrastructures operate in silos across departments or private providers. Such fragmentation undermines holistic governance and limits the ability to derive cross-sector insights necessary for resilience planning and integrated decision-making [5]. Without unified data architectures, cities cannot leverage the full potential of simulation technologies for proactive governance, highlighting the need for interoperable digital platforms that bridge operational, analytical, and administrative domains.

2.2. Digital Twin Technology in Urban Contexts

Digital Twin (DT) technology has become central to discussions on smart urban transformation due to its capacity to create dynamic, continuously updated virtual representations of physical systems [9], [6], [7]. A Digital Twin typically comprises four interconnected components: (1) the physical layer, representing real-world infrastructure; (2) the data layer, which aggregates sensor-generated data streams; (3) the computational model, responsible for analytical processing; and (4) the simulation engine, which enables scenario evaluation, prediction, and optimization [5], [6]. These multi-layered DT structures allow planners and decision-makers to test hypothetical interventions, evaluate system vulnerabilities, and predict the outcomes of various actions before implementing them in the physical environment.

Urban Digital Twins have been applied in a wide range of domains, including mobility and traffic management, energy distribution, building performance optimization, environmental monitoring, and disaster preparedness [5], [6]. For instance, mobility DTs offer real-time travel simulations, while energy DTs optimize consumption patterns and grid performance. Environmental DTs support air quality modeling and flood prediction.

Despite their potential, many existing DT deployments remain specialized and operationally isolated. They typically focus on engineering functions rather than governance processes, resulting in siloed implementations that are not integrated into municipal administrative workflows [8], [9]. This fragmentation limits the ability of Digital Twins to inform high-level decision-making, policy formulation, and cross-sector resilience strategies.

2.3. Management Information Systems in Urban Governance

Management Information Systems (MIS) play a crucial role in modern public administration by supporting planning, coordination, data consolidation, transparency, and strategic decision-making [10], [11]. In the context of digital cities, MIS platforms enable municipal authorities to aggregate information across departments, visualize operational indicators, and monitor performance metrics relevant to service delivery and urban development. MIS have evolved significantly alongside e-government advancements,

transforming from static reporting tools into interactive decision-support systems capable of real-time analytics, workflow management, and strategic forecasting [15], [16].

Yet, despite their importance, MIS are rarely connected to the engineering-driven analytical outputs of Digital Twins. City dashboards designed for policymakers typically lack access to simulation engines and real-time feedback loops that characterize Digital Twins [8]. This weak linkage results in decision-making environments where advanced urban simulations operate separately from governance structures, limiting the use of DT insights in policy development and resilience planning. This separation underscores the need for MIS architectures that can interface with Digital Twin systems, enabling holistic urban intelligence.

2.4. Gaps in Current Digital Twin and MIS Research

Across the literature, Digital Twins are predominantly conceptualized as technical or engineering tools, while their use as strategic governance mechanisms remains underexplored [9], [5], [6]. Existing studies focus heavily on the technological aspects of DT construction—data acquisition, simulation accuracy, computational design—while paying limited attention to how these systems can be embedded within governance frameworks and decision-making structures.

Furthermore, Digital Twin research rarely integrates the concept of decision intelligence or policy-driven analytics, features that are essential for resilience-oriented city management [13], [17]. The absence of administrative, organizational, and MIS-oriented layers prevents Digital Twins from contributing to broader governance objectives such as transparency, accountability, and coordinated resource allocation.

This reveals a clear research gap: the field lacks a comprehensive framework in which MIS functions as a strategic integrator between Digital Twin outputs and urban governance processes. Addressing this gap is essential for transforming Digital Twins from isolated simulation tools into core components of predictive, data-informed, and resilient urban management systems. The proposed framework developed in this paper responds directly to this gap by positioning MIS as the governing layer that operationalizes Digital Twin intelligence for city-wide decision-making.

3. Methodology

3.1. Research Design

This study employs a multi-stage methodological design combining systematic literature synthesis, conceptual framework development, and scenario-based illustration. The overall design is grounded in sociotechnical systems theory, which emphasizes the interdependence between technological infrastructures and organizational governance structures [15]. This theoretical orientation is particularly relevant for understanding how Digital Twin (DT) technologies interact with Management Information Systems (MIS) within urban environments.

The first stage involved conducting a systematic literature synthesis to map the current state of Digital Twin technologies, MIS applications, and urban resilience frameworks. Peer-reviewed sources were retrieved from Scopus, Web of Science, and IEEE Xplore using combinations of keywords such as Digital Twin, smart cities, urban resilience, management information systems, and predictive governance. Following PRISMA-style inclusion criteria, studies were selected if they: (1) examined DT or MIS in urban contexts, (2) discussed governance or decision-support applications, or (3) addressed interoperability challenges.

The second stage focused on developing a conceptual MIS–Digital Twin integration framework. Insights from the literature were synthesized using a sociotechnical systems lens to identify technological, organizational, and governance requirements for integrated digital urban platforms [15]. The framework was shaped through iterative abstraction, identifying core layers and data flows connecting Digital Twin computational engines with MIS governance dashboards.

Finally, a scenario-based design method was adopted to illustrate the application of the proposed framework. Scenario-based research is commonly used to analyze potential system behavior under specific conditions, especially in urban resilience and simulation studies [13]. The scenario developed in this study demonstrates how MIS-enabled Digital Twins could support predictive governance in a critical urban resilience context.

3.2. Data Sources

The study draws upon multiple categories of data and documentary evidence. The primary sources include peer-reviewed academic literature from Scopus, Web of Science, IEEE Xplore, ACM Digital Library, and SpringerLink. These sources provide theoretical grounding and empirical examples of Digital Twin applications, smart city infrastructures, and MIS-driven governance models.

In addition to academic literature, industry reports and technical documentation from leading organizations such as Deloitte, Siemens, and IBM were reviewed to capture current trends in Digital Twin platforms, urban simulation tools, and data interoperability technologies [6]. These reports offer practical insights into how such systems are implemented in real-world contexts.

Furthermore, municipal governance guidelines and global resilience frameworks were consulted to align the proposed integration model with contemporary policy and planning standards. Relevant resources include the United Nations Office for Disaster Risk Reduction (UNDRR) Resilience Guidelines, the European Union Smart City Framework, and the C40 Cities urban climate resilience strategies [18], [8]. These documents ensure that the proposed framework aligns with established urban resilience and predictive governance objectives.

3.3. Analytical Approach

The analytical process employed in this study consisted of three complementary steps. First, thematic clustering was conducted on the reviewed literature to identify recurring challenges, opportunities, and patterns related to Digital Twin deployment, MIS utilization, and urban resilience needs. Thematic coding was implemented to group insights into categories such as interoperability, governance integration, data flow design, and resilience indicators [19].

Second, architecture modeling techniques were used to construct the MIS–Digital Twin integration framework. This involved mapping the relationships among physical infrastructures, data acquisition layers, simulation engines, decision-support dashboards, and governance workflows. The approach adapts established methods of systems architecture design commonly used in smart city and cyber-physical system studies [20].

Third, scenario development was employed to validate the conceptual framework. Scenarios are effective analytical tools for examining how digital systems may behave under complex, uncertain conditions and for demonstrating the potential impact of technological integration on decision-making processes [21]. The scenario constructed in this study illustrates the role of MIS-enabled Digital Twins in supporting proactive urban resilience management.

4. Proposed MIS–Digital Twin Integration Framework

4.1. Conceptual Overview

The proposed MIS–Digital Twin Integration Framework reconceptualizes the relationship between operational data environments and municipal governance by placing the Management Information System at the center of decision-making processes [22], [23]. Although Digital Twins are capable of generating real-time simulations, forecasting system behaviors, and modeling urban dynamics at high fidelity, their value is significantly reduced when these outputs remain confined to technical domains. By embedding Digital Twin intelligence directly within MIS dashboards, cities can transform simulation results into governance actions, enabling a shift from traditional reactive management to anticipatory, predictive governance. In this model, MIS acts as the strategic interface through which data flows, simulation outputs, and administrative processes converge, creating a unified platform for resource allocation, early warning mechanisms, resilience planning, and cross-departmental coordination. Consequently, the integration turns Digital Twins into a policy-oriented asset that supports long-term strategic planning and real-time operational oversight [24].

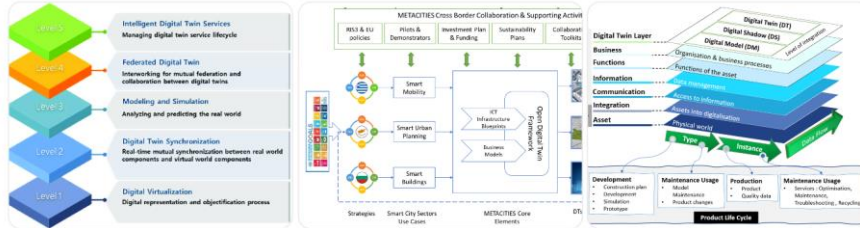


Fig. 1. MIS–Digital Twin Integration Architecture

Figure 1 visualizes the five-layer architecture, beginning with the physical sensing infrastructure and progressing upward through data integration, simulation logic, MIS governance tools, and AI-driven decision intelligence.

4.2. Multi-Layered Framework Architecture

The five-layer architecture that supports this integration operates as a continuous vertical system rather than a collection of isolated modules. At the foundational level, physical infrastructure and IoT devices continuously generate real-time observations from the city, capturing information related to mobility conditions, energy consumption, environmental factors, water systems, and structural performance. These data streams move into the data layer, where a unified data lake aggregates, standardizes, and secures them through interoperability protocols and API connections [25]. This layer ensures that every dataset—regardless of origin—becomes compatible with simulation engines and governance tools.

Above the data foundation lies the Digital Twin computational layer, which performs the complex processes of modeling, simulation, and scenario forecasting. Real-time calibration ensures that the virtual representation accurately reflects the physical city, allowing simulations to predict disruptions, estimate infrastructure stressors, and test resilience scenarios. This computational intelligence is then translated into actionable knowledge in the MIS governance layer, where municipal administrators can visualize system performance, evaluate risks, coordinate responses, and benchmark service delivery. The final decision intelligence layer uses advanced analytics to generate automated alerts, risk scoring assessments, and strategic reports, thereby assisting policymakers in anticipating issues before they escalate and optimizing resource allocation.

The following table summarizes the major functions of the data layer as applied within this framework [26], [27].

Table 1. Key Functional Elements of the Data Integration Layer

Component	Purpose
Data Lake	Provides unified storage for both raw and processed data, supporting scalable analytics and long-term record preservation.
API Integration	Enables automatic communication between technical systems, simulation engines, and MIS dashboards.
Data Governance Rules	Ensures that incoming data adhere to standards of security, quality, consistency, and traceability.
Interoperability Hub	Facilitates seamless cross-departmental data exchange, reducing fragmentation and enabling synchronized decision-making.

This table represents how the data layer forms the structural backbone of the integration model by ensuring that information originating from diverse urban systems becomes usable for both predictive simulation and administrative governance.

4.3. Governance and Interoperability Considerations

The successful implementation of an MIS–Digital Twin ecosystem depends on a governance structure that ensures transparency, ethical data use, and secure information flows. Integrating real-time simulation data with municipal decision-making processes requires formalized agreements across departments to guarantee consistent data sharing and adherence to common standards. Transparent governance mechanisms strengthen public trust, especially when predictive models influence decisions involving resource distribution or emergency interventions. Ethical considerations, including the protection of personal data, the mitigation of algorithmic bias, and the communication of predictive outcomes to the public, must be embedded into the system’s design. Furthermore, cybersecurity protections—such as encryption, intrusion detection, and compliance with international standards—are essential to safeguard IoT devices and Digital Twin models against vulnerabilities [28]. When these governance principles are applied, the MIS–Digital Twin framework becomes not only technically functional but also institutionally responsible, resilient, and aligned with democratic values of accountability and fairness.

5. Scenario-Based Application: Urban Resilience Management

5.1. Scenario Context

To demonstrate the operational value of the MIS–Digital Twin integration framework, a scenario involving urban resilience management is developed using a realistic stress condition frequently encountered in metropolitan areas. Flood risk is selected as the primary scenario because it represents one of the most pervasive and disruptive challenges faced by contemporary cities. Sudden heavy rainfall, inadequate drainage, and climate-induced increases in storm frequency can combine to produce severe flooding that affects mobility networks, housing areas, and critical infrastructures. This scenario is further justified by the availability of real-time hydrological and meteorological data that can be captured by IoT sensors and integrated into a Digital Twin environment. Although flood risk is the core focus, the conceptual logic of this scenario is equally applicable to heatwaves, traffic congestion, or sudden energy shortages. The scenario thus illustrates

how Digital Twins and MIS can coordinate predictive modeling, early warning systems, and administrative decision-making to strengthen urban resilience.

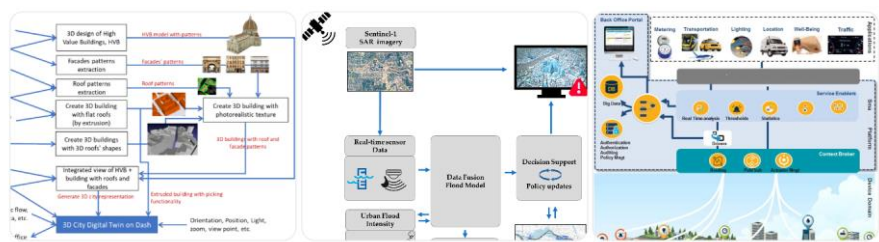


Fig. 2. Data Flow in a MIS–Digital Twin Urban Resilience Scenario

Figure 2 illustrates how sensor-generated data transition through the Digital Twin simulation engine before reaching MIS dashboards and decision intelligence modules during a resilience event such as urban flooding.

5.2. Application Process

In this scenario, the application process begins with real-time hydrological, meteorological, and infrastructural data captured by IoT sensors distributed across vulnerable zones of the city. These devices record water-level fluctuations, rainfall intensity, drainage capacity, and soil moisture, while complementary environmental sensors track weather patterns and temperature conditions. The data flow proceeds into the integrated data layer, where ingestion pipelines clean, validate, and standardize the incoming streams. From here, the information automatically feeds into the Digital Twin computational layer, which activates simulation engines calibrated for flood modeling. The Digital Twin generates spatially explicit predictions indicating where water accumulation will occur, how fast it will progress, and which infrastructures or communities are likely to be affected.

The simulation results are then transmitted directly to the MIS governance layer, where administrative dashboards present the information in formats optimized for decision-making. Municipal staff can observe emerging hotspots, projected timelines, and levels of risk. These dashboards also enable simulation-driven policy testing; for example, they allow decision-makers to evaluate the effects of redirecting traffic flows, deploying emergency pumps, or closing affected streets. The decision intelligence layer enhances this analytical process by issuing predictive alerts that warn of impending system failures, estimating the severity of impact, and providing data-driven recommendations on resource allocation. As a result, emergency services can be dispatched preemptively, drainage crews can be mobilized to critical areas, and public communications can be scheduled to warn residents of impending hazards. Throughout the event, real-time monitoring continues to synchronize the physical environment with the Digital Twin, allowing MIS to continuously update resilience assessments and support adaptive interventions.

Table 2. Key MIS–Digital Twin Functions in the Flood Scenario

Function Category	Example Outputs and Actions
Real-Time Data Integration	Water-level readings, rainfall intensity, drainage capacity, environmental forecasts
Simulation-Based Forecasting	Flood spread models, infrastructure vulnerability mapping, risk indexing
MIS Decision Support	Street closure plans, emergency deployment timelines, drainage maintenance prioritization
Predictive Intelligence	Automated alerts, severity scoring, recommended allocation of emergency resources
Adaptive Monitoring	Dynamic updating of flood simulations and revised MIS dashboards during evolving conditions

This table highlights how each component of the framework contributes to coordinated resilience management in real operational conditions.

5.3. Expected Outcomes

The application of the MIS–Digital Twin framework to this urban flood scenario produces several key governance outcomes. First, the city is able to implement proactive policy measures based on predictive insights rather than waiting for physical impacts to occur. This shift significantly reduces damages, response times, and resource waste. Second, the integration facilitates coordinated responses across multiple municipal departments, including emergency services, transportation authorities, and public works teams, all of which access synchronized information through MIS dashboards. This coordination reduces operational fragmentation, which is often a major obstacle in emergency scenarios. Finally, the framework enhances overall urban preparedness and strengthens adaptive governance by enabling continuous learning. As the Digital Twin records system behaviors and compares predicted outcomes with actual events, municipal authorities gain valuable feedback that improves future planning, infrastructure investment decisions, and disaster mitigation strategies. The result is a smarter, more resilient city capable of anticipating risks and responding effectively to complex urban challenges.

6. Findings

The findings of this study demonstrate that integrating Digital Twin capabilities within a Management Information System fundamentally enhances the intelligence, coordination, and responsiveness of urban governance mechanisms. The analysis of the proposed scenario indicates that combining real-time sensor data with simulation-driven forecasting allows city administrators to detect emerging disruptions significantly earlier than in traditional monitoring systems. As the Digital Twin continuously updates its internal models based on incoming environmental signals, MIS dashboards reflect these changes almost instantaneously, enabling municipal agencies to visualize dynamic risk developments in a unified decision environment. This creates a major shift in operational practice: whereas typical city management relies on static reports and delayed incident notifications, the MIS–DT ecosystem provides continuous situational awareness that supports preemptive interventions and refined crisis management strategies.

Furthermore, the findings confirm that the integration framework reduces governance fragmentation, a longstanding challenge in complex urban systems. When Digital Twin analytics are embedded into MIS workflows, different municipal departments—such as emergency services, transportation authorities, and public utilities—can access synchronized, cross-validated information through a single interface. This eliminates the information silos that often limit collaborative action during emergencies and allows for more coordinated and efficient deployment of resources. The scenario application highlights that decisions made in one department, such as road closures or pump scheduling, are immediately visible to other departments, reducing redundancy and conflicting interventions.

The study also reveals that predictive governance significantly improves preparedness and adaptive capacity. As the MIS aggregates both real-time observations and simulated future conditions, city officials gain the ability to compare planned interventions with projected outcomes. This transforms Digital Twins from purely technical representations into strategic tools that guide policy decisions and long-term resilience planning. The predictive alerts generated within the decision intelligence layer provide an early-warning mechanism that strengthens readiness, while the continuous feedback loop between physical conditions and virtual simulations refines model accuracy over time. The resulting governance environment is more adaptive, data-informed, and capable of learning from past events.

Taken together, these findings support the argument that integrating Digital Twins into MIS platforms elevates urban management from reactive response systems to anticipatory governance ecosystems. This transformation is essential for modern cities facing increasing climate risks, infrastructural vulnerabilities, and population pressures. The evidence from the scenario application demonstrates that the proposed architecture not only enhances operational efficiency but also contributes to more transparent, accountable, and strategic decision-making across municipal structures.

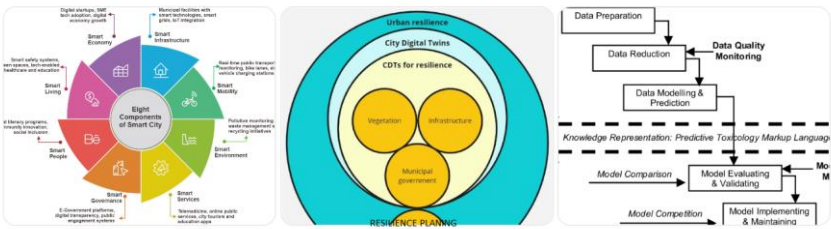


Fig. 3. Summary of Key Findings in MIS–Digital Twin Integrated Governance

Figure 3 provides a visual summary of the major findings, illustrating the transition from reactive operations toward predictive and coordinated governance enabled by the integration of Digital Twin simulation outputs with MIS decision-support structures.

7. Discussion

The integration of Digital Twin technologies within Management Information Systems represents a substantial conceptual and operational advancement in smart city governance.

The findings of this study demonstrate that such integration does more than enhance technical efficiency; it establishes a new governance paradigm in which real-time sensing, urban simulation, and policy decision-making become interlinked components of a single intelligence ecosystem. This interconnectedness addresses one of the most persistent challenges in urban management: the fragmentation of information across departments and digital platforms. By channeling all computational outputs through MIS dashboards, municipalities gain a centralized governance interface that supports coherent, evidence-based decisions across diverse administrative units.

The discussion reveals that the transition from reactive to predictive governance is one of the most significant implications of the proposed framework. Traditional municipal operations often depend on historical data and delayed incident reports, which limit the ability of public authorities to anticipate cascading failures or plan interventions with precision. Digital Twins offer a powerful means of overcoming this limitation because they simulate multiple possible futures under varying environmental or infrastructural conditions. When these simulations are integrated into MIS environments, predictive insights become embedded within the everyday workflows of decision-makers. This shift is not merely technological but institutional, requiring municipalities to adopt new governance cultures that value scenario-based planning, foresight methodologies, and anticipatory policy design.

Another important insight emerging from the study is the role of interoperability in fostering resilient city ecosystems. Without harmonized data flows, shared standards, and unified digital architectures, neither MIS nor Digital Twins can operate at their full potential. The proposed framework demonstrates that interoperability is not solely a technical concern but a governance prerequisite. Effective integration requires the establishment of cross-departmental agreements, revised administrative protocols, and multi-level governance coordination. This aligns with emerging smart city standards emphasizing transparency, accountability, and inclusiveness in digital governance. Accordingly, the proposed model contributes to bridging the existing gap between engineering-driven digital systems and socially oriented governance frameworks.

A further dimension of the discussion concerns ethical, privacy, and security implications. As cities become increasingly reliant on real-time data and predictive analytics, concerns about data protection, algorithmic fairness, and cybersecurity become central to legitimate governance. The MIS–Digital Twin integration framework highlights the need for robust ethical guidelines, compliance structures, and explainability mechanisms to ensure that predictive decision intelligence does not unintentionally reinforce bias or reduce public trust. By embedding these considerations within the model, the framework supports responsible urban innovation.

Overall, the discussion underscores that integrating Digital Twins into MIS structures expands the horizons of what constitutes smart governance—from isolated digital applications to fully interconnected, learning-based systems. This integration equips cities to manage uncertainty more effectively, coordinate complex interventions, and enhance

their adaptive capacities in the face of rising environmental and infrastructural challenges. As a result, the proposed approach not only contributes to academic debates on smart city evolution but also offers a viable strategic pathway for municipal authorities seeking to operationalize resilience in practical terms.

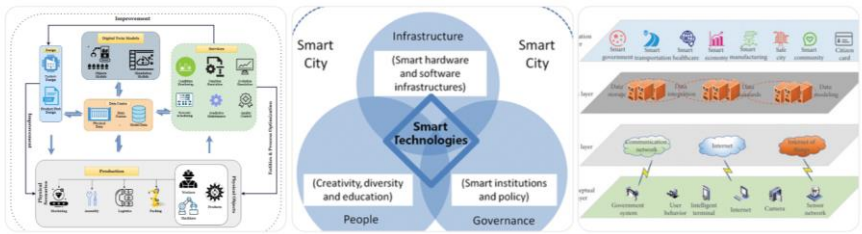


Fig. 4. Conceptual Positioning of MIS–Digital Twin Integration in Urban Governance

Figure 4 illustrates how MIS–Digital Twin integration occupies a central role within modern governance ecosystems by linking sensing infrastructures, predictive simulations, administrative workflows, and decision intelligence into a unified urban management structure.

8. Conclusion

The integration of Digital Twin technologies with Management Information Systems represents a transformative advancement in the evolution of smart and resilient cities. This study has demonstrated that the fusion of real-time sensing, simulation-based forecasting, and governance-oriented information systems creates a unified digital environment capable of supporting anticipatory and strategically informed urban management. The proposed MIS–Digital Twin Integration Framework offers a structured approach for aligning engineering-driven simulation outputs with administrative decision processes, thereby overcoming long-standing issues of fragmentation, delayed responsiveness, and limited cross-departmental coordination in municipal governance.

Through the scenario application focused on urban flood risk, the framework has shown its potential to enhance both operational efficiency and strategic foresight. By embedding Digital Twin outputs directly into MIS dashboards, policymakers gain continuous situational awareness, predictive alerts, and the ability to evaluate the effectiveness of interventions before they are deployed. This redefines how cities prepare for, mitigate, and respond to environmental challenges, shifting governance paradigms from reactive crisis management toward predictive, data-informed resilience planning. Moreover, the framework ensures institutional continuity by integrating ethical safeguards, data governance principles, and transparency mechanisms essential for responsible and trustworthy smart city development.

In addition to operational improvements, the integration model contributes theoretically by positioning MIS as a central orchestrator within digital urban ecosystems. It bridges the gap between socio-technical theory and practical urban management, demonstrating that resilient governance requires the convergence of technological infrastructures,

organizational structures, and decision intelligence. The modular nature of the framework also allows for adaptability, enabling cities to expand their capabilities as technologies evolve or new challenges arise. Ultimately, the conclusions drawn from this research highlight a scalable and future-oriented blueprint capable of guiding municipalities toward more intelligent, coordinated, and sustainable urban governance systems.

References

- [1] R. Kitchin, "The real-time city? Big data and smart urbanism," *GeoJournal*, vol. 79, no. 1, pp. 1–14, 2014.
- [2] M. Chen, S. Mao, and Y. Liu, "Big data: A survey," *Mobile Networks and Applications*, vol. 19, no. 2, pp. 171–209, 2014.
- [3] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications, and challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.
- [4] Z. Allam and Z. A. Dhunny, "On big data, artificial intelligence and smart cities," *Cities*, vol. 89, pp. 80–91, 2019.
- [5] Y. Cai, X. Zheng, and Z. Chen, "Urban digital twins: Research progress and future directions," *ISPRS International Journal of Geo-Information*, vol. 12, no. 5, Art. no. 154, 2023.
- [6] P. Datta, "Digital twins for predictive analytics," *Journal of Industrial Information Integration*, vol. 11, pp. 20–25, 2018.
- [7] A. El Saddik, "Digital twins: The convergence of multimedia technologies," *IEEE MultiMedia*, vol. 25, no. 2, pp. 87–92, 2018.
- [8] T. Bossomaier, B. Dezfouli, and K. Kang, "Digital twins and the future of smart urban management," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9645–9657, 2021.
- [9] D. Zela, "VPN virtual private network applications in data prediction," *Smart Cities and Regional Development (SCRD) Preprints*, vol. 1, no. 1, 2024.
- [10] D. Perez-Gonzalez and R. Díaz-Díaz, "Digital transformation and public governance," *Government Information Quarterly*, vol. 37, no. 4, Art. no. 101500, 2020.
- [11] P. Brous, M. Janssen, and P. Herder, "The dual effects of the Internet of Things (IoT)," *Government Information Quarterly*, vol. 35, no. 4, pp. 637–647, 2018.
- [12] S. Meerow, J. P. Newell, and M. Stults, "Defining urban resilience: A review," *Landscape and Urban Planning*, vol. 147, pp. 38–49, 2016, doi: 10.1016/j.landurbplan.2015.11.011.
- [13] R. Panchal, N. Patel, and A. Chatterjee, "Digital twin-driven decision intelligence for sustainable cities," *Sustainable Cities and Society*, vol. 74, 2021.
- [14] J. Wang, F. Ye, and L. Ma, "Digital twin-supported disaster risk management for smart cities," *Natural Hazards*, vol. 114, pp. 2301–2323, 2022.
- [15] S. Bødker and C. N. Klokmoose, "The human–computer interaction field," *Foundations and Trends in Human–Computer Interaction*, vol. 9, no. 2, pp. 73–149, 2015.
- [16] A. Cocchia, "Smart and digital city: A systematic literature review," in *Smart City*, 2014, pp. 13–43.
- [17] S. K. Haider and S. H. Mahmud, "Urban resilience in the era of digital governance," *International Journal of Disaster Risk Reduction*, vol. 60, Art. no. 102295, 2021.
- [18] S. Hosseini, A. Al Khaled, and R. T. Watson, "Decision support systems in urban planning," *Decision Support Systems*, vol. 127, pp. 113–118, 2019.
- [19] E. Glaeser and G. Ponzetto, "The political economy of urban innovation," *Journal of Urban Economics*, vol. 108, pp. 103–115, 2018.
- [20] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for Industry 4.0-based manufacturing systems," *Manufacturing Letters*, vol. 3, pp. 18–23, 2015.
- [21] Y. Zhou, X. Yao, and D. Wang, "Data governance in digital twin cities," *Information Systems Frontiers*, 2023.
- [22] V. Albino, U. Berardi, and R. M. Dangelico, "Smart cities: Definitions, dimensions, and performance," *Cities*, vol. 38, pp. 20–32, 2015.
- [23] T. V. Kumar and B. Dahiya, *Smart Economy in Smart Cities*. Singapore: Springer, 2017, pp. 73–98.
- [24] R. Akhavan and A. H. Behzadan, "Smartphone-based construction workers' activity recognition and classification," *Automation in Construction*, vol. 93, pp. 289–296, 2018.
- [25] H. Zhang, J. Zhou, and X. Li, "Integration of BIM, GIS, and IoT for smart infrastructure monitoring," *Automation in Construction*, vol. 125, Art. no. 103628, 2021.

- [26] S. E. Bibri, "Data-driven smart sustainable cities of the future: An evidence-based approach," *Sustainable Cities and Society*, vol. 72, Art. no. 103013, 2021.
- [27] S. E. Bibri and J. Krogstie, "Smart sustainable cities of the future," *Urban Technology & Informatics*, vol. 27, no. 1, pp. 1–18, 2020.
- [28] A. Sharifi and Y. Yamagata, "Urban resilience assessment," *Sustainable Cities and Society*, vol. 29, pp. 1–11, 2016.

Smart Technologies and Rural Cultural Heritage – Perspectives for Sustainable Development

Anatoly BABIN

Academy of Economic Studies of Moldova
anatolii.babin@ase.md

Rafael CILOCI

Technical University of Moldova
rafael.ciloci@fieb.utm.md

Andrei MIRZA

Public Association “Sorintex”, Moldova
sorintex.soroca@gmail.com

Abstract

Objectives: This paper examines the potential for integrating smart technologies into the sustainable preservation and promotion of rural cultural heritage, with a focus on the Precucuteni–Cucuteni–Tripolye cultural complex. The aim is to explore how digital tools and cross-border cooperation between Moldova, Ukraine, and Romania can contribute to regional revitalization and foster integration into cross-border value chains, supporting sustainable economic and social development. **Prior work:** The study builds on existing research in regional benchmarking, asset and competence mapping, as well as frameworks provided by European Smart Specialisation Strategies (S3) and Thematic Smart Specialisation Partnerships (TSSP). It aligns with recent research on sustainable regional innovation ecosystems, particularly studies addressing heritage-based innovation and cross-border cooperation within Eastern Europe. **Approach:** A mixed-methods approach was employed, combining qualitative stakeholder interviews, focus groups, regional asset mapping, and policy analysis. The methodology emphasized inclusivity of regional resources, technological capacities, and infrastructure. Pilot projects were co-designed with regional actors, supported by iterative validation through international workshops. **Results:** The findings reveal that rural heritage sites can function as cultural anchors and serve as experimental platforms for circular economy initiatives, green transition, and digital inclusion. The research identifies key thematic directions with market potential, including smart energy, digital heritage, 3D fabrication, and bioeconomy sectors. Active involvement of municipalities, NGOs, and academic institutions emerged as crucial for project implementation and cross-border collaboration. **Implications:** The study offers valuable insights for academics, regional policymakers, and practitioners seeking to leverage cultural heritage in innovation-driven regional development. It highlights the importance of integrated cross-sectoral strategies supported by EU and cross-border funding. **Value:** This research proposes a scalable, cross-sectoral framework connecting cultural heritage preservation with smart technologies and international cooperation. It uniquely positions the Precucuteni–Cucuteni–Tripolye complex as a test-bed for innovation-based territorial development across the Eastern Partnership region.

Keywords: rural innovation; cross-border cooperation; digital archaeology; circular bioeconomy; smart villages

1. Introduction

In the context of global transformations caused by climate change, the digital revolution, and growing social inequality, rural areas in Eastern European countries face acute challenges. The Republic of Moldova, where a significant portion of the population lives in rural areas, demonstrates a pressing need for sustainable solutions aimed at modernizing infrastructure, overcoming demographic decline, and reviving local economies. However, these challenges also present unique opportunities - particularly through the integration of

smart technologies and sustainable development strategies rooted in the region's cultural and natural environment.

One of Moldova's unique assets is the cultural heritage of the Precucuteni-Cucuteni-Trypillia civilization (6th–3rd millennia BC), whose archaeological artifacts attest to a high level of spatial organization, sustainable agriculture, and construction and ceramic technologies. The complex spans three countries - Moldova, Romania, and Ukraine - and is not only an object of historical study but also a potential basis for the creation of innovative models of sustainable rural development. Of particular interest is the idea of using the principles embodied in ancient settlements in the design of modern "smart villages"—autonomous, digital, energy-efficient, and socially sustainable communities. The modern concept of Smart Villages is emerging at the intersection of digitalization, renewable energy, spatial planning, and local engagement. However, its successful implementation requires consideration of the territorial specifics and cultural context. In this sense, the Precucuteni-Cucuteni-Trypillia heritage can serve not only as an archaeological resource but as an innovative benchmark for construction practices, everyday life, and closed resource cycles - the prototypes of a modern circular economy.

This study aims to identify the potential for integrating cultural and natural heritage into sustainable rural development strategies using smart technologies. Specifically, the objective is to assess the potential for transforming the archaeological and agricultural territories of the Precucuteni-Cucuteni-Trypillia complex into a cluster of smart villages, implemented through digital platforms, bio-inspired construction solutions, autonomous energy and water technologies, and innovative approaches to agricultural production and tourism. The work draws on strategic and institutional frameworks: the Smart Specialization Policy (RIS3), the EU Strategy for the Danube Region (EUSDR), in particular the activities of the WG RIS3/Danube Funding Coordination Network, as well as the Smart Villages and S3-4AlpClusters projects and initiatives of the Norwegian Institute of Cultural Heritage (NIKU). A mixed methodology is used, including political-strategic analysis, spatial modeling, and archaeological data interpretation.

Thus, the study opens the way to the development of a new model of sustainable rural development based on the synthesis of traditional knowledge and modern technologies, with a focus on local resources, cultural identity, and digital transformation.

2. Cultural and industrial heritage of Precucuteni–Cucuteni–Trypillia

The Precucuteni–Cucuteni–Trypillia complex represents one of the most significant archaeological cultures in Eastern Europe, developing at the intersection of the modern-day Republic of Moldova, Ukraine, and Romania between the 6th and 3rd millennia BC. This culture is distinguished by its level of technological mastery, social organization, and environmental sustainability, making it a unique source of knowledge about innovative and resource-saving solutions that can be applied to modern rural development.

Precucuteni–Cucuteni–Trypillia ceramics play a central role in understanding the economic and aesthetic life of ancient communities. Research shows that objects made from local

clay were often decorated with complex geometric patterns- meanders, spirals, and numeral motifs—used not only on utilitarian objects but also in ritual contexts. The study, “A complex subsistence regime revealed for Cucuteni–Trypillia sites...,” emphasizes that ceramic production was accompanied by a sustainable agricultural and livestock economy, including the use of manure for fertilizer and a balance between agricultural and livestock products, indicating a complex food supply system. [1] The economics of grain crops, tillage technologies, and storage methods in ceramics were adapted to the climatic and environmental conditions of the region. The study *Productivity of pre-modern agriculture in the Cucuteni-Trypillia area* reconstructs agricultural cycles and shows that even in the early phases of the culture, communities could maintain sustainable agriculture, including setting aside surplus produce for storage or exchange. [2]

Settlement architecture offers even more profound evidence of spatial planning and communal living. Settlements often covered large areas; archaeological excavations indicate the presence of structures where houses were built of clay and wood, with layouts including courtyards, platforms, and sometimes two-story structures. An example of a megasite is Talianki, which covers hundreds of hectares, with a building density typical of large settlements where the population could reach several thousand people. [3] Dwellings were often equipped with wooden or clay platforms (above ground or slightly recessed), with the use of straw and plant coverings in tiles and roofs, with brightly decorated surfaces, indicating concern not only for utilitarian properties but also for the visual and ritual significance of the architectural appearance.

The spatial character of each settlement was also reflected in its organizational elements central structures, squares, or cult spaces that could serve as ritual centers or contact points. One such site is Scânteia in Moldova, where the presence of houses, pits, and rooms associated with cult activities has been documented, along with the discovery of a large number of anthropomorphic figurines and ritual objects. [4] The destruction of houses by fire (apparently deliberate or associated with renewal rites) and their rebuilding at the same locations, the preservation of the building's orientation, and the layering of cultural layers testify to a deeply rooted culture of memory and repetition in planning and materials.

Ceramic production not only served utilitarian purposes but was also a crucial component of cultural identity. Studies of decorative styles reveal the dynamics of change, the adaptation of forms and ornamentation depending on contacts with neighboring cultures. The "Cucuteni C pottery" type is considered an indicator of cultural interactions, especially in the Tripolie B1 – Cucuteni A phases, when techniques related to or partially borrowed from the steppe cultures (e.g., Sredny Stog) appeared, but were interpreted and adapted within the framework of the Trypillian ceramic tradition in such a way that they did not dilute the originality. [5] Decorative motifs, firing technologies, and the choice of form (e.g., bowls, vessels, amphorae) reflect not only aesthetic but also technological stability: thin walls, heat capacity, the ability to thermoregulate, and preserve food.

Trypillian agricultural practices ensured sustainability through mixed subsistence and farming strategies: growing cereals, legumes, gathering wild plants, livestock raising with

manure, rotating fields, and likely periodic periods of dormancy or fallow. New macrobotanical data confirm that the culture was not narrowly focused on grains; its agricultural landscape included a diversity of plants, ensuring resilience in variable climatic conditions. [1] Research on ancient agricultural productivity also shows that by using organic fertilizers and changing agricultural practices, such communities could have increased crop yields and reduced the risks associated with drought or adverse weather events.

In addition to manufacturing and agriculture, craft practices indicate a highly sophisticated use of natural resources. Pottery, either hand-made or wheel-fired, fired at controlled temperatures, demonstrates the use of technologies focused on durability and resource efficiency. Traditional techniques included mixing clay with plant material, straw, or wood additives, which helped improve the insulating properties of structures and vessels, reducing heat loss and ensuring resistance to weather conditions. Archaeological layers indicate that pottery and housing structures were subjected to fires, which may have been part of rituals, but the rebuilding of houses over the same foundations speaks to the continuity and ability of society to endure losses and rebuild infrastructure.

Equally important are the aquatic and land landscapes, the relief, soil conditions, and the presence of rivers and water sources, which influenced the placement of settlements, the design of terraces, drainage systems, and canals. Although precise data on Trypillian hydraulic engineering is limited, macrobotanical and paleoclimatic studies indicate that settlement locations correlated with fertile soils and a moderate climate, with rainfall distribution sufficient for field crops, and with the proximity of pastures and forests for additional resources.

Thus, the legacy of the Precucuteni-Cucuteni-Trypillia complex includes not only material artifacts but also examples of sustainable resource management, spatial organization, and bioinspired technologies that can be adapted today as part of sustainable rural development strategies. Research shows that ceramics, architecture, and agricultural practices formed a synergistic system in which construction technologies, planning, agriculture, crafts, and aesthetics were interconnected. In this system, sustainability was not a byproduct, but a fundamental condition of life.

Table 1. Key elements of the cultural and technological heritage of the Precucuteni–Cucuteni–Trypillia complex

Heritage Component	Key Features
Ceramic production	Ornamented tableware with geometric decor; high heat resistance; a variety of forms and functions; stable recipes and firing methods.
Architecture of settlements	Cob houses with timber frames; highly insulated; two-story structures; decorative wall finishes; weather-resistant.
Agricultural practices	Mixed farming (cereals, legumes); use of organic fertilizers; pasture cattle breeding; fertility maintenance; seasonal crop rotation.
Spatial planning	Radial settlement structure; repeating house modules; presence of central squares and cult zones; use of natural relief.

Heritage Component	Key Features
Life support technologies	Production of utilitarian and ritual ceramics; controlled firing temperatures; integration of natural materials into construction; beginnings of energy efficiency.
Environmental sustainability	Use of local resources; closed cycles of production and consumption; adaptation to changing climate conditions; minimization of anthropogenic footprint.

Source: Authors' compilation based on conference participation and organizational contacts.

As the table shows, elements of the Trypillian civilization's cultural heritage not only represent archaeological value but also demonstrate a systems approach to the sustainable management of space, resources, and technology. These principles can form the basis for modern smart village strategies in cross-border rural regions, including the Republic of Moldova.

3. Smart Technologies for Sustainable Villages: Inspired by Heritage

The archaeological heritage of the Precucuteni-Cucuteni-Trypillia complex offers more than just historical evidence, but a dense network of practices and technologies shaped over centuries by a deep knowledge of the landscape, climate conditions, soil resources, and materials. Today, as sustainable development has become a key focus in rural policy, it is both possible and feasible to recreate, adapt, and integrate these ancient solutions in the context of the digital revolution, smart systems, and renewable energy. Smart specialization approaches represent a new opportunity for the regions of the three countries of Romania, Moldova, and Ukraine to explore and expand the macro-regional innovation environment, identifying opportunities for joint sectoral collaboration and applying a value chain orientation [6] to align relevant efforts in any selected area/sector where there is sufficient interest to explore the potential for collaboration. S3 offers a useful “compass” for this type of collaboration, as it encourages regions to identify common strengths and priorities for further investment in innovation. Thus, the analysis of regional S3 priorities represents a useful first step in identifying and linking related innovation interests across regions.

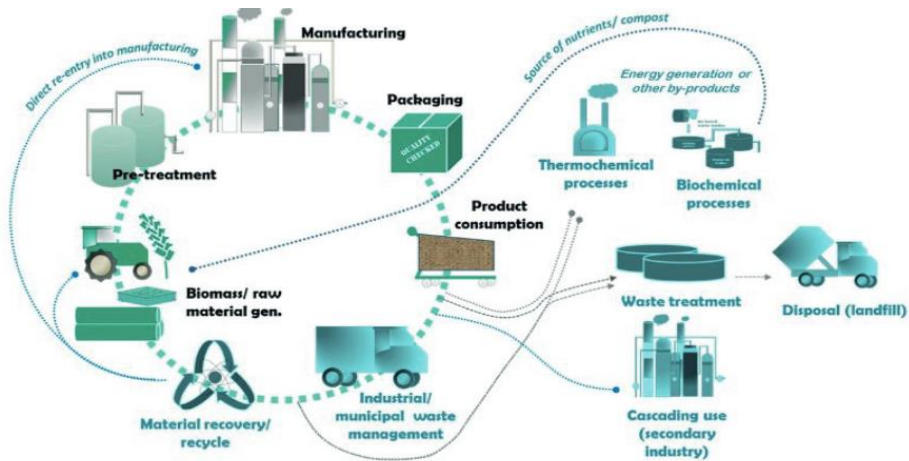


Fig. 1. Visualization of the value chain in a circular bioeconomy

Source: Lokesh et al. [7], reproduced from the Region Västernorrland support manual [8].

Modern smart technologies, inspired by the industrial and cultural heritage of Precucuteni-Cucuteni-Trypillia, represent a multifaceted set of solutions aimed at the sustainable development of rural areas. Bionic construction principles, based on the use of local natural materials and traditional adobe house-building methods, are now being transformed by innovations such as 3D printing and digital design. At the same time, autonomous energy systems based on biomass and renewable sources are being developed, integrated with smart resource management and water supply systems. In agriculture, ancient varieties and traditions are being revived, complemented by modern biotechnologies, promoting sustainable food production and the development of agritourism.

Equally important are digital archaeology and spatial planning, enabling the creation of cultural and technological clusters and smart villages based on historical identity and modern technologies. For a clear comparison and systematization, key areas of these technologies are presented, juxtaposed with specific European cases and their impact on sustainable development (Table 2).

Table 2. Modern smart technologies inspired by Trypillian heritage

Element of the Precucuteni–Cucuteni–Trypillian heritage	Modern technology / solution	Examples of implementation in Europe	Expected impact on sustainable development
Insulated adobe houses using local materials	3D printing of clay and biocomposites, straw panels, Adobe, Earth-based BIM	Project TECLA (Italy), Sieben Linden [9] (Germany)	- up to 90% energy savings on heating - reduction of CO ₂ emissions at ~25 t/house
Spatial radial planning of settlements	Spatial modeling, architecture based on cultural codes	Luče Smart Village (Slovenia) [10], Archéosite Aubechies (Belgium)	- creation of tourist and educational routes - improved planning
Autonomous resource provision, closed cycles	Biomass, solar panels, smart mini-CHPs, reed treatment systems	Losone and Dierikon (Switzerland), Langenegg (Austria)	- reduction of CO ₂ up to 1700 tons/year - complete or partial energy independence

Element of the Precucuteni–Cucuteni–Trypillian heritage	Modern technology / solution	Examples of implementation in Europe	Expected impact on sustainable development
Ancient grain and biocirculation farming system	Agrotechnology, superfoods, fermentation processes, vertical farming	Latgale Bio Cluster (Latvia), Steiermark Food Valley (Austria)	- increase in farmers' incomes - export value of local products
Symbolic ornamented ceramics	Digital design, NFT representations of cultural code, branding	Cultural Creative Clusters (Italy [11], Greece)	- development of the creative economy - growth of cultural tourism
A holistic approach to territory and resource management	Geoinformation platforms, digital twins, AI-based monitoring	SmartLand, UN-GGIM [12] Europe, INSPIRE [13] projects	- increasing the efficiency of spatial planning - risk monitoring

Source: Authors' compilation based on conference participation and organizational contacts.

Thus, the integration of traditional knowledge and innovative technologies creates sustainable clusters capable of improving quality of life, reducing the ecological footprint, and attracting new economic opportunities for rural areas, including regions of the Republic of Moldova with its unique cultural heritage. Further development and adaptation of such models in Moldovan and cross-border contexts requires consideration of the specific characteristics of local ecosystems, cultural traditions, and digital infrastructure, which will be the topic of the next section, dedicated to the concept of smart village clusters. Below, we discuss areas where technological innovation can be inspired by heritage and have already been implemented or demonstrated potential, along with examples from European practice.

Biomaterials and architectural technologies dating back to ancient prototypes. The Trypillians built from clay mixed with plant fillers, creating thick walls, and using straw and wood to ensure thermal stability, regulate humidity, and protect against extreme temperatures. These principles can be adapted to modern conditions by combining traditional recipes and natural additives with modern processing methods such as pressing, molding, and, in some cases, 3D printing. Bio development-Composites based on a mixture of clay, straw, wood chips, and organic resins can produce building blocks and panels that are water-resistant, offer good thermal insulation properties, and have a low carbon footprint. Modern research in sustainable architecture shows that natural materials, if properly processed and protected, can last for decades without significant deterioration and with minimal energy consumption for heating and cooling.

An example of successful adaptation is a German project in Brandenburg, where local clay mixtures with the addition of straw and natural fibers are used to build experimental houses with a zero energy balance (zero-Energy houses). The technologies used there combine passive heating, solar panels, and natural ventilation, while the architectural design is focused on cardinal orientation, roof overhangs, and wall thicknesses reminiscent of ancient insulation techniques. Results show that such houses in temperate climates can reduce heating energy consumption by 60%-80% compared to conventional rural homes. In the autonomous region of Aragon, Spain, a pilot house designed by the Spanish Association for Sustainable Architecture has been built. The house features walls made of

rammed earth and straw bale, and a roof covered with green plants. The interior utilizes a rainwater collection system and natural ventilation. This house not only minimizes external energy consumption but also demonstrates visual and material continuity with ancient building practices. This project serves as an educational platform where local artisans, architecture students, and the public learn traditional recipes and technologies.

Digital archaeology and geospatial technologies as a basis for design. How can the Integrated Geospatial Information Framework (IGIF) [14] and the Interregional Smart Specialization Platform be effectively utilized to develop, integrate, strengthen, and leverage geospatial information management capabilities for sustainable economic development and related resources in the Pre-Cucuteni, Arshid, Cucuteni, and Tripoli regions of Romania, Moldova, and Ukraine? The IGIF framework can help the regions of the three countries bridge the geospatial digital and innovation divide and ensure socio-economic prosperity, leaving no one behind. This unique cultural and historical cluster can serve as a catalyst for sustainable development through the effective use of geographic information systems (GIS), data management, and transnational cooperation. IGIF provides the technical and informational basis for understanding space, resources, and constraints. RIS3 identifies socioeconomic priorities based on regional strengths and the engagement of local actors. Their synergy enables more accurate, sustainable, and coordinated decision-making at the interregional level.

Table 3. Effective use of IGIF and RIS3 in the Cucuteni–Trypillia cross-border regions

Direction	The Role of IGIF (Geospatial Information)	The Role of RIS3 (Smart Specialization)	Expected effect
1. Cultural heritage and tourism	Mapping and monitoring of archaeological sites, routes, and landscapes	Development of creative industries, cultural and archaeological tourism	Growth of tourism, investment in the local economy, preservation of heritage
2. Spatial planning and sustainable land use	Land use analysis, risk assessment (erosion, flooding), zoning	Priority development of environmentally friendly agriculture and a green economy	Reducing land degradation, sustainable rural development
3. Digital transformation and bridging the digital divide	Creation of a unified GPI platform accessible to all participants	Digitalization of the economy, development of IT clusters based on local specifics	Improving digital literacy, creating jobs
4. Education and research cooperation	Geoportals with open access to data for students and scientists	Support for transnational educational and scientific programs	Skills development, knowledge creation, youth engagement
5. Transboundary management of natural resources	Monitoring the state of water, forest, and land resources	Collaborative resource management based on specialization (e.g. agroecology)	Sustainable use of resources, conflict prevention
6. Infrastructure and transport	Mapping and analysis of transport accessibility and logistics	Development of logistics hubs based on specialization priorities	Improving transport connectivity and influx of investment
7. Civic participation and governance	Platforms with public access to GPI and participation tools	Involving citizens and businesses in the formation of specialization priorities	Increasing transparency, supporting bottom-up initiatives

Direction	The Role of IGIF (Geospatial Information)	The Role of RIS3 (Smart Specialization)	Expected effect
8. Financing and investments	Visualization of priority areas for investment, availability of resources	RIS3 focus on sectors with the greatest growth potential	Attracting external financing, economic growth

Source: Authors' compilation based on conference participation and organizational contacts.

Accurate knowledge of the ancient spatial structure of Precucuteni-Cucuteni-Trypillia settlements, including the orientation of dwellings, their relationship to the landscape, the location of social centers, communication routes, and water sources, allows for not only the preservation of archaeological sites but also their use as design templates. The use of LiDAR scanning, photogrammetry and drones - already standard in archaeology - allow us to reconstruct plans, identify lost elements, and map microtopography that influences erosion, drainage, and water runoff. This data can be used in the design of modern rural developments, roads, sewerage, and water systems to minimize erosion, optimize water runoff, and utilize the landscape for natural heating and cooling. In Sweden, the "Digitala Bygder" [15] (Digital Villages) project demonstrates how geospatial data is used for village planning, environmental analysis, sustainable infrastructure connectivity, and optimal placement of new buildings. Villages there, often located near lakes or in mountainous areas, use data on topography, orientation, solar insolation, and wind flow to design developments that maximize the use of natural conditions. This reduces the need for artificial lighting and heating systems, reduces energy loss, and improves comfort. A project in Andalusia, Spain, in the municipality of Granada, used 3D reconstruction. The project involved reconstructing ancient architectural elements and traditional residential forms to incorporate roof and façade designs typical of historical architecture into a new rural residential complex, but with modern windows, thermal insulation, and utility systems. Local authorities supported the project with EU grants, and part of the funds were used to train local artisans. This demonstrates that preserving the visual identity is possible while improving the functional properties of buildings.

Autonomous life support systems: energy, water and waste management. Ancient Trypillian communities were forced to provide their own resources without relying on external grids. Agriculture, crafts, and housebuilding operated within the limits of available resources. Today, a similar approach can combine bioenergy, renewable energy sources, and smart management systems to create autonomous or semi-autonomous villages. Agricultural residues, straw, and plant waste can become feedstock for biogas and biofuel, solar panel power plants and small wind turbines can provide electricity, and geothermal systems can provide heating. In Switzerland, in the canton of Graubünden, the "BioEnergy Dorf" [16] project has been implemented, where a village uses local forest residues and biomass to generate heat and electricity. The infrastructure is designed so that agricultural waste is converted into biogas, which then powers an autonomous mini-heater - heating system, and the heat is also used in greenhouses and for hot water supply. The project demonstrates the sustainability of the model without significant dependence on centralized networks. In Italy, in the Apulia region, the "Smart Water Villages" project (with EU participation), grants supported rainwater collection and filtration systems, combined with

reuse and automated quality control systems. Local residents were trained to operate these systems, increasing efficiency and sustainability. This reduced freshwater consumption and reduced the impact on groundwater.

Agricultural technologies, gastronomy and cultural brands. While Trypillian agricultural practices were viewed as a mixture of cereals, legumes, forest plants, and livestock, contemporary projects in Europe demonstrate that the restoration of traditional plant varieties and traditional soil cultivation or fermentation methods can generate environmental, social, and economic benefits. In Brittany, France, farmers have restored local grain varieties in collaboration with research institutes and developed an agritourism brand associated with the region's culture and history. This has increased tourism, enabled the development of premium-priced products, and stimulated interest in landscape conservation. Locally produced agricultural products have become part of gastronomic routes, according to the heritage master classes and festivals. The Karjalatalo Smart Village project in Finland demonstrates how northern culture can be recreated through technology: the restoration of historic houses, the use of timber structures, the use of bioenergy, collaboration with artists and artisans, and sustainable tourism. Local residents participate in the design and implementation of projects, strengthening a sense of community, identity, and sustainability.

Information technology, digital governance and public participation. Communications, internet, sensor, and digital platform technologies are critical components of smart villages. Heritage can be preserved not only in tangible objects, but also in archives, digital reconstructions, visual representations, oral history, and crafts. Technologies enable the collection of data on temperature, humidity, building conditions, and soil, water resource management, the prediction of climate anomalies, and the optimization of resource use. In Estonia, the "Village Connect" project demonstrated how to digitize administrative and educational services using broadband internet even in remote villages, enabling young people to work remotely, study, and participate in community governance without having to migrate to cities. This reduces population loss and provides incentives for the preservation of cultural environments. In Austria, in the Salzburg region, the "HeritageBytes" project uses AR applications were created to allow residents and tourists to view ancient architectural forms, models of houses, and settlements in augmented reality, superimposing digital reconstructions onto modern buildings. This enhanced awareness of cultural context and motivated participation in restoration and sustainable construction projects.

Synergy, barriers and conditions for success. The integration of heritage and technology creates the potential for a new type of rural environment, in which traditional knowledge is not a museum piece but a source of practical solutions. When building methods are based on the materials used by ancestors, when settlement planning incorporates principles of orientation, connection to water, and sustainability, when digital tools support design, modeling, and management, an ecosystem emerges whose resilience exceeds the sum of its individual parts. However, obstacles arise. Funding is often limited, grants require strict criteria, and regulations may not recognize the use of traditional materials or certify earth

and straw structures. Competencies: Craftsmen, architects, and engineers must be trained to understand and utilize mixed methods. Infrastructure: internet, transportation, electricity—resilient connections are essential. Social factors: Residents may perceive innovations as alien to tradition; it is important that new buildings, renovations, and technologies respect cultural identity and aesthetic norms.

Cases from Europe demonstrate that success is achieved through a combination of technical innovation, public engagement, educational programs, and political/institutional support. Table 4, which compares cases of sustainable villages across Europe, demonstrates the effectiveness of architectural, energy, and digital solutions. These examples highlight that adapting local resources and cultural codes can not only reduce carbon footprints but also drive regional growth. Projects like those in Brandenburg, Andalusia, Brittany, and Finland demonstrate that sustainability is possible not through technological dominance, but through integration, adaptation, respect for heritage, and attention to the human factor.

Table 4. Comparison of cases of sustainable and smart villages in Europe

Case / Country	Integration type	Energy Savings / CO ₂	Income/impact on the local economy	Features of heritage or local resource
Sieben Linden, Germany	Eco-architecture, straw houses, 3D clay	-90% heat loss, ~25 tons of CO ₂ per house	Increasing self-sufficiency, eco-tourism	The archetype of traditional construction + digital planning
Losone, Switzerland	Biomass (wood chips), heating	-1700 tons of CO ₂ /year	Reducing costs on imported fuel	Local wood as energy carrier
Dierikon, Switzerland	Biomass CHP	-532 tons of CO ₂ /year	Affordable heat and electricity for rural areas	Agro-industrial waste
Pohjois-Satakunta, Finland	Digitalization of villages (Smart Villages)	No data on CO ₂	Budget: €54,460, ICT development in villages	Social and digital inclusion as an element of sustainability
South Karelia (Imatra), Finland	Heritage, tourism, culture	N/A	~€81 million in tourism revenue (2023)	Cultural routes, museums, digital interpretation of heritage

Source: Authors' compilation based on conference participation and organizational contacts.

The European cases suggest the following outcomes for further evaluation:

- Reduction of CO₂ emissions as a result of the transition to biomass and environmentally friendly construction—from 500 to 1,700 t per year (for settlements from 1,000 to 5,000 residents).
- Energy savings of up to 90% compared to traditional buildings (example: straw and clay houses with thermal layer construction).
- Digitalization and heritage tourism, on average, increase employment, stimulate small business development, and preserve a region's cultural identity.
- Income from cultural tourism can amount to tens of millions of euros per year in regions with a well-integrated system of cultural and natural assets (South Karelia).

4. Smart Village Cluster Concept: Integrating Heritage, Innovation, and Sustainability

Modern approaches to sustainable rural development within the European Union are increasingly focused not on mass urbanization or industrialization, but on the creation of smart, flexible, and resource-autonomous rural ecosystems. This context calls for a conceptual reassessment of the role of cultural heritage as an incentive not only for protection but also for the transformation of local spaces into innovative, socially active, and environmentally sustainable communities. Within the framework of European smart specialization policies, particularly in the context of the EU Macro-Regional Strategies and RIS3 initiatives, there is increasing attention to rural areas as laboratories for a sustainable future, where digital, energy, social, and cultural innovations can be closely integrated.

In this context, the concept of a smart village shifts from a technologically equipped settlement to an ecosystem in which sustainability is achieved through synergies between local knowledge, digital technologies, the bioeconomy, and innovative forms of governance. In the context of the Republic of Moldova, with its high cultural and historical potential and the structural vulnerability of rural areas, adapting this approach through a cluster development model is particularly relevant. The concept of smart village clusters proposed in this study aims to integrate prehistoric heritage, in particular the Precucuteni-Cucuteni-Trypillia cultural complex, into a sustainable rural development model with an emphasis on digitalization, energy efficiency, and the local economy.

One of the features of the proposed model is the synthesis of archaeological heritage with modern technologies: the reconstruction of adobe houses based on digital archaeology can serve not only as a means of preserving historical knowledge but also as a starting point for the creation of energy-efficient dwellings built using bioinspired building materials. Similarly, the restoration of Trypillian agricultural practices, including the cultivation of ancient grains and the use of organic fertilizers, finds a contemporary interpretation in sustainable agriculture, agroforestry, and food innovations based on fermentation technologies. Archaeologically accurate reconstruction of settlements, coupled with digital resource management platforms and cultural tourism, can contribute to the creation of economically viable villages integrated into regional and transboundary value chains.

In this context, the cluster approach ensures the institutional sustainability of such models. It involves the creation of territorially organized networks uniting small businesses, educational and scientific institutions, municipal authorities, and cultural and tourism operators. In Europe, similar approaches have demonstrated their effectiveness in a number of cases. For example, in the village of Langenegg (Austria), a cooperative energy production model enabled the village to achieve complete energy independence while maintaining a small and socially sustainable population. In Luče, Slovenia, a project was implemented for the digital management of village infrastructure and ecotourism development, focusing on local cultural landscapes. In Germany, the ecovillage Sieben Linden has become a platform for bio-building, artisan education, and social integration. These examples demonstrate the potential for translating local resources—material,

intangible, and institutional—into sustainable models of economic activity and social cooperation.

For Moldova, the potential for deploying such models in archaeologically significant regions, where cultural heritage can act as an anchor for innovative transformations, is particularly important. Digital technologies are key elements here, both in mapping and in village life management. The use of spatial data, sensor systems, and digital twins enables the creation of smart platforms that optimize resource allocation, environmental monitoring, and interactions between residents and management structures. In this context, the role of international frameworks such as UN-GGIM, INSPIRE, and Copernicus, which provide access to geospatial information and digital planning standards, is also relevant.

The cultural component remains an integral core of the concept. Archaeological heritage is viewed not only as an object of conservation but also as a strategic development resource capable of generating both economic and symbolic forms of capital. In the context of de-urbanization and increasing attention to biodiversity and climate neutrality, cultural identity is capable of ensuring the long-term connection of the population to the territory, thereby serving as an anthropological framework for sustainability. This necessitates the integration of heritage into education, production, and tourism systems, creating a transformable yet identity-preserving platform for sustainable development.

The functional structure of such a village-cluster involves the integration of several interconnected zones: an energy and agricultural module based on closed-loop and bioenergy principles; a production zone producing construction and handicrafts using local materials and technologies; an educational and cultural space integrated with an open-air museum and creative workshops; and a digital platform enabling monitoring, management, and participation. The spatial and architectural planning of these zones could be based on the radial and concentric patterns of ancient settlements, ensuring both symbolic continuity and functional logistics.

The smart village cluster's economic model is based on diversified revenue streams, including bioenergy, sustainable agriculture, eco-tourism, cultural tourism, sustainable building materials production, handicrafts and design, and educational services. Funding can be secured through a combination of European funds (including Interreg, Horizon Europe, LIFE, and the Danube Transnational Programme), national programs, private investment, and local cooperative structures. A key element of sustainability is local community participation in management and production, which requires preliminary training, youth engagement, and the creation of incubators and educational platforms.

Thus, the proposed concept of a smart village cluster in Moldova draws on the potential of cultural heritage as a foundation for technological and social innovation. It aims to develop resilient territories capable not only of adapting to climate and economic challenges but also of fostering new forms of life that combine tradition, digitalization, and local autonomy. Given the transboundary nature of the Precucuteni-Cucuteni-Trypillia cultural complex, this model can be scaled up for interregional cooperation within the Danube

macroregion and the Black Sea region, creating a common cultural and economic space where heritage becomes the foundation of the future.

Project S3-4AlpClusters [17] (Smart Specialisation Strategies to build an Innovation model for Alp Clusters) worked within the framework of the Interreg Alpine Space program during 2016-2019. The goal was to create an innovation model that helps overcome the main barriers in the implementation of smart specialization strategies: from identifying promising areas and priorities, through stimulating cooperation between regions, to supporting a real industrial revolution (smart industrial transition). We chose this practice to consider, using the example of the Alpine Macroregion, how elements of S3-4AlpClusters are applicable to the concept of smart villages-clusters using the example of "Precucuteni"-Cucuteni-"Tripolye." And we found that the project provides several useful conceptual and methodological guidelines that can be adapted:

1. Modeling Transformative Activities (TA): S3-4AlpClusters systematizes the process of identifying which activities (technological, manufacturing, service) can truly transform a region's economic structure. In our case, this could include bio-based construction materials, digital archaeology, sustainable food, or heritage-based tourism. It's important that the selected TAs be sustainable, draw on local resources and culture, and be institutionally supported.
2. Participation of clusters and interregional cooperation. The project demonstrated the importance of regions exchanging experience, knowledge, and technology, especially when it comes to innovation and sustainable development. In "Precucuteni-ArshidCucuteni-Tripolye's" cross-border nature is part of the advantage and the implementation of the smart village concept-clusters could benefit greatly if partners from Romania and Ukraine were included and if a collaboration model similar to that of S3 were applied-4AlpClusters.
3. Circular economy and clusters as drivers of innovation: S3-4AlpClusters incorporates circularity, which is important for rural areas, especially those with a heritage where resources (clay, earthenware, agricultural waste, ceramics) have a history of cyclical use. Implementing circular approaches borrowed from the model can increase sustainability and reduce waste.
4. Practitioner support tools. The project has created training tools and methodologies that help regions and clusters assess their strengths, develop strategies, and set priorities. In our case, before launching smart village clusters, it would be appropriate to develop a similar methodology: a local potential assessment, a SWOT analysis, and a rigorous risk assessment -analysis of cultural heritage, resources and technological capabilities, resource maps, assessment of community interest and infrastructure readiness.

Project S3-4AlpClusters illustrates how smart specialization strategies can be realized through clusters and transformative activities, especially when they draw on a region's resource potential—whether scientific, artisanal, or technological. The innovation model developed by S3-4AlpClusters proposes a systematic approach to setting priorities, fostering interregional cooperation, and developing clusters based on the circular economy. Such elements could form the basis of the smart village cluster concept in the Precucuteni

-Cucuteni-Trypillia area: from the production of biomaterials based on clay and agricultural waste to digital archaeology and cultural tourism, with the active role of municipalities and partnerships between Moldova, Romania, and Ukraine.

Table 5. Smart village cluster model based on archaeological and resource potential

Model component	Description of functionality	Potential in the example of Precucuteni–Cucuteni–Trypillia (PCT)
Cultural core	Open-air museum, settlement reconstruction, Virtual Reality / Augmented Reality (VR/AR) experience	Recreating Trypillian buildings with digital archaeology
Bioenergy and autonomy	Mini – Combined Heat and Power (CHP), solar power plants, biogas, energy efficiency	Use of straw, wood residues, and viticulture waste
Digital Management Platform	Village digital twin, climate and consumption monitoring, citizen participation	Geodata + platform based on UN Global Geospatial Information Management (GGIM)/INSPIRE
Production of biomaterials	Construction using local materials: clay, straw, rammed earth, 3D printers	Connection with traditional PCT houses, replicable low-cost modules for villages
Education and creative industries	Residences, vocational schools, summer universities	Partnership with Norwegian Institute for Cultural Heritage Research (NIKU), universities of Moldova, Ukraine, and Romania
Tourism and the Experience Economy	Ecotourism, gastronomy, archaeological routes, cultural events	Creation of the PCT tourism cluster, new revenues from agro- and cultural tourism
Circular systems	Closed cycles of water, energy, and waste	Combination with local practices: compost, biofermentation, agroforestry

Source: Authors' compilation based on conference participation and organizational contacts.

The launch of pilot village clusters should follow the entrepreneurial discovery process (EDP) logic underlying smart specialization (S3) approaches, with a focus on the subregional level, encompassing the territories of specific settlements. The proposed starting point is the selection of an archaeologically significant area - for example, near the villages of Stauceni or Orhei - where scientific research is already underway, infrastructure is in place, and interest from local communities is evident. The next step should be the formation of an interdisciplinary working group bringing together representatives of local and district authorities, universities, research institutes, NGOs, agricultural and tourism businesses, and digital solution providers. This approach allows for the identification of local competencies, untapped resources, and cultural assets that could become growth areas. In this context, the pilot project acts as an experimental platform, linked to access to EU funding mechanisms – INTERREG, Horizon Europe, EIT, LIFE and the Danube Transnational Programme – and can become the basis for testing solutions in the fields of digital archaeology, sustainable land management, bioenergy and creative industries, with the prospect of scaling up to other territories of the Precucuteni-Cucuteni-Trypillia cultural complex.

The method for assessing resource and cultural potential within the smart village cluster model is built as an integral element of the entrepreneurial discovery process (EDP) at the community and subregional levels. This approach enables the integration of local knowledge with external data and strategic planning in the spirit of smart specialization (S3). The assessment begins with a SWOT analysis covering the socio-economic status, level of digitalization, infrastructure constraints, and human resource potential. This is followed by mapping archaeological, natural, and spatial resources using available platforms and standards - such as INSPIRE, Copernicus, and UN-GGIM - enabling geographic information interoperability and cross-regional comparison. Particular attention is paid to inventorying intangible heritage-including traditional practices, oral knowledge, craft techniques, and forms of cultural identity - that can be integrated into new economic and educational models. The final component of the methodology is the identification of "transformative activities"—those that have the potential to change the structure of the local economy by leveraging a combination of cultural heritage, digital solutions, and sustainable practices. This could include, for example, digital archaeology, biomaterial production, artisanal bio-design modeling, or gastronomic tourism that reflects the historical and cultural characteristics of the region.

This opens up opportunities for integrating clusters based on cultural heritage and the bioeconomy into broader green value chains, particularly in areas such as local sourcing, eco-design, closed-loop production, and capacity development and certification. The stages of cluster formation in such conditions may be as follows:

1. Establish an institutional core, including academic and research institutions, municipalities, museums, and archaeological institutes. This core is responsible for knowledge gathering, strategy development, and initial management.
2. Attracting small and medium-sized businesses connected to local assets: agritourism, sustainable agriculture, bio-based construction materials, and heritage-based crafts and design. These businesses can become participants in regional value chains that complement the critical sectors, including through green solutions.
3. Develop a collaborative governance platform (Governance Model) that includes local governments, business associations, universities, and civil society. This will ensure transparency, inclusiveness, and sustainability of decision-making.
4. Joining transnational and macro-regional networks, including initiatives within the EU Macro-Regional Strategies, the Danube Transnational Programme, and the Ukrainian Cluster Alliance (UCA). The latter is already implementing a project portfolio aimed at enhancing resilience, export potential, and cross-border cooperation. An example is the initiative to create cluster bridges with the EU, which could be used to test the cluster village model within the framework of cooperation between Moldova, Ukraine, and Romania.
5. Launching educational programs and incubators for young people, which is especially important in the context of brain drain and de-urbanization. Young people should be involved in both digital transformation and heritage revitalization processes – through programs in agricultural innovation, digital archaeology, VR/AR development, and sustainable entrepreneurship.

Thus, the Precucuteni-Cucuteni-Trypillia complex can be seen as a potential test-bed for cross-border initiatives combining digitalization, green transition and cultural identity.

The EIT Silicon Valley Hub [18] platform can become a key facilitator in the transfer of technological solutions and the building of partnerships. In particular, the creation of digital twins of archaeological settlements, the development of bioenergy solutions, and export models for sustainable building materials made from clay and agro-waste pave the way for collaboration with transatlantic startups, universities, and investors. For countries within the Precucuteni-Cucuteni-Trypillia cultural complex, such integration can transform cultural heritage into an active component of smart specialization, contributing not only to the preservation of identity but also to inclusive economic development.

The EIT Silicon Valley Hub platform offers unique opportunities for European regions and clusters seeking to establish innovative collaboration with leading US ecosystems, including universities, startups, and venture capital firms in Silicon Valley. For smart village clusters in the PCT zone, the following areas of collaboration are possible.

Table 6. EIT Silicon Valley Hub Activities Relevant to the PCT Cluster

EIT Silicon Valley Hub Program Focus	Potential for a PCT cluster
EIT Global Outreach Programme	Presentation of the smart village cluster model as an example of "heritage-based innovation" on international platforms.
Soft Landing for Startups	Support for startups in the fields of digital archaeology, 3D construction using biomaterials, and sustainable agritourism.
Open Innovation Challenges	Collaborative projects with universities and businesses in the United States to develop solutions in sustainable management, digitalization of tourism, and AI archaeology.
Transatlantic Dialogue on Regulation	Work on a regulatory framework for the export of cultural products and technologies with a focus on TTC and ESG approaches.

Conclusions and Recommendations

Cultural heritage, particularly in archaeologically rich regions of Eastern Europe, is increasingly recognized not only as an object of preservation but as a resource for innovation, local entrepreneurship, social cooperation, and digital transformation. The proposed smart village-cluster model, based on the integration of digital technologies, bioeconomy, and the heritage of the Precucuteni – Cucuteni - Trypillia cultural complex, demonstrates high potential for scaling and adaptation across different countries, depending on their institutional and integration contexts.

For Romania, as an EU member state, the transformation of rural territories aligns with the goals of the European Green Deal, the Digital Decade, and Smart Specialisation strategies. Cultural heritage here can serve as a driver for tourism, education, and eco-construction innovation. Key priorities include the integration of archaeological and spatial data into governance systems (using INSPIRE and Copernicus frameworks), the development of

digital twins of cultural landscapes, and interdisciplinary educational programs that combine digital archaeology with sustainable land use.

For the Republic of Moldova, with limited resources and institutional vulnerabilities, priority should be given to pilot projects that demonstrate the viability of the model. Moldova can act as a testbed for bioeconomic solutions based on local practices, digital transformation of small rural areas, and youth engagement in revitalizing and reinterpreting intangible heritage. Strengthening spatial data governance (in line with UN-GGIM and INSPIRE), enhancing geospatial capacity at the municipal level, and supporting digitalization in rural tourism, bioenergy, and construction are essential steps.

For Ukraine, which is facing the challenge of large-scale territorial reconstruction, integrating sustainable recovery with cultural landscape preservation is critical. The smart village clusters could act as suppliers of innovation and sustainability platforms. Special focus should be placed on harmonizing spatial data standards, restoring archaeological sites using digital tools, and developing regional knowledge-sharing platforms.

Scaling Potential

The smart village-cluster model can be adapted and replicated in other regions of the Danube macro-region, the Eastern Partnership, and the Black Sea area. Shared archaeological heritage and common challenges - such as depopulation, landscape degradation, and job scarcity - create favorable conditions for transnational implementation. Platforms like EIT Silicon Valley Hub, Interreg Danube, or Horizon Europe Missions can serve as foundations for new consortia and funding mechanisms.

Recommendations

- For public authorities: integrate support for smart village-clusters into national and regional strategies, ensure regulatory and financial frameworks, and promote cross-border and interregional cooperation using harmonized spatial planning standards.
- For universities and research institutes: develop interdisciplinary programs combining archaeology, digital technology, and sustainable development; support applied research labs in collaboration with local communities.
- For donors and investors: support pilot initiatives with mixed funding models, develop tools to measure cultural and social impact, and finance the deployment of digital platforms and models in rural regions.

Acknowledgments: The research was carried out in the framework of the research subprogram 020408 "Research on ensuring sustainable development and increasing the competitiveness of the Republic of Moldova in the European context".

References

- [1] W. Kirleis, M. Dal Corso, G. Pashkevych, et al., "A complex subsistence regime revealed for Cucuteni–Trypillia sites in Chalcolithic eastern Europe based on new and old macrobotanical data," *Vegetation History and Archaeobotany*, vol. 33, pp. 75–90, 2024, doi: 10.1007/s00334-023-00936-y.
- [2] A. Shukurov, G. Sarson, M. Videiko, et al., "Productivity of premodern agriculture in the Cucuteni–Trypillia area," *Human Biology*, vol. 87, no. 3, 2015, doi: 10.13110/humanbiology.87.3.0235.

- [3] Y. Rassamakin and F. Menotti, “Chronological development of the Tripolye culture giant-settlement of Talianki (Ukraine): 14C dating vs. pottery typology,” *Radiocarbon*, vol. 53, no. 4, pp. 645–657, 2011, doi: 10.1017/S0033822200039102.
- [4] C.-M. Mantu Lazarovici et al., “Scânteia, Iași, Dealul Bodeștilor (La Nuci),” *Cronica Cercetărilor Arheologice*, report 2347, 2003. [Online]. Available: <https://cronica.cimec.ro/Public/Detalii.php?d=Scanteia-Iasi-Dealul-Bodestilor-La-Nuci-2003&k=2347>
- [5] N. Burdo, “The Cucuteni C pottery in the Cucuteni–Trypillia cultural complex (formulation of the problem and a brief historiography),” *Tyragetia*, new ser., vol. X [XXV], no. 1, 2016. [Online]. Available: https://www.nationalmuseum.md/en/press_releases/journal_tyragetia/the_cucuteni_c_pottery_in_the_cucuteni_trypillia_cultural_complex_formulation_of_the_problem_and_a_brief_historiography/
- [6] J. Woolford, E. Amanatidou, E. Gerussi, and J. M. Boden, *Interregional Cooperation and Smart Specialisation: A Lagging Regions Perspective*, EUR 30691 EN. Luxembourg: Publications Office of the European Union, 2021, doi: 10.2760/25586.
- [7] K. Lokesh, L. Ladu, and L. Summerton, “Bridging the gaps for a ‘circular’ bioeconomy: Selection criteria, bio-based value chain and stakeholder mapping,” *Sustainability*, vol. 10, no. 6, art. 1695, 2018, doi: 10.3390/su10061695.
- [8] Region Västerbotten, *Adopting a Value Chain Approach to Inter-regional S3 Collaboration across the Baltic Sea Region: Support Manual*, 2022. [Online]. Available: <https://regionvasterbotten.se/VLL/Filer/Support%20Manual-%20Adopting%20a%20Value%20Chain%20approach%20to%20inter-regional%20S3%20collaboration%20across%20the%20Baltic%20Sea%20Region.pdf>
- [9] Ecovillage Sieben Linden, “Sieben Linden.” [Online]. Available: <https://siebenlinden.org/en/ecovillage-2/sieben-linden/>
- [10] COMPILE Project, “Pilot site Luče.” [Online]. Available: <https://main.compile-project.eu/sites/pilot-site-luce/>
- [11] Cluster Cultura e Creatività, “About the cluster.” [Online]. Available: <https://www.creativefvg.eu/en/about-the-cluster/>
- [12] UN-GGIM: Europe, “About us.” [Online]. Available: <https://un-ggim-europe.org/about-us/>
- [13] Publications Office of the European Union, “INSPIRE datasets on the European Data Portal,” 2026. [Online]. Available: <https://data.europa.eu/en/news-events/news/inspire-datasets-move-european-data-portal>
- [14] United Nations Committee of Experts on Global Geospatial Information Management, “United Nations Integrated Geospatial Information Framework (UN-IGIF): Overview.” [Online]. Available: <https://ggim.un.org/UN-IGIF/overview/>
- [15] Smart Rural Areas, “Digital village twin: Veberöd, Sweden.” [Online]. Available: <https://www.smartrural21.eu/smart-solution/digital-village-twin/>
- [16] Presence Switzerland, “The Swiss valley on the verge of becoming 100% organic.” [Online]. Available: <https://houseofswitzerland.org/swissstories/history/swiss-valley-verge-becoming-100-organic>
- [17] Interreg Alpine Space, “S3-4AlpClusters.” [Online]. Available: <https://www.alpine-space.eu/project/s3-4alpclusters/>
- [18] EIT Global Outreach, “EIT Hub Silicon Valley.” [Online]. Available: <https://www.go-eit.eu/eit-silicon-valley-hub/>

Designing Climate-Smart Edible Gardens through Geospatial Ecological Profiling: A Case Study of Măgurele, Ilfov

Miruna-Elena Iliescu-Vasile

National University of Political Studies and Public Administration, Bucharest, Romania

Miruna.iliescu@comunicare.ro

Abstract

This research explores the integration of climate-adaptive urban agriculture into peri-urban ecosystems, using the case of Măgurele, Ilfov County, Romania. The main objective is to develop a methodology for planning small-scale, low-input edible gardens that are tailored to local ecological conditions while contributing to food resilience and sustainable urban design. The study addresses the urgent need to enhance biodiversity, soil health, and ecosystem services in underutilized suburban spaces by identifying plant species with high compatibility to site-specific environmental parameters. The paper builds upon recent interdisciplinary work in urban gardening, agroecology, and spatial planning that emphasize localized sustainability and resilient infrastructure. It contributes to this discourse by applying a data-driven ecological profiling method to inform plant selection and garden structuring in urban fringe contexts. To capture site evidence, the research employs a geospatial assessment framework using remote sensing datasets. Environmental indicators such as land surface temperature, normalized vegetation index (NDVI), total precipitation, evapotranspiration, terrain aspect, and topsoil pH are extracted and used to construct a seasonal ecological baseline. A multi-criteria suitability scoring model is then developed to assess the compatibility of more than twenty edible plant species. The results demonstrate that a diverse range of seasonal crops, including common vegetables and lesser-known edible wild plants, can be strategically layered and rotated to fit local microclimatic and soil conditions. The analysis confirms the feasibility of establishing productive, adaptive gardens even in densely built peri-urban contexts. This study offers a replicable methodology for planners, researchers, and community stakeholders seeking to implement resilient urban food systems. Its main contribution lies in bridging ecological data with practical garden design, offering an accessible model for climate-aware green infrastructure development in peri-urban Europe.

Keywords: urban resilience; low-maintenance cultivation; micro-agriculture; geospatial analysis; climate-adaptive design

1. Introduction

Urban and peri-urban agriculture (UPA) has reemerged as a strategy to improve food security, promote sustainable land use, and enhance resilience in the context of climate change. In Romania, peri-urban areas like Măgurele, Ilfov have faced rapid land transformation, often without integrated ecological planning. This study proposes a minimal-input edible garden model, grounded in climate-smart agriculture (CSA) and powered by geospatial analysis, to explore the feasibility of seasonal planting based on environmental parameters extracted remotely.

The research introduces a novel scoring model for edible plant selection adapted to local ecoclimatic constraints. The goal is to offer a scientifically validated framework for designing climate-adapted urban gardens using Earth Observation data and open-access agronomic indicators.

In Romania, current urban-gardening practices rely predominantly on qualitative guidance, community initiatives, and emerging municipal policies, yet lack standardized methods for integrating climatic variables into planting decisions. Existing manuals and local frameworks outline ecological principles and participatory models, but do not employ

geospatial diagnostics or quantitative suitability criteria for crop selection. This methodological gap limits the ability of practitioners and local authorities to design climate-adaptive systems grounded in empirical data. By introducing a reproducible remote-sensing workflow and a species-suitability scoring model, the present study provides a technical contribution that complements existing practice and supports evidence-based planning for edible gardens in urban and peri-urban environments.

2. Literature Review

Urban gardening has emerged as a practical response to food insecurity, environmental degradation, and the increasing need for greener cities. Studies indicate that small-scale food production in urban settings enhances food resilience while improving microclimates, soil quality, and community well-being [1], [2]. These micro-interventions are particularly impactful in peri-urban areas where land availability is limited but ecological potential remains underutilized. As urban and peri-urban agriculture (UPA) evolves from subsistence activity to multifunctional infrastructure, edible landscapes increasingly serve not only as productive spaces but also as micro-systems that support climate regulation, ecological buffering, and social cohesion within climate-smart cities.

A growing body of research highlights the value of integrating geospatial and remote-sensing datasets into urban agriculture planning. Earth Observation technologies have been used to evaluate land surface temperature, NDVI, precipitation, and soil characteristics, thereby supporting data-driven decisions regarding species selection and site suitability [3]. The present study follows this direction by proposing a species-compatibility scoring model grounded in environmental constraints derived from MODIS, CHIRPS, ERA5-Land, and SoilGrids datasets.

Educational and participatory frameworks also contribute to this evolving field. The Urban Soul curriculum emphasizes the integration of digital tools with ecological literacy, advocating for localized data interpretation, participatory design, and long-term environmental education as key components of urban-garden planning. This aligns with the methodological principles applied in our research, particularly in defining seasonally adaptive, climate-sensitive plant selections.

Existing literature further underscores the absence of standardized, data-based models for choosing plant species according to environmental suitability rather than tradition or aesthetics. This gap is especially significant in Central and Eastern Europe, where climate variability and soil heterogeneity remain underaddressed in urban agriculture planning [4], [5]. The methodological framework proposed in this study contributes to filling this gap by combining multi-source environmental data layers with species-specific ecological thresholds into a reproducible scoring process.

In Romania, interest in urban gardening has expanded, supported by practical manuals, ecological design guides, and emerging policy initiatives. The *Permacultură Urbană* manual provides an ecological design foundation, outlining principles such as soil regeneration, mulching, no-dig methods, companion planting, and stratified vegetation structures [6]. Complementing this ecological basis, the *Guide for Setting Up an Urban Garden* offers applied recommendations for micro-interventions, phased planting, adaptive

calendars, and efficient irrigation tailored to compact urban spaces [7]. The Guideline for Community Micro-Green Spaces expands these approaches by promoting modular raised beds, spontaneous vegetation, composting, and biodiversity-focused maintenance, providing accessible and scalable methods for both residents and local authorities [8].

At the infrastructural level, the Local Public Policy Proposal for Community Gardens (Cluj-Napoca) reframes urban gardening as a component of productive green infrastructure aligned with European nature-based solution (NBS) frameworks. It defines four typologies of community gardens: micro-modular, parcel-based, urban orchards, and multifunctional green spaces, each mapped to specific spatial patterns within dense housing areas and underused “green pockets” [9]. The document advocates transitioning from informal gardening practices to regulated, participatory, municipally supported interventions integrated into urban-planning instruments such as PUZ and PUD.

Across these sources, several consistent themes connect national practice to the scientific approach adopted in this study. Romanian guidelines emphasize the need for environmental profiling (sun exposure, soil parameters, drainage, and microclimate) as a prerequisite for species selection, mirroring the remote-sensing-based profiling in our methodology. All reviewed documents support ecological compatibility as the basis for plant choice, aligning with the scoring system developed here. Moreover, the layered-garden logic found in permaculture and community-garden typologies directly corresponds to our stratified garden-planning model. Finally, Romanian resources repeatedly highlight scalability and replicability, from balcony gardens to multifunctional community plots, resonating with smart-city perspectives that embed micro-agricultural systems within broader climate-resilience frameworks.

Collectively, this body of work shows that urban gardening in Romania is shifting from informal, grassroots practice toward integrated, data-informed, policy-supported interventions. This evolution further validates the relevance of our approach, which operationalizes satellite-based environmental profiling and plant compatibility scoring as tools for climate-smart micro-agriculture planning in urban and peri-urban environments.

3. Methodology

The methodology employed in this study integrates geospatial data extraction, environmental profiling, ecological scoring, and spatially optimized garden design to evaluate the suitability of edible plant cultivation within a 250-meter buffer area in Măgurele, Romania. Using Google Earth Engine as the primary analytical platform, the study synthesizes multi-source environmental datasets to construct a detailed micro-climatic and edaphic profile of the site. These environmental parameters are then used to develop a quantitative plant–environment compatibility scoring system, which informs a stratified garden planning model tailored to local conditions. Collectively, the methodological steps provide a replicable framework for assessing urban and peri-urban food-growing potential in smart-city contexts.

3.1. Study area and data collection

The analysis was conducted for a 250-meter buffer zone delineated around a reference point located in Măgurele, Romania (44.3522 N, 26.0228 E). This micro-scale spatial unit was

selected in order to capture fine-grained environmental conditions relevant for urban–peri-urban food-growing systems within a smart-city framework.

Environmental variables were extracted using Google Earth Engine (GEE), which provides standardized and temporally consistent geospatial datasets suitable for environmental profiling at local scales. The study incorporated the following data sources:

- MODIS LST Day 1 km: Land Surface Temperature (daytime)
- MODIS NDVI: Normalized Difference Vegetation Index
- CHIRPS Daily: Precipitation (quasi-global, daily)
- ERA5-Land: Evapotranspiration (hourly reanalysis data)
- SRTM Aspect: Terrain aspect derived from the Shuttle Radar Topography Mission
- OpenLandMap Soil Attributes: Soil pH at 0–5 cm depth

All datasets were clipped to the 250-meter buffer and aggregated using mean or directional statistics, depending on variable characteristics. Data were extracted for the most recent multi-year period available for each dataset to ensure representativeness.

3.2. Environmental profiling

A descriptive environmental profile of the study area was constructed using the extracted variables. Mean daytime land surface temperature was 32.36 °C, indicating pronounced heat accumulation in the warm season. Vegetation greenness, expressed via NDVI, averaged 0.275, characteristic of sparse to moderate vegetation cover in peri-urban environments. Annual precipitation totaled approximately 246 mm, consistent with known dry-season patterns for southern Romania. Evapotranspiration data yielded a value of approximately -327 mm, which was treated as a data-quality artifact but retained for relative-comparison purposes. Topographic orientation (aspect) averaged 112°, corresponding to an east-southeast exposure. Soil pH at 0–5 cm was 6.5, suggesting slightly acidic yet agriculturally favorable conditions.

Table 1 Environmental profile based on extracted variables.

Parameter	Dataset / Source	Value	Interpretation
Land Surface Temperature (daytime, mean)	MODIS LST Day 1 km	32.36 °C	High summer thermal load; heat-tolerant species required
NDVI (mean)	MODIS NDVI	0.275	Sparse-to-moderate vegetation cover; low photosynthetic density
Annual Precipitation	CHIRPS Daily	246 mm/year	Low rainfall; high reliance on drought-resistant crops
Evapotranspiration	ERA5-Land	−327 mm	Data-quality artifact; indicative of evapotranspirative stress regime
Terrain Aspect	SRTM Aspect	112° (ESE)	Morning sun exposure; reduced afternoon heat stress
Soil pH (0–5 cm)	OpenLandMap Soil Attributes	6.5	Slightly acidic; suitable for a broad range of edible species

Source: Authors' calculations based on GEE datasets

These variables were subsequently used to characterize micro-environmental constraints and opportunities for edible plant cultivation by identifying the thermal, hydrological, vegetative, and edaphic conditions that influence species performance. This enabled a precise assessment of which crops can physiologically tolerate the local climate and soil parameters, and which planting strategies can be optimized for spatial and seasonal variation.

3.3. Plant scoring system

A list of more than 20 edible plant species was compiled based on documented ecological preferences, specifically tolerances or optimal ranges for temperature, precipitation, evapotranspiration, vegetation cover (NDVI), and soil pH. For each species, a compatibility score ranging from 0 to 1 was calculated. The scoring function compared the known ecological requirements of each species with the observed environmental profile of the study area. Scores closer to 1 indicated high compatibility and therefore higher suitability for cultivation within the defined buffer zone. This structured scoring approach enabled a reproducible and scalable assessment of plant–environment fit within urban and peri-urban smart-city contexts.

3.4. Stratified garden planning

Based on the seasonal compatibility scores, a stratified (layered) garden model was designed to optimize space, light availability, and ecological interactions. The planning approach integrated:

- Vertical stratification: use of multi-tier and modular beds to maximize sunlight interception;
- Horizontal stratification: arrangement of crops in layers based on root depth, canopy structure, and water requirements;
- Seasonal rotation schemes: crop placement adjusted according to seasonal shifts in temperature and NDVI;

- Companion planting principles: pairing species to enhance growth, soil health, and pest resilience.

This stratified garden design aligns with smart-city sustainability objectives by creating resource-efficient, ecologically responsive micro-agricultural systems.

4. Results

4.1. Environmental suitability scores

The plant scoring system yielded clear differentiation between species with high, moderate, and low compatibility with the environmental conditions observed in the Măgurele buffer zone. Of the 20+ edible species evaluated, approximately 35 percent received high suitability scores (0.75–1.00), 45 percent were moderately suitable (0.40–0.74), and the remaining 20 percent scored poorly (<0.40). Species with high drought tolerance, moderate heat resistance, and a preference for slightly acidic soils consistently ranked highest.

Table 2. Highest-scoring edible species for Măgurele, Ilfov

Rank	Species	Score	Notes
1	Rosemary	0.92	Excellent heat & drought tolerance
2	Thyme	0.89	Highly resilient perennial
3	Amaranth	0.85	Performs well under heat stress
4	Kale	0.78	Good multi-season adaptability
5	Swiss chard	0.74	Heat-tolerant leafy green

Source: Authors’ plant–environment scoring model

Plants such as rosemary (*Rosmarinus officinalis*), thyme (*Thymus vulgaris*), kale (*Brassica oleracea*), amaranth (*Amaranthus* spp.), and Swiss chard (*Beta vulgaris* subsp. *cicla*) achieved top scores due to their broad environmental resilience and compatibility with local temperature and soil pH values. Conversely, species with high moisture requirements or lower heat tolerance, such as spinach, lettuce, and certain coriander varieties, scored significantly lower.

4.2. Spatial and structural planning output

The stratified garden model produced a structured cultivation plan tailored to seasonal conditions. During high-temperature months, vertical layering favored heat-tolerant aromatic herbs placed in upper tiers to maximize airflow, while root vegetables and leafy greens were positioned in lower-shade zones to reduce evapotranspiration stress. Seasonal rotations suggested the introduction of cold-tolerant species, such as winter radish and hardy greens, during cooler months when NDVI values increase slightly.

Companion-planting simulations identified beneficial pairings such as rosemary–sage for pest deterrence, kale–chard for complementary root structures, and amaranth–basil for canopy balance. Overall, the resulting model demonstrated that an optimally layered micro-garden could maintain year-round productivity despite relatively low precipitation and elevated summer temperatures.

5. Discussion

The results demonstrate the viability of micro-agricultural systems in peri-urban smart-city settings when supported by high-resolution environmental profiling. The local thermal regime and low annual precipitation underscore the importance of selecting heat- and drought-tolerant species, consistent with agricultural sustainability literature [1], [2]. The strong performance of Mediterranean herbs and resilient leafy greens aligns with climatic conditions in southern Romania, where prolonged warm periods and intermittent rainfall favor stress-tolerant crops.

Moderate NDVI values (0.275) indicate sparse vegetation cover driven by anthropogenic land-use pressures and semi-arid summer conditions. Under these constraints, stratified micro-gardening systems can increase local vegetation density while providing thermal buffering, shading, and microclimate moderation. These outcomes align with the Guideline for Community Micro-Green Spaces, which identifies interstitial “green pockets” as priority areas for ecological regeneration in dense residential zones [8], and support smart-city objectives for mitigating urban heat island effects [4], [5].

The analysis also resonates with insights from the Local Public Policy Proposal for Community Gardens (Cluj-Napoca), which highlights degraded inter-block spaces and fragmented green strips as underused resources in Romanian cities [9]. The suitability of low-water-demand species identified here directly supports the policy’s recommended typologies—modular micro-gardens, parcel-based gardens, and urban orchards—designed for low maintenance and adaptability to variable site conditions. The effective use of stratified gardens in areas with uncertain soil quality is consistent with the Guide for Setting Up an Urban Garden, which promotes raised beds and container systems as practical solutions for contaminated or compacted soils [7].

Although the negative evapotranspiration value in the ERA5-Land dataset reflects a data-quality artifact, multi-variable normalization ensured stable species ranking. Future improvements may involve incorporating local sensor networks or citizen-science observations, in line with the participatory monitoring practices promoted in the Urban Permaculture Manual [6].

From an implementation perspective, the stratified garden model optimizes productivity in spatially constrained environments—a finding relevant for Romanian housing estates, where inter-block green areas are common yet underutilized. The vertical and horizontal layering strategies used in the model are consistent with ecological design principles in permaculture [6] and with urban-gardening methodologies emphasizing multifunctionality, biodiversity, and spatial efficiency [7], [8]. Agroecological practices such as companion planting, mulching, and layered canopy structuring further enhance ecological stability and reduce maintenance requirements.

Overall, these findings provide actionable insights for municipal authorities, community organizations, and smart-city planners seeking scalable, data-driven approaches to integrating productive green infrastructure into peri-urban landscapes. By combining remote-sensing environmental profiling, quantitative plant-suitability scoring, and stratified spatial design, the methodology offers a replicable, low-cost tool that

complements ongoing Romanian initiatives to formalize community gardening, regenerate inter-block areas, and expand nature-based solutions at neighborhood scale [8], [9]. As such, it advances both the scientific foundations and the practical deployment of climate-adaptive micro-agriculture in Romanian smart-city development.

6. Conclusion

This study demonstrates that integrating satellite-derived environmental profiling with a structured plant suitability assessment provides a robust foundation for designing sustainable micro-agricultural systems within smart-city contexts. The 250-meter buffer zone in Măgurele exhibits environmental conditions favorable to a targeted set of heat- and drought-tolerant edible species, while stratified garden planning enables efficient use of limited space through vertical and horizontal layering.

The results underscore the potential for small-scale, modular urban agriculture to enhance local resilience, increase biodiversity, and support climate-adaptive food production. By leveraging open-access geospatial datasets and replicable scoring methods, the approach outlined here can inform urban planning, community gardens, and educational interventions aimed at promoting green infrastructure.

Future work should focus on validating the model through field experiments, integrating real-time sensor data, and exploring socio-economic dimensions such as user adoption, cost efficiency, and community engagement. Overall, the findings contribute to the emerging literature on smart-city food systems and highlight practical pathways for implementing data-driven, sustainable micro-agriculture in urban environments.

References

- [1] S. Sanyé-Mengual, G. Orsini, and F. Gianquinto, "Agricultural sustainability in urban contexts: rooftop and city farming," *Journal of Cleaner Production*, vol. 122, pp. 1–10, 2015.
- [2] K. Specht et al., "Urban agriculture of the future: An overview of sustainability aspects of food production in and on buildings," *Agriculture and Human Values*, vol. 31, no. 1, pp. 33–51, 2014, doi: 10.1007/s10460-013-9448-4.
- [3] N. Mazzetto, A. Vianello, and L. Gios, "Integrating remote sensing and agroecological data for urban farming planning," *Urban Agriculture & Regional Food Systems*, vol. 10, no. 1, pp. 22–36, 2025.
- [4] W. Lyu, T. Törnqvist, and J. Niemi, "Urban agriculture potential under climate variability in Central and Eastern Europe," *Environmental Research Letters*, vol. 19, no. 3, pp. 1–14, 2024.
- [5] Food and Agriculture Organization of the United Nations, *Climate-Smart Agriculture Sourcebook*, 2nd ed. Rome, Italy: FAO, 2017.
- [6] Asociația Română de Permacultură, *Permacultură urbană: Manual de activități de protecție și regenerare a mediului*. Cluj-Napoca, Romania, 2014.
- [7] Fundația (conform documentului), *Ghid pentru amenajarea unei grădini urbane*. Romania, 2024.
- [8] *Aspire to Change*, *Îndrumarul pentru micro-spații verzi de comunitate*. Romania, 2025.
- [9] URBASOFIA, ADI Zona Metropolitană Cluj, Asociația S.O.S., and Asociația Clujul Sustenabil, *Propunere de politică publică locală pentru grădinile comunitare*. Cluj-Napoca, Romania, 2023. [Online]. Available: <https://www.clujmet.ro/wp-content/uploads/2024/04/PPP-gradinarit-urban.pdf>

Work–Life Balance for Female Employees in the Advertising–Marketing Sector: The Influence of AI Use

Cristina Leovaridis

*National University of Political Studies and Public Administration (SNSPA), Bucharest, Romania
cristina.leovaridis@comunicare.ro*

Camelia-Georgiana Gheorghe

*National University of Political Studies and Public Administration (SNSPA), Bucharest, Romania
gheorghe_camelia-georgiana25m@student.comunicare.ro*

Gabriela V. Popescu

*National University of Political Studies and Public Administration (SNSPA), Bucharest, Romania
gabriela.popescu@comunicare.ro*

Abstract

In knowledge-based organizations, employee satisfaction, loyalty, and work–life balance are closely linked. Advertising–marketing organizations rely on the involvement and expertise of highly qualified professionals. An additional challenge is gender inequality: women allocate more time to unpaid domestic work, which affects their participation in the labor market and their professional development. The objective of our qualitative research, conducted through semi-structured interviews, was to identify the work–life balance of female employees in advertising–marketing and the effects of AI use on it. Between February and April 2025, ten non-managerial female employees and five female managers from various organizations were interviewed. Findings showed that work–life balance in the advertising–marketing sector represented a major challenge for employees, regardless of hierarchical position, and that this balance varied depending on periods of intense activity and personal responsibilities. Both non-managerial employees and their managers face a high workload and the difficulty of disconnecting from professional tasks during personal time. A common point is that both groups considered schedule flexibility and company support essential for managing time effectively. A notable difference between employees and managers is the amount of personal time sacrificed: while non-managerial employees report that it is rare for them to sacrifice family or personal time, managers are forced to do so much more frequently, working overtime almost daily and being contacted often outside working hours, an indication of the additional pressure and responsibilities associated with leadership positions. The integration of AI into the work of advertising professionals has reduced the time allocated to repetitive tasks; however, these benefits are diminished by performance pressure and expectations of constant connectivity, if organizations do not establish clear policies regarding AI use and the protection of employees' personal time.

Keywords: working conditions; highly qualified employees; knowledge-based organizations; work flexibility

1. Introduction

The current concern of both employees and managers regarding the balance between personal life and professional life reflects an increased awareness of the impact that the pace and demands of contemporary professional life have on individual well-being and, implicitly, on organizational performance, since a workforce that is exhausted, stressed, and lacking time for personal activities is less productive, less creative, and more prone to burnout. Therefore, finding a balance between these dimensions is an important factor for the long-term sustainability and success of both employees and companies.

The advertising–marketing sector is representative of this topic, because it is characterized by a fast-paced work environment, tight deadlines, the pressure of constant innovation, and a competitive market. It is a professional field that requires a high level of commitment, and where the boundary between working time and free time is more difficult to draw. In the advertising–marketing sector, employees are constantly exposed to high levels of stress,

pressure, and the demand to remain permanently connected, which makes maintaining a balance between work and personal life a major challenge.

The pandemic period of 2020 further intensified discussions about flexibility, remote work, and the importance of employee well-being, highlighting the vulnerabilities of organizations that often prioritize productivity at the expense of employees' mental and physical health. In this context, combined with the continued existence of disparities in the European labor market between women and men, the study of work-life balance among female employees in the advertising-marketing sector addresses a current and highly relevant topic for the advertising industry in our country and beyond.

2. Working conditions of employees in the advertising sector in the context of digitalization

Work-life balance represents a person's ability to efficiently manage their time and energy so as to achieve satisfaction in both professional and personal life [1]. The concept of well-being at work is much more complex than it may seem. Beyond job satisfaction and the emotions experienced, it also includes the way in which work influences other aspects of life as well as the quality of psychological experiences in the workplace. It is a holistic state of well-being, that combines both professional and personal aspects [2].

While quality of life may be considered objective through factors such as income level or access to various services, subjective well-being refers to the individual's perception of their own life. This personal assessment can vary from one person to another, even under similar living conditions. The difference is explained by the fact that each person has their own values, aspirations, and interpretations of reality [3]. The evaluation of working conditions is an indicator of the individual's perception of professional life, this concept is complex and varies depending on the specifics of the workplace, the field of activity, or the profession; based on this subjective evaluation, one can compare how people perceive and value the quality of their own work [4].

As part of working conditions, the balance between working time and free time is a complex notion that depends on several factors, such as time spent at work, schedule flexibility, job security, workplace health and safety, and access to continuous training. Such a balance is important for individual well-being and long-term success [5]. Work-life balance is a challenge in the advertising sector: two-thirds of Romanian employees in the field are compelled to work during their free time, in the evenings or on weekends, in order to finish their tasks, which has a negative impact on their personal lives [6].

In advertising and marketing, the work climate varies depending on the agency: in smaller Romanian agencies, emphasis is placed on human relationships and friendship, whereas multinational companies often focus on internal competition and task fulfillment. The dimensions of the work climate range from autonomy, teamwork, creativity and friendliness on one end, to discipline, respect for rules and meeting objectives on the other, values that enhance performance and goal achievement [7].

A distinctive aspect of knowledge-intensive organizations - such as advertising agencies, compared to other types of organizations, is their nature as knowledge-centered structures. An advertising agency is a knowledge-intensive organization due both to the nature of the

work (the creation of symbolic messages based on the creativity and expertise of industry professionals) and to its focus on motivating personnel, who are predominantly highly qualified “gold-collar” employees. Although brand image and networks of relationships are important, the success of an agency depends on the competencies, development, satisfaction and loyalty of its employees [8]. Another specific feature is the ability to find innovative solutions to complex problems by leveraging employee expertise. These companies achieve remarkable performance due to their employees’ knowledge, since in knowledge-intensive work, solving complex problems requires abstract thinking and the ability to combine information in unconventional ways [5].

In professional organizations - which include advertising agencies - success depends on employee involvement and competencies. Flexible structures and open communication allow adaptation to change and the development of creative solutions. The most important factors for motivating and retaining employees in the long term are offering a good work–life balance, combined with interesting projects and opportunities for professional growth for expert employees [5]. A knowledge worker is someone who “transforms personal and corporate experience into knowledge by attracting, evaluating, applying, sharing, and disseminating it within the organization in order to solve specific problems or create value” [9].

The pandemic period brought a series of transformations to professional life in Romania across all sectors, leading to a reorganization of work methods, discipline and routines; work–life balance changed, also influencing lifestyle. Even employees in the creative industries - known for their freedom and creativity - experienced difficulties. Advertising specialists reassessed their resources and reconsidered their approaches depending on the relationship between client, agency and consumer. The industry shift toward innovation and technology had already enabled a more flexible adaptation, even before the pandemic, and the change in work practices in advertising was already a necessity, accelerated by digitalization [10].

Placing content on social media platforms (such as Instagram and Twitter) or on YouTube has transformed the consumer from a passive recipient into an active one, that is, into a user. The current stage experienced by any employee in an advertising agency is the need to adapt to the tools now provided by artificial intelligence, regardless of the position they hold within the agency [11]. The benefits of AI use in the advertising sector most frequently mentioned in the specialized literature refer to: the personalization of advertising messages based on collecting and analyzing consumers’ previous online behaviors [12], [13], [14]; much more precise segmentation through the use of real-time data collection and predictive analytics to identify consumers’ individual needs and preferences [15]; automation in advertising and marketing processes, including the use of chatbots and virtual assistants [16], [17]; and increased efficiency of advertising campaigns, including more accurate measurement of their effects, in real time, followed by extremely rapid adjustments [18], [19]. McKinsey & Company has shown that most of the potential value of AI is associated primarily with marketing and sales-related fields [20]; similarly, a global survey indicated that, in 2022, 87% of marketing professionals used AI to bridge the gap between online and offline experiences - a notable increase from the previous year (71%). Moreover, 88% of marketing professionals leveraged the power of AI to automate various processes,

including reporting, surpassing the previously recorded 83% [17]. Although the digital era offers numerous opportunities, it also comes with a series of challenges for employees in the advertising sector. The most common challenges are the speed and volume of change, and the rapid pace of technological development, which forces marketing and communication specialists to confront issues such as rapid changes in consumer behavior or the emergence of new communication channels.

The pandemic context of 2020 accelerated the adoption of digital technologies. Before the pandemic, videoconferencing was a tool used rarely, but the pandemic transformed these platforms into essential instruments for work, learning and social interaction. This rapid transition was accompanied by a series of unexpected challenges. While technologies such as Zoom allowed us to remain connected during isolation, their intensive use led to the emergence of new phenomena, such as “Zoom fatigue”, a condition characterized by anxiety, mental exhaustion and emotional depletion [21]. After these changes, employees working in the Romanian advertising sector increasingly desire flexibility in terms of workplace and working hours. Even after the pandemic, most employees in Romanian advertising expected an increase in remote work [21]. Employees and managers in advertising adapted quickly to the flexible schedule offered by working from home, although the volume of work increased; this working arrangement was considered a necessity in the field even before the pandemic [21].

Total flexibility – the kind that advertising professionals sometimes perceive as complete freedom – has been considered a paradox, because it has generated self-exploitation. At times, in order to complete a project on time, industry professionals work beyond regular hours, especially since the creative nature of advertising is a type of work in which boundaries are difficult to impose, particularly when passion is also part of the campaign-building process. This aspect leads to self-exploitation, with work invading personal space and private life, which translates into ignoring household responsibilities or neglecting one’s health for the sake of professional success. Professionals want to work at their own pace, in the space and moment of their choosing, often sacrificing personal life in order to achieve professional goals [11].

Advertising managers have acknowledged the importance of work–life balance, taking measures such as wellbeing programs, online breaks and team-building games. They have tried to limit the number of tasks to reduce pressure, offering schedule flexibility and measuring effectiveness through task completion. They also reduced the frequency and duration of online meetings, discussing only urgent and important matters. However, managers’ claims are only partially confirmed by their employees; a significant number of advertising employees expressed dissatisfaction with the high workload, overtime and difficulties in managing their free time. Employees wished for more understanding and financial support, considering they personally covered expenses for electricity, internet and online platforms [21].

During the pandemic, the difficulty of separating professional life from personal life was a reality for 58% of advertising employees, who tried to disconnect from work outside official working hours. Regarding the management of tasks during regular working hours (9 a.m.-6 p.m.), more than one-third of advertising professionals felt no change during the

pandemic, but for one-fifth (20%) it became more difficult, while for 19% it became easier. In the future, almost half of employees (49.6%) would prefer to work remotely for a maximum of two days per week, while 35% would like to work from home three or more days [22].

According to the most recent study conducted by UAPR on employee satisfaction in the communication industry, 7% of respondents work full-time from home, 10% work full-time from the office, and 68% come to the office at least two days per week. 69% of participants believe that work–life balance has improved with the introduction of the hybrid work model. The highest level of satisfaction appears among young people (18-24 years), with 77% agreement, followed by the 55-64 years age group (75%) and the 45-54 years age group (73%). On the other hand, only 64% of respondents aged 25 to 34 agree that work–life balance has improved since the introduction of hybrid work [23]. The hybrid work system offers, according to the majority of employees, the advantage of eliminating commuting. On the other hand, remote work also presents challenges, most of them social – such as maintaining connections with colleagues and team meetings – while challenges related to the work environment or performance are mentioned less frequently. In a competitive industry with a fast work rhythm, 27% of respondents state that they always feel stressed at work; among Mid-Management respondents, this percentage rises to 33%. More than half (56%) of respondents believe that gender balance in the industry is improving. Agreement on this topic increases to 77% among Starter-level respondents (with less than two years of experience) [23].

3. Gender inequalities in the labor market and their consequences

In the past decade, many changes have occurred for women in the labor market, especially for those in leadership positions. Research shows that organizations led by women are more innovative, have a stronger organizational culture and higher performance levels, and that women leaders, in addition to their skills, serve as a source of inspiration for other women [24]. Beyond the benefits for organizational culture, gender balance in leadership also has a financial advantage: companies in which at least 30% of top managers are women can achieve financial results up to 48% higher compared to companies with lower or no female representation in leadership positions [25].

The share of women in Romania's employed population increased slightly - from 44% to 46% between the 2002 and 2021 censuses. There is also a rise in the number of female specialists, who reached 60% of all specialists in 2021, compared with 51% in 2002 [26]. However, Romania records one of the largest gender gaps in labor market participation: the employment rate for women is 59.1%, approximately 19 percentage points lower than that of men, which stands at 77.7%, and below the European average of 69.3%. This indicates a major gender disparity in the labor market [27].

The employment rate – an important indicator for analyzing labor market dynamics – highlights a gender gap of 10.2 percentage points in the EU in 2023. This difference, calculated for individuals aged 20–64, shows that women remain less present in the labor market compared to men [28]. Although progress has been made regarding gender equality in the labor markets of the European Union, considerable disparities remain between member states: in 2023, Nordic countries such as Finland (0.2 pp), Lithuania (1.5 pp),

Estonia (2.4 pp) and Latvia (3.1 pp) reported the smallest differences between male and female employment rates, while in Southern and Eastern Europe, countries such as Romania (19.1 pp), Italy (19.5 pp) and Greece (19.8 pp) reported the largest gaps, caused mainly by the underrepresentation of women in the labor market [28].

In the European Union, women continue to earn less than men. In 2018, the average hourly wage of women was 14.4% lower than that of men. This difference varies significantly among EU member states, from 1.4% in Luxembourg to 21.8% in Estonia, while Romania recorded a difference of 5.5% [28]. Furthermore, beyond hourly pay disparities, there is also a significant difference in annual earnings between women and men, amplified by the fact that women work fewer hours and hold more part-time positions [28].

According to Eurostat data for 2022, only 45.4% of Romanian women and 62.7% of Romanian men were employed, a low employment rate compared to other EU member states. This gap reflects a structural issue in the Romanian labor market, namely the significantly smaller proportion of employed women compared to men and to the EU average, indicating a lower female workforce participation [27].

Romania ranks among the EU countries with the smallest gender pay gap, only 5.5%: this lower wage gap suggests, on average, similar salaries between women and men. But this statistic can be misleading because women's employment rate in Romania is low. At the same time, women often work in lower-paid sectors and occupy less senior positions, while men dominate well-paid fields such as technology and engineering. Another relevant factor is that many women choose flexible work arrangements, such as part-time work or remote work, to more easily balance professional life with family responsibilities [27].

An analysis of research on work–life balance has allowed for a classification of the most important factors influencing it, into nine main categories, offering a theoretical perspective on the topic. These are: work-family conflict, individual characteristics, family dynamics, work-related aspects, common work-family factors, the impact of conflict, personal strategies, organizational policies and dedicated programs [6]. There are also other factors that contribute to the difficulty of maintaining a balance between professional and personal life. Among the most important are the lack of childcare services - kindergartens and after-school programs are limited in Romania; inflexible working hours - a European study shows that fixed working hours represent an obstacle to work–life balance, especially for women; and the unequal distribution of responsibilities, as women continue to carry out most household tasks [1]. Research shows that negative working conditions significantly affect employees' quality of life, limiting free time and deteriorating social relationships. Moreover, the lack of time spent with family leads to feelings of guilt and loss [6].

In theory, in a democratic society that promotes equality, attracting women to the labor market should be a natural process. However, in practice, due to the persistence of traditional gender roles within the family, many women face significant challenges when trying to reconcile their careers with personal life [29]. The European Commission notes that, while the demand for a flexible and mobile workforce is increasing, women face more obstacles in balancing professional and personal life. The lack of care services, gender stereotypes and the unequal distribution of family responsibilities often force women to opt

for part-time work contracts, to the detriment of their professional development; moreover, this disparity can contribute to the lower presence of women in leadership positions and to the gender pay gap [30].

There is a link between the unequal distribution of domestic work and gender inequalities in the labor market: the fact that women allocate more time to unpaid household work significantly affects their participation in the labor market and their professional development. Traditionally, women are seen as the primary caregivers in the family, while men are viewed as responsible for providing financial support. This unequal division of labor is confirmed by statistical data showing that women in Romania spend far more time on unpaid household tasks compared to men. According to 2022 data, 87% of Romanian women engage daily in domestic work, compared to 49% in Germany and 54% in Luxembourg. This difference, more than 25% above the European Union average, demonstrates the strong presence of the traditional role of women as primary caregivers in Romanian families [26].

Even though the gender disparity in employment has decreased, the employment rate remains higher for men than for women in all EU states. At the EU-27 level, in 2021 the overall employment rate for individuals aged 20-64 was 73.1%, with 78.5% for men and only 67.7% for women. These differences are explained by the fact that women are often forced to choose between advancing their careers and dedicating time, for a period, to family and children. More flexible working arrangements and the reduction of gender stereotypes regarding domestic responsibilities could, in the medium and long term, lead to an increase in the employment rate among women [31].

Romanian professionals in leadership roles place high importance on following personal passions (97.5%) and financial independence (96.9%), closely followed by the desire for a balanced family life (94.4%). The difference is that, while men place passion first, women prioritize financial independence, and family is a priority for both genders - ranking third, with 95.3% of female leaders and 93.6% of male leaders including it in their top preferences [32].

The reason why few mothers build a career is most often related to the concern that doing so might negatively affect their children's development. However, a maternal role model who pursues her passions can inspire children to develop their own aspirations, regardless of gender. At the same time, the absence of an involved maternal figure may have negative consequences on children's emotional development [33]. The greatest challenge for working mothers is caring for sick children. The need to provide medical care and constant supervision forces many parents to make changes in their work schedules; studies show that more than one-third of mothers are forced to take medical leave when their child is ill, which may negatively affect their career and work-life balance in the long term [33]. In young couples, the addition of children and the professional development of both partners generate a new dynamic, in which gender roles are constantly renegotiated. Women are often the first to initiate these changes and influence the couple's relationship by promoting a more equal distribution of responsibilities [29]. According to the Global Gender Gap Report, at the current pace of progress, it will take approximately 132 years to achieve full gender equality at the global level [25].

4. Work–life balance of female employees in the advertising–marketing sector.

Qualitative interview research

4.1. Research methodology

The general objective of this research is to identify the work–life balance of female employees in the advertising–marketing sector and the influence of AI use at work on it. This objective involves a detailed analysis of how female employees in this sector balance professional demands with personal responsibilities. The main purpose is to understand the specific challenges these employees face - from professional pressure to managing free time and personal relationships. At the same time, this research aims to identify the factors that influence or hinder the balance between work and personal life, including the influence of AI on this balance, as well as the measures adopted to maintain stability and harmony between the two dimensions.

The research method used is qualitative, involving interviews with ten non-managerial female employees (Group 1) and five female employees in managerial positions (Group 2) - specifically, the managers of the interviewed non-managerial employees - from the advertising–marketing sector. As the research instrument, we chose the semi-structured, in-depth interview, which enables us to gather complex data from participants in both groups. The interview guide for Group 1 contained thirty questions, and the guide for Group 2 contained thirty questions as well.

The interview participants are women employed in the advertising–marketing sector. The selection criteria were specifically female gender and professional experience in advertising–marketing. Diversity was ensured in terms of age, departments in which the respondents work, type of agency (both multinational and local), positions held, years of experience in the field, and personal/family situations such as marital status and number of children, in order to obtain a comprehensive perspective on their experiences regarding work–life balance. We interviewed non-managerial employees and managers from two different advertising agencies, to enable comparison. One of the agencies is multinational, with a few hundred employees. It provides all advertising services, being part of a group that includes creative, media and public relations agencies. The second agency where we conducted interviews with employees and their managers is a small, Romanian-owned agency with around 20 employees, offering both creative and media services. These interviews were conducted between February and April 2025 and each lasted, on average, forty-five minutes.

Based on the general objective of the study and the key concepts presented in the theoretical section, we formulated four research questions for the first group, consisting of non-managerial employees (What are the employees' dissatisfactions/satisfactions in advertising regarding the fulfillment of family responsibilities in relation to professional life?; How can female employees manage their time so as not to be forced to give up family or social commitments because of work?; What are the effects of AI use in the agencies where they work on the work–life balance?; What are their recommendations and suggestions for a healthy work–life balance?), and four research questions for the second group, consisting of managerial employees (What are employees' dissatisfactions and satisfactions in advertising regarding the fulfillment of family responsibilities in relation to

professional life?; What are employees' expectations regarding the support provided by the company for managing family and personal responsibilities?; What measures are taken to improve this balance?; What is the influence of AI use on the activity in advertising agencies?).

Respondents in Group 1 hold various positions such as Junior Digital Account Executive, Account Executive, Media Planner, Social Media Specialist, Strategic Planner and PPC Specialist in client service, digital, social media and strategy departments. They have at least one year of experience in these advertising agencies and are employed full-time, working approximately 40 hours per week. They are between 21 and 31 years old. More than half are in relationships, two of them have one child each, and the rest are not in a relationship. Most live with their partners and do not care for other dependents.

Respondents in Group 2 are the managers of the employees in the first group. They are between 29 and 44 years old and hold leadership positions such as Digital Lead, Senior Strategic Planner, Senior Account Executive, Manager Account Executive and Social Media Manager in strategy, client service, digital and social media departments. They have at least three years of experience in these advertising agencies, are employed full-time, and work approximately 45 hours per week. Four of them are married, three of them have children; one manager is married without children, and one is single. Most live with their partners and children, and more than half care – though not directly – for other family members, such as parents and/or parents-in-law.

4.2. Analysis and interpretation of the data

4.2.1. Analysis and interpretation of data obtained from interviews with non-managerial female employees in the advertising–marketing sector

Dissatisfactions and satisfactions experienced by advertising female employees regarding the fulfillment of family responsibilities in relation to professional life

Female employees state that the work–life balance depends greatly on the period and on personal circumstances; some of them are students, others are mothers, therefore the balance between the two dimensions is never equal, and finding this equilibrium is a constant challenge: “At the moment, I can’t say that there is truly a balance because I’m also in my final university year, I’m working, I have responsibilities at home as well, it’s a bit stressful but I manage because I enjoy what I do” (R1). There are also employees who, despite all these, manage to have a healthy balance: “I’ve managed to reach quite a good work–life balance. Of course, it also depends on the period, but generally it’s fine, especially since I don’t have a family or children - otherwise I think it would be quite hard for me” (R2). Regarding the greatest challenges in attempting to find this balance, most employees mentioned the heavy workload due to multiple responsibilities, difficulties in time management, unexpected situations both at home and at the office, the lack of schedule flexibility, or difficulty disconnecting from work: “The psycho-emotional disconnection from the workplace. Many times, even though the schedule ended at 6 p.m., my thoughts and emotional state remained stuck in work contexts and I couldn’t move past them quickly” (R3). At the same time, through its work-related policies and practices, the company may either support or hinder female employees in achieving a balance between

work and personal life. Most employees are helped by flexible schedules: “We have a very relaxed schedule - working from home or the office as we want [...]” (R4), but some do not benefit from a very flexible schedule: “The schedule is too strict, every minute is counted, but somehow it’s fair so that all employees are equal and no differences appear. Just like I’m a student and have a weird schedule, others may need to be elsewhere during the day, and it was more useful for everyone that the schedule be flexible” (R5).

The most common aspects that make female employees feel fulfilled are the projects they work on, the results of campaigns, the teams they belong to, and the fact that they work in a field they are passionate about: “The feeling of professional fulfillment comes from creative projects and from collaborating with a talented team, which also fulfills me in my personal life” (R2). All female employees reported that they feel supported and understood by colleagues and supervisors in their effort to find a balance between work and personal life: “Yes, my manager understands the need for balance and encourages us to take time off when necessary. For example, she has suggested that I take a day off after a stressful period” (R6). Regarding benefits and facilities, the standard ones exist - such as annual leave and rest days; some agencies offer time-management courses, others provide a flexible schedule and understanding. All of these are helpful for female employees.

Ways of managing time so as not to give up family or social commitments because of work

At some point, all respondents felt overwhelmed by the multiple responsibilities in their lives. Even though some now feel they have managed to achieve balance, there were or still are moments when they feel overwhelmed by multiple situations - whether related to work, during busy periods with many deadlines and limited time, or to personal or family circumstances, when responsibilities as mother, wife, student and employee overlap: “There are ups and downs. At the moment I feel overwhelmed because I also have my bachelor’s thesis this year, I have been working for relatively little time, and I also moved in with my partner. There are many new things that make me feel overwhelmed sometimes because there are many responsibilities, but I know it won’t always be like this” (R1). Regarding time spent with family or sacrificed personal time, they state that this does not happen very often, but it does occur during busy periods; moreover, they tend to sacrifice personal time when they also have other responsibilities outside the workplace: “Work time is work time, and it’s a normal full-time schedule, but combined with university responsibilities, it feels like it takes up all my time and that my life becomes just work and nothing else” (R5). None of the respondents felt that their career had been affected because of family responsibilities: “I haven’t felt that, maybe because I don’t have family responsibilities and all my focus is on my career” (R7).

Most employees use digital calendars, to-do lists, and task prioritization to manage their time efficiently - ideally completing their tasks during work hours: “Each day begins with a priority list. Any additional task that appears during the day is placed depending on its priority and classified as important or manageable within a wider time horizon. All tasks must be mapped onto the eight-hour workday [...]” (R3). Regarding time allocated to professional and personal activities, more than half of respondents have a ratio of 60% professional activities and 40% personal activities, spending on average 8-10 hours per day working, 2 hours on household tasks, and the remaining time as personal time; however,

on weekends they dedicate personal time to family and hobbies: “During the week I allocate more hours to professional activities, and personal ones are limited, but on weekends I strictly focus on personal activities; exceptions are very rare” (R8). Or “I’d say it always depends. No week is the same. Some periods are more relaxing, others more stressful - either at work or at home, or the child is sick, or there’s a very important project. I’d say it’s 50-50” (R2).

To the interview question “How flexible is your work schedule? Can you adjust it according to personal or family needs?”, all female employees responded that their schedule is quite flexible and can be adjusted when needed. To the question “How often do you have to work outside working hours or on weekends?”, all respondents said unanimously that they very rarely work outside normal hours - except during extremely busy periods or when they choose to stay and finish tasks, and that they do not work at all during weekends. To the question “How often are you contacted by colleagues or clients outside working hours?”, responses indicate that they are contacted outside working hours only for urgent situations requiring immediate resolution; otherwise, they respect work and personal time boundaries. To the final question about working arrangements, “Do you have the possibility to work from home or remotely?”, all answers were affirmative: all these respondents can work from home or remotely, some of them as much as they want, others for two days a week.

From the responses to “Do you feel comfortable refusing additional tasks when you are already overloaded?”, it appears that one-third of respondents feel comfortable refusing extra tasks: “Yes, this behavior is actually encouraged. Overloading can lead to decreased quality and the risk of major errors in campaigns or materials, so it is important to ensure that all colleagues work at their full potential in a healthy and feasible way” (R3). Meanwhile, a quarter do not feel comfortable or in a position to refuse additional tasks: “I don’t feel comfortable, and I don’t want to refuse because I’m at the beginning and I want to learn as much as possible” (R1). Another interview question addressed the impact of professional demands on employees’ personal lives: “How do you handle situations where you must postpone or cancel a personal commitment because of work?”. Responses were mixed: some female employees said they had not encountered such situations because this does not happen in their agency, or because they do not make personal plans during working hours: “Honestly, I don’t really make plans during working hours if I know I cannot take time off” (R5); while others had encountered such situations, but very rarely: “I try to avoid them, but sometimes they are unavoidable; still, I communicate clearly and look for alternative solutions” (R9). The question “Do you have access to employee support programs?” explores the presence and accessibility of resources offered by the employer to support employee well-being and facilitate work-life balance. The responses show that most employees have not needed such support programs and do not know whether they exist: “Since I didn’t need them, I haven’t looked into such services or support” (R10). Others, however, are aware of certain benefits offered by the company, for example: “Yes - extra vacation days, discounts for certain subscriptions, time-management courses, health insurance and more” (R2).

The influence of AI use on the work-life balance

Regarding the professional activities for which non-managerial respondents use AI, they mainly mentioned tasks that are strategically neutral and low-stakes, such as drafting texts

or synthesizing information during the initial documentation phase related to a received brief: “I used it in research and documentation processes, when I needed a quick overview of a topic I didn’t know much about beforehand, for example in the banking or construction sectors etc.” (R3).

AI is also used for routine tasks, such as drafting preliminary texts, rephrasing messages or summarizing very long documents, especially when deadlines are tight and the pressure to deliver results quickly is high: “It helped me quickly generate ideas when I was under time pressure” (R4). Respondents also mentioned the usefulness of AI in obtaining several solution options in a short time, including in cases of creative block, but emphasized that the final decision remains human and belongs to the professionals: “I noticed I no longer wasted so much time on easy, repetitive tasks” (R1); “Sometimes it helped me overcome initial creative block. I also use it to generate elegantly phrased email drafts” (R7); “It gives us more angles of thinking on the same subject, but from which we, humans, still have to choose” (R2). The advertising specialists interviewed also noted the use of AI in structuring presentations for pitches, in generating possible creative concepts during brainstorming phases, though final responsibility always remains with the human actor.

As for the effects of AI use on the time allocated to completing tasks - and thus on work-life balance - respondents mentioned a moderate increase in the speed of completing simple, repetitive tasks, and thus a visible increase in efficiency in routine activities. However, the time gained is not used for personal life (family, friends, rest etc.), but is dedicated, on the one hand, to reformulating and correcting/adjusting AI-generated outputs, selecting the most suitable ones, and on the other hand, to training and improving their skills in using the new tools. All this takes place against a backdrop of increased expectations regarding efficiency from management and clients: since they know that employees use AI tools, they request even faster delivery of results, increasing pressure and generating stress: “Yes, AI generates multiple versions, but adjusting them requires extra time” (R6); “Clients impose shorter deadlines than a few years ago, because they know that now we can use AI” (R3).

Recommendations from employees for a healthy work-life balance

Based on the analysis of the responses, female employees most need schedule flexibility in order to achieve work-life balance. Although they already benefit from some flexibility, they wish to choose personally the periods in which they adjust their schedules. They also request support programs for mothers with childcare responsibilities: “Even though I don’t have children, I think workshops for kids held and organized within the agency could help. These sessions could provide after-school support for parents who finish work later” (R3). Additionally, employees expressed the need for support from the company and managers regarding specific needs, wanting to feel heard and understood: “To pay attention to each person’s needs and offer benefits tailored to those needs” (R8); and “More active and involved communication, more understanding, and relaxed discussions on this topic, so that employees feel at ease when requesting a day off or a more flexible schedule on days that they know will be busier” (R10).

4.2.2. Analysis and interpretation of data obtained from interviews with managerial female employees in the advertising–marketing sector

Ways of managing time so as not to give up family or social commitments because of work

To the question “How would you describe your work–life balance at this moment?”, female managers - unlike non-managerial employees, who were still able to find some balance - answered that they do not really have a balance between professional and personal life, spending less time with their families than they would like: “At the moment, balance doesn’t really exist. There are periods when professional life is more demanding, and I have little time and energy for my family and myself; other times I manage to find a more balanced rhythm, but it requires better time management” (M1). The most common challenges are a very heavy workload, unexpected situations in both personal and professional life, proper time management, establishing boundaries, and disconnecting from work during personal time: “I think my biggest challenge is precisely finding this balance between personal and professional life. I have a demanding work schedule and two small children - it’s difficult; unexpected situations can appear both at work and at home” (M2).

The next questions relate to time management and the schedule female managers have. The first is: “How often do you have to sacrifice time spent with family or personal activities because of professional demands?”. From their responses, it is clear that for managers this happens quite often: “Quite often I have to sacrifice time dedicated to friends, hobbies or simply my own relaxation because of professional demands. There are evenings when I have to work overtime, weekends when I have to check emails or prepare presentations” (M3). From the answers to the next question - “How much time do you allocate, on average, to professional activities and how much to personal activities?” - we learned that the time allocated to professional activities is greater than that allocated to personal activities. Work occupies most hours of the day, with an eight-hour schedule plus extra hours, while personal activities occur mainly on weekends: “For professional activities, I have my job hours plus extra hours if needed; but weekends, with few exceptions, and holidays are for me and my family” (M4). Regarding how often female managers have to work overtime, on weekends, or how often they are contacted by colleagues or clients outside working hours, it emerged that they work overtime almost every day during the week, but not during weekends, with minor exceptions: “Quite often, almost every day during the week, but it depends on the period. I don’t work on weekends, maybe very rarely” (M5). They are contacted by colleagues or clients outside working hours fairly often, mostly in urgent situations: “I am contacted by colleagues or clients outside working hours only if it’s about urgent questions that can’t wait until the next day” (M5).

The next interview questions explore time-management strategies, work-organization methods and coping mechanisms used by female managers in the advertising–marketing sector when conflicts arise between professional demands and personal commitments. From their responses, we learned that they try to avoid situations in which they need to postpone or reschedule, but there are periods when it is necessary to postpone a personal plan - in such cases they communicate the situation and reschedule if possible: “I try to anticipate busy periods at work and avoid making important personal plans during those

times” (M3). Regarding the organization of time, what works best for them is task prioritization, setting personal boundaries, or delegating tasks to their team: “I try to be as organized as possible at work, make priority lists, block time in my calendar for important tasks and avoid distractions. I communicate with the team and clients about my availability. At home, I try to establish routines for the child, involve my husband in household tasks, and make the most of the time we spend together” (M1).

The support offered by the company for managing family and personal responsibilities

Female managers consider the greatest challenges faced by female employees to be: the lack of time spent with family, the social pressure to be a good mother, wife and outstanding employee - “Finding a balance between professional and family demands, even employees without children have other responsibilities and it can be difficult. Another challenge is social pressure because there are different expectations for women regarding professional and personal roles” (M5). In addition, they believe that current policies and practices may contribute to achieving a work–life balance, but they are not sufficient or tailored - they are mostly standard policies: “Company policies offer a certain level of flexibility, but they could be improved to better meet the needs of employees with family responsibilities. Currently, the benefits focus more on health and professional development, but they could be expanded to include more direct support for family responsibilities” (M3).

The next two questions refer to the actual solutions and the real support that female employees receive from the agency: “What types of support do you consider most useful for employees in managing family and personal responsibilities?” and “Are there specific policies or programs in the company aimed at supporting female employees’ work–life balance?”. Managers responded that the most useful support solutions would be more days off and flexibility, task automation, encouraging work–life balance within the team, and childcare programs. Regarding company policies, they stated that these are mostly standard policies, not tailored to the needs of each female employee: “We have a remote work policy and a time-management program, but there are no specific support programs for childcare” (M1).

Based on the responses received, it appears that female managers are concerned about the well-being and the personal-professional balance of their female employees. Most often, they encourage a healthy balance through open and effective communication, respecting working hours, and equitable task distribution in order to avoid overload: “I encourage this balance by offering support in task prioritization, support for time-management courses, organizing the team so that tasks are distributed fairly, and experience sharing across various projects to make work time more efficient.” (M4). Regarding the possibility of flexible schedules for employees needing to resolve personal matters, managers show understanding and try to find solutions adapted to individual needs: “I handle these situations with empathy and understanding, analyzing each case individually and trying to find solutions that work both for the employee and for the team” (M3).

As for the resources available to help with balance management, most female managers say that resources do exist and include time-management courses, stress-management courses, flexible schedules and remote work: “Currently, resources are limited. There are leave policies, but we do not have a dedicated department or specific programs to support

female employees in this regard” (M1). Interviewees believe that female employees’ greatest expectations from the company refer to understanding their needs and providing real support: “I think female employees expect the agency to understand and respect their personal and family needs, the possibility to openly discuss challenges related to balance, support for childcare or for caring for other dependents” (M2).

The influence of AI on activity in advertising agencies

Regarding the role of AI in the departments they manage, the interviewed managers acknowledged the advantages of using AI in automating tasks, generating content, faster campaign execution, reducing costs, personalizing messages, and segmenting audiences: “An obvious benefit is time savings: until now, we used to write 15 versions of ad copy over several days; now we have these 15 versions in about 10 minutes, with a well-crafted prompt, of course” (M3); “Since clients want things faster and cheaper, with the help of AI we can offer them exactly what they want” (M5).

At the same time, the newly emerged organizational challenges are not ignored, such as: organizing training sessions for employees to familiarize them with the new tools as a result of the new competencies required; the resistance of some employees to technology; the creation of new positions adapted to technological changes; and integrating AI-related processes into the agency’s workflow: “We developed an internal AI training program for our employees, so they can stay up to date with everything new in this field, taught by external AI specialists - it was absolutely necessary given the speed of technological evolution” (M4); “Agencies that want to keep up will create new positions for people who will dedicate most of their activity to efficiently integrating AI into the company’s operations: Prompt Architect, AI Content Director, AI Personalization Specialist, AI Automation Engineer” (M1); “We have already started integrating AI-related processes into our agency’s workflow; we still have work to do, but we have made the first steps” (M2).

Measures implemented to improve work–life balance

Based on the female managers’ responses, we found that the measures they take to prevent female employee overload include distributing tasks within the team, maintaining open communication, monitoring workload, and offering feedback and recognition for work performed: “To prevent overload and ensure a supportive environment, I respect deadlines, plan projects realistically, offer regular feedback, and make myself available to discuss any issues” (M5). All the interviewed managers are open to suggestions from female employees. These suggestions are collected during weekly meetings and periodic one-on-one discussions, which also help ensure that implemented measures are adapted to specific needs. Regarding involvement and problem-solving, female managers state that they listen to employees’ needs and work together with them to resolve situations: “By listening to each female employee regarding the issues they face, and I try to solve them - if it is within my control - through the previously mentioned methods” (M4).

5. Conclusions

Since gender inequalities persist in the European labor market, including in Romania, where women represent a smaller share of the workforce and face wage disparities, work–life balance remains a challenge, influenced by a series of factors including individual

characteristics, family dynamics, work-related aspects, the lack of childcare services, inflexible working hours, and the unequal distribution of household responsibilities. Work–life balance is an important factor for motivating and retaining employees in advertising agencies. In the advertising sector, where creativity and employee expertise are essential for organizational success, female employees face challenges such as rapid technological change, cultural diversity, and the need for flexibility.

The results of the research conducted with the first group showed that work–life balance is a constant challenge for female employees in advertising, varying depending on the period and personal circumstances (for some respondents, for example, being students or mothers). The main sources of dissatisfaction relate to the heavy workload, difficulties in time management, and the inability to emotionally disconnect from work after hours. On the other hand, sources of satisfaction come from creative projects, teamwork and passion for the field, elements that contribute to the personal fulfillment.

Both non-managerial female employees and their female managers have, at certain moments, felt overwhelmed by multiple responsibilities - whether due to workload or personal and family circumstances. Although sacrificing personal or family time is not a frequent practice, it does occur during peak periods.

In the advertising agencies where the respondents from the first group work, AI tools are used for a wide range of tasks, but primarily in the initial stages of developing an advertising campaign: preliminary documentation on certain subjects and synthesizing information, content reformulation, drafting initial versions of texts, visual elements, creative concepts, emails etc. - in short, tasks considered to have low strategic stakes. The selection and adjustment of AI-generated outputs to client requirements, consumer cultural context, market specifics etc. are always performed by human agents - that is, by professionals in the agencies. Although the speed of information generation is higher, the overall time investment remains approximately the same, because extra time is needed for analysis, discernment and decision-making regarding AI-generated proposals. This is in addition to the effort required for familiarization and upskilling with constantly evolving technologies.

Female employees' recommendations for achieving work–life balance are primarily related to working hours, specifically their flexibility. There were also recommendations for support programs dedicated to mothers, such as workshops or after-school programs organized by agencies.

The results of the research conducted with the second group of respondents showed that female managers perceive the main challenges faced by employees in their teams to be the lack of time spent with family and the social pressure to fulfill multiple roles simultaneously. According to them, current company policies offer some flexibility, but are not sufficient or specific enough to address the needs of female employees with family responsibilities. Managers consider that the most useful support would be offering more flexible schedules, automating tasks and implementing childcare programs.

Managers acknowledge the economic benefits of integrating AI into agency activities (reduced execution time and costs), but also the associated challenges that generate

organizational changes - such as redefining competencies required of current employees, providing AI-related training, creating new positions for AI specialists, and developing innovative solutions for new client demands. The results of our research show similarities with the findings of other studies, according to which organizational culture is also an important factor in the successful integration of AI in organizations: cultural readiness, rather than technical infrastructure, fundamentally influences the effectiveness of AI integration [34]. The use of AI is emphasized exclusively as a tool for advertising professionals, not as a replacement for them. The effects of AI on improving work–life balance are relative: the time saved on repetitive tasks taken over by AI is instead devoted to analysis, adaptation, interpretation, verification, contextualization and decision-making, as well as upskilling employees so that they can work with continuously evolving AI technologies. Through these conclusions, our research aligns with the findings of other authors, who assert that lifelong learning is essential for professionals to adapt to evolving demands in a rapidly advancing technological landscape, ensuring they remain resilient, relevant and capable of navigating the complexities of a dynamic work environment [35]. Moreover, the benefits of AI are diminished by performance pressure and the expectation of being constantly connected, especially if organizations do not establish clear policies regarding AI use and the protection of employees’ personal time.

To prevent overload among female employees, the interviewed managers strive to distribute tasks fairly within the team, maintain open communication, monitor workload and provide feedback. They are also open to suggestions from employees. The study found that work–life balance in the advertising–marketing sector represents a significant challenge for female employees, regardless of hierarchical position, and that this balance fluctuates depending on peak workload periods and personal responsibilities. Both non-managerial female employees and their female managers face a high volume of work and difficulty disconnecting from professional tasks during personal time. A similarity is that both groups consider schedule flexibility and company support essential for managing their time effectively. A difference between employees and their managers is the amount of personal time sacrificed: while non-managerial employees state that they rarely sacrifice family or personal time, managers are forced to sacrifice it much more frequently, working overtime almost daily and being contacted often outside working hours. This difference highlights the additional pressure and responsibilities associated with managerial positions.

A methodological limitation is that although the results of this study provide a useful perspective on work–life balance among female employees in the advertising–marketing sector, the samples used are not representative of all types of agencies and departments. In addition, the study focused on a limited set of variables; therefore, other factors - such as organizational culture or individual characteristics of team members - may also influence the results. Furthermore, the study was conducted within a specific cultural and geographical context, and the findings may be influenced by these particularities, limiting their applicability in other contexts. In the future, studies with larger and more diverse samples could be conducted. The results of this research should be interpreted within the specific context of the advertising agencies studied. This study focused on a specific time period, and the results may not remain valid in the long term.

Rapid changes in organizational environments and technological developments may influence team dynamics and the ways in which female employees - with or without managerial positions - manage their time to achieve a balanced relationship between work and personal life. A future research direction for this study could further explore the effects of emerging technologies, such as artificial intelligence, on the work–life balance of female employees in the advertising–marketing sector, comparatively across different European countries, to identify how organizational cultures shaped by national cultures and labor policies contribute to the formation of this balance.

References

- [1] D. Petrovai, *Eficiență în viața profesională și în cea personală*. Timișoara, Romania: Centrul Parteneriat pentru Egalitate, 2006.
- [2] E. Losii, "Starea de bine a angajaților în cadrul echipelor de muncă," *Univers Pedagogic*, no. 4(80), pp. 17–26, 2023.
- [3] M. Vasile, "Bunăstarea subiectivă în România: Factori care influențează satisfacția cu viața și bunăstarea mentală," *Calitatea Vieții*, vol. 30, no. 3, pp. 299–312, 2019.
- [4] I. Mărginean, "Calitatea vieții în România: prezent și perspective," *Calitatea Vieții*, vol. 21, no. 3–4, pp. 231–237, 2010.
- [5] C. Leovaridis, *Noi caracteristici ale calității vieții în contextul economiei cunoașterii și al competiției pe plan european: aspecte organizaționale și manageriale*. Bucharest, Romania: Editura Expert, 2013.
- [6] C. Leovaridis and E.-M. Vătămănescu, "Aspects regarding work–life balance of high-skilled employees in some Romanian services sectors," *Journal of Eastern Europe Research in Business & Economics*, vol. 2015, art. 969136, 2015, doi: 10.5171/2015.969136.
- [7] C. Leovaridis and D.-M. Cismaru, "Characteristics of organizational culture and climate in knowledge-intensive organisations," *Romanian Journal of Communication and Public Relations*, vol. 16, no. 2, pp. 35–56, 2014.
- [8] C. Leovaridis and I. Răchită, "Storytelling în agențiile de publicitate – O cercetare calitativă," *Revista Română de Sociologie*, vol. 30, no. 1–2, pp. 67–105, 2019.
- [9] V. Sornlertlamvanich, *Managing Knowledge Workers*. Knowledge Management System, 2005.
- [10] R. Surugiu and M. Moraru, "Strategii de adaptare a muncii în agențiile de publicitate din România în perioada pandemică," in *Integrare prin cercetare și inovare*, pp. 119–122, 2022.
- [11] R. Surugiu and M. Moraru, *Agencia de publicitate. Reconfigurări ale muncii în industria creativă*. Bucharest, Romania: Tritonic, 2025.
- [12] J. Wang, "Screening soft information: Evidence from loan officers," *RAND Journal of Economics*, vol. 51, no. 4, pp. 1287–1322, 2020, doi: 10.1111/1756-2171.12357.
- [13] J. Kietzmann, J. Paschen, and E. Treen, "Artificial intelligence in advertising: How marketers can leverage artificial intelligence along the consumer journey," *Journal of Advertising Research*, vol. 58, no. 3, pp. 263–267, 2018, doi: 10.2501/JAR-2018-035.
- [14] Y. Zhang, I. W. Tsang, and L. Duan, "Collaborative generated hashing for market analysis and fast cold-start recommendation," *IEEE Intelligent Systems*, vol. 35, no. 5, pp. 84–95, 2020, doi: 10.1109/MIS.2020.3025197.
- [15] J. Zhong, "[Retracted] Exploring and researching ideological and political education of college students' psychological quality for the development of artificial intelligence," *Mobile Information Systems*, vol. 2021, art. 2453385, 2021, doi: 10.1155/2021/2453385.
- [16] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," in *Proc. 3rd Int. Conf. Learning Representations (ICLR)*, 2015. [Online]. Available: <https://arxiv.org/abs/1412.6980>
- [17] V. Kumar, A. R. Ashraf, and W. Nadeem, "AI-powered marketing: What, where, and how?" *International Journal of Information Management*, vol. 77, art. 102783, 2024, doi: 10.1016/j.ijinfomgt.2024.102783.
- [18] A. Goldfarb and C. Tucker, "Privacy regulation and online advertising," *Management Science*, vol. 57, no. 1, pp. 57–71, 2011, doi: 10.1287/mnsc.1100.1246.
- [19] E. Brynjolfsson and A. McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. New York, NY, USA: W. W. Norton & Company, 2014.
- [20] M. Chui et al., "Notes from the AI frontier: Applications and value of deep learning," *McKinsey & Company*, Apr. 17, 2018. [Online]. Available: <https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-applications-and-value-of-deep-learning>
- [21] C. Leovaridis and E.-G. Păun, "Echilibrul muncă – viața personală în perioada pandemiei. O comparație între sectoarele IT și publicitate," *Revista Română de Sociologie*, no. 1–2, pp. 23–51, 2022.
- [22] UAPR, *UAPR Survey: Lucrul în publicitate în perioada pandemiei*. Bucharest, Romania, 2021.

- [23] UAPR, UAPR Survey: Studiul de satisfacție a angajaților din industria comunicare. Atitudini și emoții cheie. Bucharest, Romania, 2024.
- [24] McKinsey & Company, Women in the Workplace 2024, 2024.
- [25] MKOR, “În căutarea echilibrului: O analiză a leadershipului feminin în afacerile din România,” 2024. [Online]. Available: <https://mkor.ro/blog/analiza-leadershipului-feminin-in-afacerile-din-romania/>
- [26] Friedrich-Ebert-Stiftung, “Cum a evoluat participarea femeilor din România în economie, în ultimii 20 de ani,” Monitorul Social, Mar. 25, 2024. [Online]. Available: <https://romania.fes.de/ro/e/cum-a-evoluat-participarea-femeilor-din-romania-in-economie-in-ultimii-20-de-ani.html>
- [27] Friedrich-Ebert-Stiftung, “Inegalitățile dintre femei și bărbați în participarea pe piața muncii. Cum stă România comparativ cu alte țări din Uniunea Europeană?” Monitorul Social, Jul. 15, 2024. [Online]. Available: <https://romania.fes.de/ro/e/inegalitatile-dintre-femei-si-barbati-in-participarea-pe-piata-muncii-cum-sta-romania-comparativ-cu-alte-tari-din-uniunea-europeana.html>
- [28] Eurostat, “Gender statistics,” Apr. 2024. [Online]. Available: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Gender_statistics
- [29] A. B. Sănduleasa, Politici familiale, ocupare și roluri de gen: o analiză privind influența factorilor culturali asupra atitudinilor față de participarea femeilor pe piața muncii, 2016.
- [30] C. Leovaridis and A. Nicolăescu, “Raportul viață profesională – viață privată, preocupare de actualitate a UE în domeniul pieței muncii,” Revista Română de Sociologie, no. 1–2, pp. 108–122, 2011.
- [31] R. Moldoveanu, Femeile și bărbații – parteneriat de muncă și viață. Bucharest, Romania: Institutul Național de Statistică, 2022.
- [32] MKOR, “De 8 martie sărbătorim diversitatea.” [Online]. Available: <https://mkor.ro/blog/de-8-martie-sarbatorim-diversitatea>
- [33] I. Chistruga-Sinchevici and N. Borgan, “Provocări în reconcilierea vieții de familie și vieții profesionale a mamelor cu copii de vârstă preșcolară,” Revista de Filosofie, Sociologie și Științe Politice, vol. 179, no. 1, pp. 128–139, 2019.
- [34] R. M. Benshams, “Cultivating organizational culture for AI integration: A framework for Smart Cities and Regional Development,” Smart Cities and Regional Development Journal, vol. 9, no. 4, pp. 125–137, 2025, doi: 10.25019/cmstt369.
- [35] A.-C. Alexandru, “Building a smart economy: Training the workforce in multi-source data and AI-enhanced economic analysis,” in Proc. 12th Smart Cities Int. Conf. (SCIC), vol. 12, Resilient Communities Empowered by Collective Intelligence. Bucharest, Romania: Pro Universitaria, 2024, pp. 265–283. [Online]. Available: <https://www.scrd.eu/index.php/scic/article/view/696>

Structuring and Activation of Knowledge for Intelligent Legal Systems in Smart Cities: Towards Transparent and Fair Justice

Nicolae Pelin

Academy of Economic Studies of Moldova, Chişinău
nicolae.ion.pelin@gmail.com

Abstract

This paper proposes a conceptual architecture for structuring and activating legal knowledge in intelligent systems that could assist first-instance courts and digital public services. It asks how formal rules and ontologies can be combined with large language models while preserving human responsibility for legal interpretation and decisions. The analysis draws on the author's earlier work in logic programming, selected literature on legal AI, and documented digital-justice initiatives in Europe, the United States, and China. Exploratory conversations with language models informed the design, but the paper does not report a working prototype, a comparative performance test, or measured effects on judicial outcomes. The proposed architecture has four linked functions: extracting facts from documents; representing relevant norms, exceptions, and case relationships; checking inferences against those representations; and presenting reasons, uncertainties, and an audit record to a human user. Language models could help process unstructured text and support dialogue, while rule-based components could make selected reasoning steps traceable. The comparison distinguishes cross-border information exchange and public-sector algorithmic oversight from actual automated adjudication. Estonia provides an example of digital infrastructure, but its Ministry of Justice has stated that it has not developed an AI judge for small claims. For the Republic of Moldova, the paper recommends a phased evaluation of narrowly defined assistance tasks, starting with transparent rules, verified data extraction, judicial review, and regular updates to the knowledge base. Open-textured norms, contested facts, bias, privacy, and errors in language-model output limit what formalization can establish. Any gains in consistency, processing time, cost, or public trust remain hypotheses that require case-level testing and independent assessment before deployment.

Keywords: logical models; computational law; judicial accountability; hybrid reasoning; explainable AI

1. Introduction

Artificial intelligence (AI) can assist legal research and court administration, but its use in judicial work raises questions about transparency, consistency, and fairness. This paper proposes a hybrid architecture for assistance rather than automated adjudication. The author's earlier work examined logic-based AI in law [1] and the fairness–law–procedure framework [2]. Symbolic representations, including rules and ontologies, can be combined with language models for text processing, subject to verification and human review.

Horn clauses provide one way to represent conditional rules; the author's work on logic programming offers background for this approach [3]. A 1981 conference abstract proposed joint handling of deterministic, fuzzy, and probabilistic information in industrial process control [4]. Its relevance to legal systems is an analogy, not evidence of judicial performance.

Dialogue may help identify missing facts and explain how a proposed conclusion was reached. Exploratory exchanges with Gemini, ChatGPT, and Grok informed the conceptual design in this article, but no prototype or controlled evaluation is reported.

2. Knowledge Structuring in the Legal Field

An intelligent legal assistant requires explicit representation of relevant norms and facts, followed by controlled use of that representation. Candidate knowledge elements include:

- A source hierarchy, including the constitution, codes, and other applicable instruments.
- Relations among norms, including exceptions and temporal validity.
- Deontic categories such as obligation, prohibition, and permission.
- Epistemic distinctions between established facts, assertions, and uncertain evidence.

2.1. Logical Formalization of Law

Horn clauses can encode some legal provisions as conditional rules: if specified conditions are established, a stated consequence follows within the model. Potential benefits include:

- Traceable inference steps for rules that have been correctly encoded.
- Reproducible outputs for the same verified inputs and rule version.
- Structured links to relevant prior decisions where their legal status is clear.

These benefits depend on accurate fact extraction, valid encoding, and handling of exceptions. Ontologies can link participants, events, legal acts, and dates; knowledge graphs can represent such relationships without replacing judicial interpretation.

2.2. Knowledge Activation through Dialogue

A proposed dialogue workflow would have three stages:

- Identify facts and participants from documents, with human verification of extracted data.
- Ask targeted questions about missing or disputed information.
- Transform verified text into a structured case representation for rule checks.

The interface should show the source and status of each fact, the applicable rule version, and the limits of any inference.

2.3. Problems of Formalization and Limitations

Formalization and language-model processing have important limits:

- Open-textured legal concepts and contested facts may resist precise encoding.
- Language models can misread documents or invent content, requiring independent verification.
- Changes in legislation and case law require versioned updates and review.

A hybrid design can combine different tools, but neither fuzzy nor probabilistic output establishes the legal correctness of a conclusion.

3. Intelligent Modules in the Legal System

The proposed legal assistant has distinct modules for fact extraction, knowledge representation, inference, and explanation. Their separation could support maintenance and auditing, provided interfaces, data provenance, and human responsibilities are specified.

3.1. Fact Extraction Module

This module is designed for the collection and primary structuring of information. Data sources may include:

- Judicial documents, complaints, and applications.
- Electronic registries, normative databases.
- Precedents and decisions of previous courts.

The LLM performs a preliminary analysis of the text, highlighting key events, participants, and legal categories, after which the data is converted into a structured format suitable for logical analysis. For instance, the textual description of a conflict can be converted into a graph where nodes are participants and objects, and edges represent legal actions and consequences.

3.2. Knowledge Formalization Module

The formalized knowledge base is the core of the system. This module includes:

- Logical rules describing legal norms in the form of Horn clauses.
- Ontologies linking legal concepts, participants, and actions.
- Precedent graphs, allowing the use of experience from past decisions.

This module would represent applicable norms, exceptions, and case relationships in a form that a rule engine can inspect. Context-dependent or evaluative provisions require explicit uncertainty and human interpretation rather than a presumption of complete formalization.

3.3. Reasoning and Inference Module

Symbolic AI operates at this level, performing strict logical inference. The main functions are:

- Application of rules to structured data.
- Verification of the consistency of facts and norms.
- Identification of possible contradictions and logical errors.
- Preparation of substantiated conclusions for subsequent presentation to the user.

Probabilistic models could help prioritize review and estimate uncertainty. Their outputs should be calibrated and tested on relevant cases; they cannot establish the legally correct result on their own.

3.4. Explanation and Dialogue Module

An explanation and dialogue module would present the basis and limits of a recommendation to a user. Its proposed functions are:

- Conversion of logical inference into text accessible to the user.
- Conducting dialogue to clarify data and correct the conclusion.
- Ensuring transparency, allowing the judge or specialist to see every step of the reasoning.
- Creation of audit records for all system actions.

A language model could present verified information in natural language. Whether this improves understanding or trust would need to be assessed with users.

3.5. Advantages of Modular Architecture

- Transparency — record the source and reasoning steps for each recommendation.
- Flexibility — support controlled updates to data sources and rules.
- Consistency — test whether the same verified inputs and rule version produce reproducible recommendations.
- Dialogue support — let users clarify data and request explanations.
- Scalability — measure system performance under realistic case volumes.

This modular architecture is a design proposal for first-instance court assistance. Its reliability, workload effects, and suitability for a particular jurisdiction would need prototype testing.

4. International Experience

International examples illustrate different forms of court digitalization, risk assessment, and algorithmic governance. They are not a controlled comparison of the effectiveness or fairness of AI adjudication.

4.1. European Union

The European e-CODEX system supports secure cross-border judicial communication; it does not itself provide automated legal reasoning [5]. Separately, the Council of Europe's CEPEJ Ethical Charter sets out principles for responsible AI in judicial systems, including fundamental rights, quality, transparency, and user control [6]. In the architecture proposed here, AI would assist professionals while legal decisions remain subject to human authority and review.

- Transparency of algorithms.
- Explainability of decisions.
- Audit and quality control.

4.2. USA

In the United States, risk-assessment tools such as COMPAS have been used to inform criminal-justice decisions. ProPublica’s investigation raised concerns about error and racial disparity in one such tool [7]. This example cautions against treating predictive scores as objective findings or substitutes for judicial scrutiny.

4.3. United Kingdom and Canada

The United Kingdom’s Algorithmic Transparency Recording Standard provides a way for public bodies to disclose how and why they use algorithmic tools [8]. Canada’s Algorithmic Impact Assessment supports a directive covering federal administrative decisions made or assisted by automated systems [9]. These are public-sector governance examples; they do not demonstrate mandatory registries or independent audits for all judicial AI tools in either country.

4.4. China

China’s Supreme People’s Court has issued policy on the development and use of AI to support judicial work, including smart-court applications [10]. The policy describes ambitions and safeguards; it does not by itself establish measured gains in fairness or processing speed. With judges retaining responsibility for decisions, potential support functions include:

- Classifying and routing cases for administrative review where authorized.
- Assisting with drafts of routine legal text for judicial verification.
- Connecting relevant information systems and public services under appropriate safeguards.

Potential benefits include faster access to information and administrative support. Independent evidence on accuracy, transparency, and effects on parties is needed before drawing conclusions about fairness or public trust.

4.5. Estonia

Estonia provides a well-documented digital-government infrastructure, including the X-tee/X-Road data-exchange layer [11]. Its Ministry of Justice has explicitly stated that it has not developed an AI judge for small claims or general court proceedings [12]. The example therefore concerns digital infrastructure and possible administrative support, not an evaluated AI adjudication pilot.

- Secure data exchange between public information systems.
- Digital court files and procedural services, subject to applicable access rules.
- Human review and traceable use of any automated assistance.
- Ongoing assessment of accessibility, privacy, and system performance.

Estonia’s experience with public digital services can inform infrastructure design, while its official position underscores the distinction between digitizing procedures and replacing a judge.

4.6. Comparison of Estonian and Chinese Approaches

Estonia and China illustrate different digital-justice initiatives. Estonia's X-tee supports secure data exchange and its Ministry has ruled out the reported AI-judge project; China's Supreme People's Court has set out an AI policy for assistance in judicial work. These sources do not permit a quantitative comparison of efficiency, transparency, or public trust. Any lessons for Moldova should be tested against its legal framework, institutional capacity, and safeguards.

4.7. Recommendations for Countries with Limited Resources

- Phased implementation of intelligent modules: first, the automation of typical procedures, then the integration of LLM and analytical tools.
- Use of lightweight ontologies and open-source tools to reduce development costs.
- Ensuring transparency and audit to minimize corruption risks.
- Training specialists and judges to work with the intelligent system.
- Preservation of institutional accountability: AI serves as an auxiliary tool, the final decision is made by a human.

4.8. Rationale for Testing Logical Models in the Justice System of the Republic of Moldova

For the Republic of Moldova, alignment with European legal standards and limited institutional resources may make a narrow, auditable pilot more useful than a broad automation program. The case for logical models rests on three considerations:

Written law and traceable rules. Moldova's civil-law tradition places weight on statutory texts. Conditional rules can make selected legal requirements easier to inspect, but open-textured terms, disputed facts, exceptions, and legal hierarchy still require human interpretation. A Horn-clause representation cannot guarantee a unique, correct judgment.

Conflict detection during legal alignment. Formal models could flag possible inconsistencies between encoded provisions and changes made during alignment with EU law. Such flags require legal review: a logical conflict in a model may reflect incomplete encoding, different scopes, timing, or interpretive rules rather than a defect in legislation.

Accountability. Versioned rules, source links, and audit trails may help a judge and parties see the basis of a recommendation. They do not eliminate discretion or corruption risk; institutional controls, contestability, and independent evaluation remain necessary.

The role of statistical methods. Natural-language processing may assist with extracting candidate facts from unstructured records. Probabilistic models can estimate uncertainty, while SHAP and LIME are explanation techniques for model outputs rather than probabilistic models themselves. Patterns of appeal or reversal could identify questions for review, but they cannot prove that a statute or encoded rule is legally wrong.

For Moldova, a phased pilot should test whether transparent rule representations and verified text extraction improve specific assistance tasks. Evaluation should compare

accuracy, error types, time, cost, fairness, and the ability of parties to challenge outputs. Human judges remain responsible for legal conclusions.

5. Integration of Knowledge-Based Modules with Language Models

A proposed hybrid system would assign verified rule checks to symbolic components and document processing and dialogue to large language models (LLMs). The design aims to use each component for a defined task while making errors and uncertainty visible.

5.1. Principles of Hybrid Architecture

The main principles of integration primarily boil down to the separation of functions, where Symbolic Modules are responsible for strict logical inference and verification of data consistency, and LLM analyze unstructured text, perform semantic interpretation, and ensure user dialogue. This is followed by a two-stage approach "interpretation → verification", where at the first stage LLM processes documents, identifies facts, and formulates hypotheses, and at the second stage symbolic AI verifies these hypotheses against legal rules. Furthermore, a natural language interface is provided, where LLM acts as a link between the user and the logical inference module, and the user receives clear explanations, can clarify data, and correct conclusions.

5.2. Architecture of Module Interaction

The hybrid system consists of the following components:

- Fact Extraction Module, which processes judicial documents, complaints, and regulatory acts; highlights key elements (participants, events, legal categories); converts data into a structured format for logical analysis.
- Knowledge Formalization Module, which uses logical rules, ontologies, and precedent graphs; builds a formal case model for symbolic AI; ensures the uniformity of data representation.
- Reasoning and Inference Module applies formalized rules to structured data; identifies contradictions and logical errors; prepares preliminary conclusions for presentation to the user.
- Dialogue and Explanation Module converts the logical inference into natural language text; conducts a dialogue with the user, clarifying missing information; creates audit records of all system actions for verification.

The proposed interactions allow checks at each stage; whether they reduce interpretation errors must be demonstrated with representative cases.

5.3. Application at the Level of First-Instance Courts

At the level of first-instance courts, a pilot could assess whether this architecture assists with:

- Automating case preparation, including the collection and structuring of information.
- Verifying the correctness of logical inferences, ensuring decision consistency.

- Generating explainable conclusions for judges, lawyers, and parties to the case.
- Measuring whether case preparation time or costs change, without assuming that savings will follow.

5.4. Advantages and Limitations

Potential advantages include traceable rule use, auditable steps, and adaptable interfaces. These are design goals rather than observed outcomes.

The limitations are related to the complexity of formalizing all legal norms; the need for constant updating of the knowledge base and rules; requirements for the quality of initial data and the correct functioning of LLMs; the necessity of training personnel to work with the system.

5.5. Conclusions

The integration of symbolic modules with language models allows for the creation of a hybrid intelligent system capable of:

- Processing complex legal texts.
- Ensuring the transparency and explainability of decisions.
- Maintaining strict logical inference and adapting to new cases.
- Supporting the judge and other justice bodies in their daily work.

This proposed approach combines rule checks and dialogue-based processing; it requires legal validation and testing before use in decisions.

6. Potential for Further Development

Possible extensions include multimodal inputs and predictive components, but each adds data-quality, privacy, and validation demands.

6.1. Multimodal Data

A future pilot could evaluate additional forms of information, such as:

- Audio and video recordings of court hearings.
- Documents in PDF format, images, and emails.
- Data from external registries or city services where lawful, necessary, and relevant to a case.

Such inputs would require secure handling, provenance checks, and human review before they could inform a case.

6.2. Specialized Language Models

Specialized legal language models could be tested for:

- Accuracy in extracting and interpreting candidate legal text.
- Error rates when processing complex normative acts.

- Support for identifying legislative changes, subject to expert review and version control.

Specialized models might improve task-specific performance, but this requires jurisdiction-specific evaluation and ongoing updates.

6.3. Outcome Prediction and Scenario Modeling

Predictive and scenario tools might be studied for:

- Estimating possible outcomes from prior decisions, with attention to selection bias and legal change.
- Modeling alternative case scenarios under selected legal rules and assumptions.
- Presenting alternative scenarios for professional review without claiming to improve decision quality.

6.4. Intelligent Legal Assistants

Assistants for judges, lawyers, and citizens could be evaluated for:

- Drafting routine text for human verification.
- Asking users to clarify missing details.
- Suggesting potentially relevant norms and decisions with source links.
- Providing traceable supporting reasons and clear limits for each recommendation.

7. Architecture of the Future Intelligent Legal System

7.1. Construction Principles

A proposed system should be evaluated against the following design principles:

- Modularity — separate fact extraction, formalization, reasoning, and dialogue, with defined interfaces.
- Hybridity — assign defined tasks to symbolic and language-model components.
- Explainability — present traceable rule steps and clearly identify uncertain model output.
- Contextuality — account for case facts, applicable law, and the legal status of prior decisions.
- Scalability — test throughput and error rates at realistic case volumes.
- Institutional accountability — keep legal decisions under human authority, with AI as an auxiliary tool.

7.2. Multi-Level Structure

- Data and Pre-processing Level: document collection, information structuring, primary analysis.
- Knowledge Formalization Level: creation of ontologies, construction of precedent graphs and logical rules.

- Reasoning and Inference Level: application of formalized rules, identification of contradictions, generation of conclusions.
- User Interaction Level: dialogue with LLM, explanation of decisions, possibility of data clarification and conclusion correction.

An audit function should record inputs, sources, versions, corrections, and human decisions at each level.

7.3. Integration with Smart City Infrastructure

Connections to municipal or government platforms should be limited to lawful, necessary case information, with:

- Data exchange with registries and databases.
- Integration with interdepartmental interaction platforms.
- Ensuring cybersecurity and personal data protection.

7.4. Quality Control and Feedback

For reliable operation of the system, the following is necessary:

- Constant control over the correctness of logical inferences.
- Monitoring the operation of LLM, including the identification of potential errors.
- Feedback from judges and users, allowing for the improvement of models and rules.
- Maintenance of audit logs for decision verification.

7.5. Advantages and Perspectives

A pilot could test whether this architecture can:

- Improve the transparency and consistency of case preparation.
- Reduce processing time and costs for defined assistance tasks.
- Support phased adoption while preserving judicial safeguards.
- Provide a basis for connecting relevant public services where lawful.

8. Conclusion

This article has proposed a framework for structuring legal knowledge and using it in a hybrid court-assistance architecture. Its main conclusions are:

1. A hybrid approach could combine traceable rule checks with flexible text processing and dialogue. Legal accuracy and fairness would depend on verified inputs, complete safeguards, and human review.
2. A modular design separates fact extraction, knowledge representation, inference, and explanation so that each component can be tested and audited.

3. The international examples concern different activities: Estonia's digital infrastructure, China's policy for AI assistance, EU cross-border exchange, and public-sector oversight in the United Kingdom and Canada. They do not establish comparable judicial outcomes.
4. For Moldova, logical models could support selected rule checks and conflict screening, while statistical tools may help identify uncertain inputs or anomalies. Neither approach can prove that a legal decision is fair.
5. Future work could test multimodal inputs, specialized language models, outcome estimates, and assistance interfaces on representative cases.
6. Any deployed architecture should specify modular responsibilities, explainability, legal context, privacy, security, and institutional accountability.

Claims of shorter processing times, lower costs, greater consistency, or increased trust require prospective evaluation rather than inference from the architecture alone.

The proposed system is therefore a research agenda for transparent, human-supervised legal assistance in digitally connected public services.

References

- [1] N. Pelin, "Iskusstvennyi intellekt, osnovannyi na logike i pravo" [Artificial intelligence based on logic and law], in *Omul, criminologia, știința*, vol. 1, Chișinău, Moldova, 2023, pp. 562–568. [Online]. Available: https://ibn.idsi.md/sites/default/files/imag_file/562-568.pdf (in Russian).
- [2] N. Pelin, "Sistemnyi podkhod k kompiuternomu analizu informatsii o kachestve raboty pravoprimenitelia v triade 'spravedlivost-pravo-protsedura'" [A systems approach to computer analysis of legal work in the fairness–law–procedure triad], in *Tradiție și inovare în cercetarea științifică*, vol. 2, Bălți, Moldova, 2025, pp. 106–113. [Online]. Available: https://ibn.idsi.md/sites/default/files/imag_file/106-113_25.pdf (in Russian).
- [3] N. Pelin and S. Pelin, "Aspecte teoretice ale programării logice" [Theoretical aspects of logic programming], *Studia Universitatis Moldaviae, Seria Științe Exacte și Economice*, no. 3(13), pp. 72–81, 2008 (in Romanian).
- [4] N. I. Pelin, V. I. Borshevici, O. F. Prodan, et al., "Ob odnom podkhode k predstavleniiu obiedinennoi modeli ASU TP" [On an approach to representing a unified process-control model], in *Problemy sozdaniia i vnedreniia ASU TP*, Chișinău, Moldova, 1981 (in Russian).
- [5] European Commission, "Communication on Digitalisation of Justice in the European Union and Proposal for e-CODEX Regulation," 2020. [Online]. Available: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/digitalisation-justice/communication-digitalisation-justice-european-union-and-proposal-e-codex-regulation_en
- [6] European Commission for the Efficiency of Justice, *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment*. Strasbourg, France: Council of Europe, 2018. [Online]. Available: <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>
- [7] J. Angwin, J. Larson, S. Mattu, and L. Kirchner, "Machine Bias," *ProPublica*, May 23, 2016. [Online]. Available: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
- [8] Government Digital Service, "Algorithmic Transparency Recording Standard Hub," GOV.UK, 2023. [Online]. Available: <https://www.gov.uk/government/collections/algorithmic-transparency-recording-standard-hub>
- [9] Treasury Board of Canada Secretariat, "Algorithmic Impact Assessment," Government of Canada. [Online]. Available: <https://www.canada.ca/en/government/system/digital-government/digital->

government-innovations/responsible-use-ai/automated-decision-making/algorithmic-impact-assessment.html

- [10] Supreme People's Court of the People's Republic of China, "Opinions on Regulating and Strengthening the Application of Artificial Intelligence in Judicial Fields," 2022. [Online]. Available: <https://www.court.gov.cn/zixun/xiangqing/382461.html>
- [11] Estonian Information System Authority, "Data exchange layer X-tee." [Online]. Available: <https://www.ria.ee/en/state-information-system/data-exchange-platforms/data-exchange-layer-x-tee>
- [12] Ministry of Justice and Digital Affairs of Estonia, "Estonia does not develop AI Judge," 2022. [Online]. Available: <https://www.justdigi.ee/en/news/estonia-does-not-develop-ai-judge>

Structurarea și activarea cunoștințelor pentru sisteme juridice inteligente în orașe inteligente: către o justiție transparentă și echitabilă

Nicolae Pelin

Academia de Studii Economice din Moldova, Chișinău

nicolae.ion.pelin@gmail.com

Rezumat

Lucrarea propune o arhitectură conceptuală pentru structurarea și activarea cunoștințelor juridice în sisteme inteligente care ar putea sprijini instanțele de fond și serviciile publice digitale. Întrebarea centrală este cum pot fi combinate regulile formale și ontologiile cu modelele lingvistice mari, păstrând responsabilitatea umană pentru interpretarea dreptului și luarea deciziilor. Analiza se bazează pe lucrările anterioare ale autorului în programarea logică, pe literatura selectată privind IA juridică și pe inițiative documentate de digitalizare a justiției din Europa, SUA și China. Dialogurile exploratorii cu modele lingvistice au contribuit la formularea arhitecturii, însă lucrarea nu prezintă un prototip funcțional, un test comparativ de performanță ori efecte măsurate asupra hotărârilor judecătorești. Arhitectura are patru funcții corelate: extragerea faptelor din documente; reprezentarea normelor aplicabile, a excepțiilor și a relațiilor dintre cazuri; verificarea inferențelor în raport cu aceste reprezentări; și prezentarea motivelor, incertitudinilor și a unui jurnal de audit unui utilizator uman. Modelele lingvistice ar putea prelucra texte nestructurate și sprijini dialogul, iar componentele bazate pe reguli ar putea face trasabili anumiți pași ai raționamentului. Comparăția internațională distinge schimbul transfrontalier de informații și supravegherea algoritmică din sectorul public de judecata automatizată propriu-zisă. Estonia oferă un exemplu de infrastructură digitală, dar Ministerul Justiției a declarat că nu a dezvoltat un judecător IA pentru litigiile cu valoare redusă. Pentru Republica Moldova, lucrarea recomandă evaluarea etapizată a unor sarcini de asistență precis delimitate, începând cu reguli transparente, extragerea verificată a datelor, control judiciar și actualizarea periodică a bazei de cunoștințe. Normele cu termeni evaluativi, faptele contestate, prejudecățile algoritmice, confidențialitatea și erorile modelelor lingvistice limitează ceea ce poate demonstra formalizarea. Posibilele câștiguri de coerență, timp, cost și încredere publică rămân ipoteze ce necesită testare pe cazuri și evaluare independentă înainte de implementare.

Cuvinte-cheie: modele logice; drept computațional; responsabilitate judiciară; raționament hibrid; explicabilitatea IA

1. Introducere

Inteligența artificială (IA) poate sprijini cercetarea juridică și administrarea instanțelor, dar utilizarea ei în activitatea judiciară ridică probleme de transparență, consecvență și echitate. Lucrarea propune o arhitectură hibridă de asistență, nu o judecată automatizată. Cercetările anterioare ale autorului au abordat IA bazată pe logică în drept [1] și relația dintre echitate, lege și procedură [2]. Reprezentările simbolice, inclusiv regulile și ontologiile, pot fi combinate cu modele lingvistice pentru prelucrarea textului, sub rezerva verificării și a controlului uman.

Clauzele Horn oferă o modalitate de reprezentare a regulilor condiționale; lucrarea autorului despre programarea logică oferă un punct de plecare pentru această abordare [3]. Un rezumat de conferință din 1981 a propus prelucrarea comună a informațiilor deterministe, fuzzy și probabilistice în controlul proceselor industriale [4]. Relevanța sa pentru justiție este o analogie, nu o dovadă de performanță judiciară.

Dialogul poate ajuta la identificarea faptelor lipsă și la explicarea unei concluzii propuse. Schimburile exploratorii cu Gemini, ChatGPT și Grok au contribuit la proiectarea conceptuală, dar lucrarea nu prezintă un prototip sau o evaluare controlată.

2. Structurarea Cunoștințelor în Sfera Juridică

Un asistent juridic inteligent necesită reprezentarea explicită a normelor și faptelor relevante, urmată de utilizarea controlată a acestei reprezentări. Elementele candidate includ:

- Ierarhia izvoarelor de drept, inclusiv constituția, codurile și celelalte acte aplicabile.
- Relațiile dintre norme, inclusiv excepțiile și valabilitatea lor în timp.
- Categoriile deontice precum obligația, interdicția și permisiunea.
- Distincția epistemică dintre fapte stabilite, susțineri și probe incerte.

2.1. Formalizarea Logică a Dreptului

Clauzele Horn pot codifica anumite dispoziții juridice ca reguli condiționale: dacă sunt stabilite condițiile specificate, în model urmează consecința prevăzută. Beneficiile potențiale includ:

- Pași de inferență trasabili pentru reguli codificate corect.
- Rezultate reproductibile pentru aceleași date verificate și aceeași versiune a regulilor.
- Legături structurate cu decizii anterioare relevante, atunci când statutul lor juridic este clar.

Aceste beneficii depind de extragerea corectă a faptelor, codificarea validă și tratarea excepțiilor. Ontologiile pot lega participanți, evenimente, acte juridice și date, iar grafurile de cunoștințe pot reprezenta asemenea relații fără a înlocui interpretarea judiciară.

2.2. Activarea Cunoștințelor prin Dialog

Un flux de dialog propus ar avea trei etape:

- Identificarea faptelor și a participanților din documente, cu verificarea umană a datelor extrase.
- Adresarea unor întrebări punctuale privind informațiile lipsă sau contestate.
- Transformarea textului verificat într-o reprezentare structurată a cauzei, pentru verificarea regulilor.

Interfața ar trebui să arate sursa și statutul fiecărui fapt, versiunea regulii aplicabile și limitele oricărei inferențe.

2.3. Problemele Formalizării și Limitări

Formalizarea și prelucrarea prin modele lingvistice au limite importante:

- Noțiunile juridice evaluative și faptele contestate pot rezista unei codificări precise.

- Modelele lingvistice pot interpreta greșit documente sau pot genera conținut inventat, necesitând verificare independentă.
- Modificările legislative și jurisprudențiale necesită actualizări versionate și revizuire.

O proiectare hibridă poate combina instrumente diferite, dar nici rezultatul fuzzy, nici cel probabilistic nu stabilesc singure corectitudinea juridică a unei concluzii.

3. Modulele Inteligente în Sistemul Juridic

Asistentul juridic propus are module distincte pentru extragerea faptelor, reprezentarea cunoștințelor, inferență și explicație. Separarea lor ar putea sprijini mentenanța și auditarea, dacă sunt definite interfețele, proveniența datelor și responsabilitățile umane.

3.1. Modulul de Extracție a Faptelor

Acest modul este conceput pentru colectarea și structurarea primară a informațiilor. Sursele de date pot include:

- Documente judiciare, plângeri și cereri.
- Registre electronice, baze de date normative.
- Decizii anterioare ale instanțelor, cu precizarea statutului lor juridic.

Modulul ar putea face o analiză preliminară a textului, identificând evenimente, participanți și categorii juridice. Datele extrase trebuie verificate înainte de transformarea lor într-o reprezentare structurată, de exemplu un graf al relațiilor dintre participanți, obiecte, acțiuni și consecințe juridice.

3.2. Modulul de Formalizare a Cunoștințelor

Baza de cunoștințe formalizată este nucleul sistemului. Acest modul include:

- Reguli logice care descriu anumite norme de drept sub formă de clauze Horn.
- Ontologii care leagă conceptele juridice, participanții și acțiunile.
- Grafuri ale deciziilor anterioare, utilizate în limitele statutului lor juridic.

Acest modul ar reprezenta normele aplicabile, excepțiile și relațiile dintre cauze într-o formă examinabilă de un motor de reguli. Dispozițiile dependente de context sau evaluare impun exprimarea incertitudinii și interpretare umană, nu prezumția unei formalizări complete.

3.3. Modulul de Raționament și Inferență

La acest nivel funcționează IA simbolică, efectuând inferențe logice riguroase. Funcțiile principale sunt:

- Aplicarea regulilor la datele structurate.
- Verificarea coerenței faptelor și normelor.
- Identificarea posibilelor contradicții și erori logice.
- Pregătirea concluziilor fundamentate pentru prezentarea ulterioară utilizatorului.

Modelele probabilistice ar putea ajuta la prioritizarea revizuirii și estimarea incertitudinii. Rezultatele lor trebuie calibrate și testate pe cauze relevante; ele nu pot stabili singure soluția corectă din punct de vedere juridic.

3.4. Modulul de Explicație și Dialog

Un modul de explicație și dialog ar prezenta utilizatorului temeiul și limitele unei recomandări. Funcțiile propuse sunt:

- Transformarea inferenței logice într-un text accesibil utilizatorului.
- Desfășurarea dialogului pentru clarificarea datelor și corectarea concluziei.
- Asigurarea transparenței, permițând judecătorului sau specialistului să vadă fiecare pas al raționamentului.
- Crearea de înregistrări de audit pentru toate acțiunile sistemului.

Un model lingvistic ar putea prezenta informațiile verificate în limbaj natural. Dacă această funcție sporește înțelegerea sau încrederea trebuie evaluat împreună cu utilizatorii.

3.5. Avantajele Arhitecturii Modulare

- Transparență — înregistrarea sursei și a pașilor de raționament pentru fiecare recomandare.
- Flexibilitate — actualizarea controlată a surselor de date și a regulilor.
- Consecvență — testarea reproductibilității recomandărilor pentru aceleași date verificate și aceeași versiune a regulilor.
- Suport prin dialog — posibilitatea de a clarifica datele și de a solicita explicații.
- Scalabilitate — măsurarea performanței la volume realiste de cauze.

Această arhitectură modulară este o propunere pentru asistența instanțelor de fond. Fiabilitatea, efectele asupra volumului de muncă și adecvarea la o anumită jurisdicție necesită testarea unui prototip.

4. Experiența Internațională

Exemplele internaționale ilustrează forme diferite de digitalizare a justiției, evaluare a riscului și guvernanta algoritmică. Ele nu constituie o comparație controlată a eficienței sau echității judecății automatizate.

4.1. Uniunea Europeană

Sistemul european e-CODEX sprijină comunicarea judiciară transfrontalieră securizată; el nu oferă în sine raționament juridic automat [5]. Separat, Carta etică a CEPEJ a Consiliului Europei stabilește principii pentru utilizarea responsabilă a IA în sistemele judiciare, inclusiv drepturile fundamentale, calitatea, transparența și controlul utilizatorului [6]. În arhitectura propusă aici, IA ar asista profesioniștii, iar deciziile juridice ar rămâne sub autoritate și control uman.

- Transparența algoritmilor.

- Explicabilitatea deciziilor.
- Auditul și controlul calității.

4.2. SUA

În Statele Unite, instrumente de evaluare a riscului precum COMPAS au fost utilizate pentru a informa decizii în justiția penală. Investigația ProPublica a ridicat probleme privind erorile și disparitățile rasiale ale unui asemenea instrument [7]. Exemplul avertizează împotriva tratării scorurilor predictive ca fapte obiective sau ca substitut al examinării judiciare.

4.3. Marea Britanie și Canada

Standardul britanic Algorithmic Transparency Recording Standard oferă instituțiilor publice o modalitate de a declara cum și de ce folosesc instrumente algoritmice [8]. În Canada, Algorithmic Impact Assessment sprijină o directivă aplicabilă deciziilor administrative federale luate ori asistate de sisteme automatizate [9]. Acestea sunt exemple de guvernare a sectorului public; nu demonstrează existența unor registre obligatorii sau audituri independente pentru toate instrumentele IA judiciare din cele două țări.

4.4. China

Curtea Supremă a Poporului din China a emis o politică privind dezvoltarea și utilizarea IA pentru sprijinirea activității judiciare, inclusiv aplicații ale instanțelor inteligente [10]. Documentul descrie obiective și garanții, dar nu demonstrează prin el însuși câștiguri măsurate de echitate sau viteză. Cu păstrarea responsabilității judecătorilor pentru decizii, funcțiile de sprijin posibile includ:

- Clasificarea și repartizarea cauzelor pentru revizuire administrativă, acolo unde este autorizată.
- Asistență la redactarea unor texte juridice de rutină, pentru verificare judiciară.
- Conectarea sistemelor informaționale și a serviciilor publice relevante, cu garanții adecvate.

Beneficiile potențiale includ acces mai rapid la informații și sprijin administrativ. Sunt necesare dovezi independente privind precizia, transparența și efectele asupra părților înainte de a trage concluzii despre echitate sau încrederea publică.

4.5. Estonia

Estonia oferă un exemplu de infrastructură digitală de stat bine documentată, inclusiv platforma de schimb de date X-tee/X-Road [11]. Ministerul Justiției a declarat explicit că nu a dezvoltat un judecător IA pentru litigii cu valoare redusă sau pentru procedurile judiciare generale [12]. Exemplul privește infrastructura digitală și posibila asistență administrativă, nu un proiect-pilot evaluat de judecată automatizată.

- Schimb securizat de date între sistemele informaționale publice.
- Dosare judiciare și servicii procedurale digitale, sub rezerva regulilor de acces aplicabile.

- Control uman și utilizare trasabilă a oricărei asistențe automatizate.
- Evaluarea continuă a accesibilității, confidențialității și performanței sistemului.

Experiența Estoniei cu serviciile publice digitale poate informa proiectarea infrastructurii, iar poziția oficială a ministerului subliniază diferența dintre digitalizarea procedurilor și înlocuirea unui judecător.

4.6. Comparația Abordărilor Estoniei și Chinei

Estonia și China ilustrează inițiative diferite de digitalizare a justiției. X-tee din Estonia sprijină schimbul securizat de date, iar Ministerul Justiției a infirmat proiectul de «judecător IA» relatat în presă; Curtea Supremă a Poporului din China a stabilit o politică pentru asistența IA în activitatea judiciară. Aceste surse nu permit o comparație cantitativă a eficienței, transparenței sau încrederii publice. Lecțiile posibile pentru Moldova trebuie testate în raport cu cadrul său juridic, capacitatea instituțională și garanțiile necesare.

4.7. Recomandări pentru țările cu resurse limitate

- Implementarea etapizată a modulelor, începând cu sarcini administrative bine delimitate și testate înaintea integrării LLM.
- Evaluarea ontologiilor simple și a instrumentelor cu sursă deschisă în raport cu costurile și cerințele de mentenanță.
- Asigurarea transparenței și a auditului, alături de controale instituționale împotriva abuzurilor.
- Instruirea specialiștilor și a judecătorilor pentru lucrul cu sistemul inteligent.
- Păstrarea responsabilității instituționale: IA servește ca instrument auxiliar, decizia finală este luată de om.

4.8. Motive pentru testarea modelelor logice în justiția Republicii Moldova

Pentru Republica Moldova, apropierea de standardele juridice europene și resursele instituționale limitate ar putea face mai util un proiect-pilot restrâns și auditabil decât un program amplu de automatizare. Argumentul pentru modelele logice are trei componente:

Dreptul scris și regulile trasabile. Tradiția juridică continentală a Republicii Moldova pune accent pe textele legislative. Regulile condiționale pot facilita verificarea unor cerințe juridice, însă termenii evaluativi, faptele contestate, excepțiile și ierarhia normelor necesită în continuare interpretare umană. O reprezentare prin clauze Horn nu poate garanta o hotărâre unică și corectă.

Depistarea conflictelor în procesul de aliniere juridică. Modelele formale ar putea semnala posibile neconcordanțe între dispozițiile codificate și modificările adoptate în procesul alinierii la dreptul UE. Semnalele necesită analiză juridică: un conflict logic din model poate proveni dintr-o codificare incompletă, domenii de aplicare diferite, momente diferite sau reguli de interpretare, nu neapărat dintr-un defect al legislației.

Responsabilitatea instituțională. Regulile versionate, legăturile către surse și jurnalele de audit ar putea ajuta judecătorul și părțile să examineze temeiul unei recomandări. Ele nu

elimină discreția ori riscul de corupție; rămân necesare controale instituționale, posibilitatea contestării și evaluarea independentă.

Rolul metodelor statistice. Prelucrarea limbajului natural poate ajuta la extragerea unor fapte candidate din documente nestructurate. Modelele probabilistice pot estima incertitudinea, în timp ce SHAP și LIME sunt tehnici de explicare a rezultatelor modelelor, nu modele probabilistice în sine. Tiparele de apel sau de casare pot indica probleme de examinat, dar nu dovedesc că o lege ori o regulă codificată este greșită din punct de vedere juridic.

Pentru Moldova, un proiect-pilot etapizat ar trebui să testeze dacă reprezentările transparente ale regulilor și extragerea verificată a textului îmbunătățesc anumite sarcini de asistență. Evaluarea trebuie să compare precizia, tipurile de erori, timpul, costul, echitatea și posibilitatea părților de a contesta rezultatele. Judecătorii rămân responsabili pentru concluziile juridice.

5. Integrarea Modulelor Bazate pe Cunoștințe cu Modelele Lingvistice

Sistemul hibrid propus ar alocă verificările bazate pe reguli componentelor simbolice, iar prelucrarea documentelor și dialogul modelelor lingvistice mari (LLM). Proiectarea urmărește definirea unei sarcini pentru fiecare componentă și evidențierea erorilor și incertitudinilor.

5.1. Principiile Arhitecturii Hibride

Integrarea ar separa funcțiile: modulele simbolice ar verifica reguli și coerența datelor, iar modelele lingvistice ar prelucra textul nestructurat și ar sprijini dialogul. Un flux în două etape, «interpretare → verificare», ar identifica fapte candidate și ipoteze, apoi le-ar confrunța cu reguli codificate. Interfața ar oferi utilizatorului acces la surse, explicații și posibilitatea de a corecta datele. Verificarea regulilor nu ar substitui analiza juridică a unor fapte ori norme contestate.

5.2. Arhitectura de Interacțiune a Modulelor

Sistemul hibrid constă din următoarele componente:

- Modulul de Extracție a Faptelor care prelucrează documentele judiciare, plângerile și actele normative; evidențiază elementele cheie (participanți, evenimente, categorii juridice); transformă datele într-o formă structurată pentru analiza logică.
- Modulul de Formalizare a Cunoștințelor care utilizează reguli logice, ontologii și grafuri de precedente; construiește un model formal al cazului pentru IA simbolică; asigură uniformitatea reprezentării datelor.
- Modulul de Raționament și Inferență aplică regulile formalizate la datele structurate; identifică contradicțiile și erorile logice; pregătește concluziile preliminare pentru prezentarea utilizatorului.
- Modulul de Dialog și Explicație transformă inferența logică în text în limbaj natural; poartă dialogul cu utilizatorul, clarificând informațiile lipsă; creează înregistrări de audit ale tuturor acțiunilor sistemului pentru verificare.

Interacțiunile propuse permit verificări la fiecare etapă; dacă reduc erorile de interpretare trebuie demonstrat pe cauze reprezentative.

5.3. Aplicarea în instanțele de fond

La nivelul instanțelor de fond, un proiect-pilot ar putea evalua dacă arhitectura sprijină:

- Automatizarea pregătirii cazurilor, inclusiv colectarea și structurarea informațiilor.
- Verificarea corectitudinii inferențelor logice, asigurând coerența deciziilor.
- Generarea de concluzii explicabile pentru judecători, avocați și părțile în cauză.
- Măsurarea schimbărilor în timpul și costul pregătirii cauzelor, fără a presupune că vor apărea economii.

5.4. Avantaje și Limitări

Avantajele potențiale includ utilizarea trasabilă a regulilor, pași auditabili și interfețe adaptabile. Acestea sunt obiective de proiectare, nu rezultate observate.

Limitările sunt legate de complexitatea formalizării tuturor normelor de drept; necesitatea actualizării constante a bazei de cunoștințe și a regulilor; cerințele privind calitatea datelor inițiale și corectitudinea funcționării LLM; necesitatea instruirii personalului pentru lucrul cu sistemul.

5.5. Concluzii

Funcțiile unui sistem hibrid propus ar fi:

- Prelucrarea textelor juridice complexe, cu verificarea datelor extrase.
- Prezentarea motivelor și limitelor recomandărilor.
- Verificarea inferențelor în raport cu reguli formalizate și versiuni documentate.
- Sprijinirea activității profesioniștilor fără transferarea responsabilității deciziei către sistem.

Aceste funcții necesită validare juridică și testare înaintea utilizării în decizii.

6. Potențialul de Dezvoltare Ulterioară

Extensiile posibile includ date multimodale și componente predictive, dar fiecare adaugă cerințe de calitate a datelor, confidențialitate și validare.

6.1. Date Multimodale

Un proiect-pilot viitor ar putea evalua și alte forme de informație, precum:

- Înregistrări audio și video ale ședințelor de judecată.
- Documente în format PDF, imagini și e-mailuri.
- Date din registre externe sau servicii urbane, când accesul este legal, necesar și relevant pentru o cauză.

Aceste intrări ar necesita prelucrare securizată, verificarea provenienței și control uman înainte de a putea informa o cauză.

6.2. Modele Lingvistice Specializate

Modelele lingvistice juridice specializate ar putea fi testate pentru:

- Precizia extragerii și interpretării fragmentelor juridice relevante.
- Rata erorilor la prelucrarea actelor normative complexe.
- Identificarea modificărilor legislative, sub rezerva controlului experților și a versiunilor documentate.

Modelele specializate ar putea îmbunătăți performanța unor sarcini, dar această ipoteză necesită evaluare în jurisdicția vizată și actualizări permanente.

6.3. Prognozarea Rezultatelor și Modelarea Scenariilor

Instrumentele predictive și de modelare a scenariilor ar putea fi studiate pentru:

- Estimarea unor rezultate posibile din hotărâri anterioare, ținând cont de selecția datelor și schimbările legislative.
- Modelarea unor scenarii alternative ale cauzei pe baza unor norme și ipoteze alese.
- Prezentarea scenariilor pentru examinare profesională, fără a pretinde că îmbunătățesc calitatea deciziei.

6.4. Asistenți Juridici Inteligenți

Asistenții pentru judecători, avocați și cetățeni ar putea fi evaluați pentru:

- Redactarea unor texte de rutină pentru verificare umană.
- Solicitarea clarificării detaliilor lipsă.
- Sugerarea unor norme și decizii potențial relevante, cu trimiteri la surse.
- Furnizarea unor argumente de sprijin trasabile și a limitelor clare pentru fiecare recomandare.

7. Arhitectura unui viitor sistem juridic inteligent

7.1. Principii de Construcție

Un sistem propus ar trebui evaluat în raport cu următoarele principii de proiectare:

- Modularitate — separarea extragerii faptelor, formalizării, raționamentului și dialogului, cu interfețe definite.
- Hibriditate — atribuirea unor sarcini definite componentelor simbolice și lingvistice.
- Explicabilitate — prezentarea pașilor trasabili ai regulilor și identificarea clară a incertitudinii generate de modele.
- Contextualitate — luarea în considerare a faptelor cauzei, a dreptului aplicabil și a statutului juridic al deciziilor anterioare.

- Scalabilitate — testarea capacității de prelucrare și a ratelor de eroare la volume realiste.
- Responsabilitate instituțională — păstrarea deciziilor juridice sub autoritate umană, cu IA ca instrument auxiliar.

7.2. Structură pe Mai Multe Niveluri

- Nivelul de Date și Prelucrare Preliminară: colectarea documentelor, structurarea informațiilor, analiza primară.
- Nivelul de Formalizare a Cunoștințelor: crearea ontologiilor, construirea grafurilor de precedente și a regulilor logice.
- Nivelul de Raționament și Inferență: aplicarea regulilor formalizate, identificarea contradicțiilor, generarea concluziilor.
- Nivelul de Interacțiune cu Utilizatorul: dialog cu LLM, explicarea deciziilor, posibilitatea de clarificare a datelor și corectare a concluziilor.

O funcție de audit ar trebui să înregistreze intrările, sursele, versiunile, corecțiile și deciziile umane la fiecare nivel.

7.3. Integrarea cu Infrastructura Orașului Inteligent

Conexiunile cu platformele municipale sau guvernamentale ar trebui limitate la datele necesare unei cauze, la care accesul este permis de lege, și ar presupune:

- Schimb de date cu registrele și bazele de date.
- Integrare cu platformele de interacțiune interdepartamentală.
- Asigurarea securității cibernetice și protecției datelor cu caracter personal.

7.4. Controlul Calității și Feedback-ul

Pentru funcționarea fiabilă a sistemului este necesar:

- Controlul constant al corectitudinii inferențelor logice.
- Monitorizarea funcționării LLM, inclusiv identificarea erorilor potențiale.
- Feedback de la judecători și utilizatori, permițând îmbunătățirea modelelor și regulilor.
- Ținerea jurnalelor de audit pentru verificarea deciziilor.

7.5. Avantaje și Perspective

Un proiect-pilot ar putea testa dacă această arhitectură poate:

- Îmbunătăți transparența și consecvența pregătirii cauzelor.
- Reduce timpul și costurile pentru sarcini de asistență definite.
- Sprijini adoptarea etapizată, cu păstrarea garanțiilor judiciare.
- Oferi o bază pentru conectarea serviciilor publice relevante, acolo unde legea permite.

8. Concluzie

Articolul a propus un cadru pentru structurarea cunoștințelor juridice și utilizarea lor într-o arhitectură hibridă de asistență judiciară. Concluziile principale sunt:

1. O abordare hibridă ar putea combina verificări trasabile ale regulilor cu prelucrarea flexibilă a textului și dialogul. Precizia juridică și echitatea ar depinde de date verificate, garanții adecvate și control uman.
2. O proiectare modulară separă extragerea faptelor, reprezentarea cunoștințelor, inferența și explicația, astfel încât fiecare componentă să poată fi testată și auditată.
3. Exemplele internaționale privesc activități diferite: infrastructura digitală a Estoniei, politica Chinei pentru asistență IA, schimbul transfrontalier al UE și supravegherea algoritmică din sectorul public britanic și canadian. Ele nu stabilesc rezultate judiciare comparabile.
4. Pentru Moldova, modelele logice ar putea sprijini verificări selectate ale regulilor și semnalarea unor posibile conflicte, în timp ce instrumentele statistice pot ajuta la identificarea datelor incerte ori a anomaliilor. Niciuna dintre abordări nu dovedește că o decizie juridică este echitabilă.
5. Cercetările viitoare ar putea testa date multimodale, modele lingvistice specializate, estimări ale rezultatelor și interfețe de asistență pe cauze reprezentative.
6. Orice arhitectură implementată ar trebui să definească responsabilități modulare, explicabilitate, context juridic, confidențialitate, securitate și responsabilitate instituțională.

Afirmările privind reducerea duratei și costurilor, creșterea consecvenței sau a încrederii necesită evaluare prospectivă; ele nu decurg din simpla descriere a arhitecturii.

Sistemul propus constituie, așadar, o agendă de cercetare pentru asistență juridică transparentă, sub supraveghere umană, în servicii publice conectate digital.

Referințe

- [1] N. Pelin, “Iskusstvennyi intellekt, osnovannyi na logike i pravo” [Inteligența artificială bazată pe logică și drept], în Omul, criminologia, știința, vol. 1, Chișinău, 2023, pp. 562–568. [Online]. Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/562-568.pdf (în limba rusă).
- [2] N. Pelin, “Sistemnyi podkhod k kompiuternomu analizu informatsii o kachestve raboty pravoprimeritelia v triade ‘spravedlivost–pravo–protsedura’” [Abordare sistemică a analizei informatice a activității juridice în triada echitate–lege–procedură], în Tradiție și inovare în cercetarea științifică, vol. 2, Bălți, 2025, pp. 106–113. [Online]. Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/106-113_25.pdf (în limba rusă).
- [3] N. Pelin și S. Pelin, “Aspecte teoretice ale programării logice,” Studia Universitatis Moldaviae, Seria Științe Exacte și Economice, nr. 3(13), pp. 72–81, 2008.
- [4] N. I. Pelin, V. I. Borshevici, O. F. Prodan ș.a., “Ob odnom podkhode k predstavleniiu obiedinennoi modeli ASU TP” [Despre o abordare a reprezentării unui model unificat de control al proceselor], în Problemy sozdaniia i vnedreniia ASU TP, Chișinău, 1981 (în limba rusă).
- [5] Comisia Europeană, “Communication on Digitalisation of Justice in the European Union and Proposal for e-CODEX Regulation,” 2020. [Online]. Disponibil: <https://commission.europa.eu/strategy-and->

policy/policies/justice-and-fundamental-rights/digitalisation-justice/communication-digitalisation-justice-european-union-and-proposal-e-codex-regulation_en

- [6] Comisia Europeană pentru Eficiența Justiției, European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment. Strasbourg: Consiliul Europei, 2018. [Online]. Disponibil: <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment>
- [7] J. Angwin, J. Larson, S. Mattu și L. Kirchner, "Machine Bias," ProPublica, 23 mai 2016. [Online]. Disponibil: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
- [8] Government Digital Service, "Algorithmic Transparency Recording Standard Hub," GOV.UK, 2023. [Online]. Disponibil: <https://www.gov.uk/government/collections/algorithmic-transparency-recording-standard-hub>
- [9] Treasury Board of Canada Secretariat, "Algorithmic Impact Assessment," Guvernul Canadei. [Online]. Disponibil: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/automated-decision-making/algorithmic-impact-assessment.html>
- [10] Curtea Supremă a Poporului din Republica Populară Chineză, "Opinions on Regulating and Strengthening the Application of Artificial Intelligence in Judicial Fields," 2022. [Online]. Disponibil: <https://www.court.gov.cn/zixun/xiangqing/382461.html>
- [11] Estonian Information System Authority, "Data exchange layer X-tee." [Online]. Disponibil: <https://www.ria.ee/en/state-information-system/data-exchange-platforms/data-exchange-layer-x-tee>
- [12] Ministerul Justiției și Afacerilor Digitale din Estonia, "Estonia does not develop AI Judge," 2022. [Online]. Disponibil: <https://www.justdigi.ee/en/news/estonia-does-not-develop-ai-judge>

AI-driven disinformation and IoT weaknesses: operational cyber management, legal compliance and resilience strategies

Sebastian Avăcăriței,
University Alexandru Ioan Cuza of Iasi
sebastian.avacaritei24.07@gmail.com

Mihaela Tofan
University Alexandru Ioan Cuza of Iasi
Institute of Legal Research, Romanian Academy
mtofan@uaic.ro

Abstract

This presentation examines the intersection between AI-driven disinformation campaigns and cyber vulnerabilities in IoT-enabled environments and proposes an integrated operational and regulatory framework for resilient legal protection. Recent EU instruments impose stronger obligations on organisational prudent conduct and on delivery of goods and services that create systemic digital risk: the NIS2 framework raises management accountability and requires formalised cyber risk assessments and governance. The Digital Operational Resilience Act mandates ICT risk-management and resilience testing for financial actors. At the same time, the Cyber Resilience Act sets horizontal security requirements for products with digital elements, including IoT devices. Simultaneously, the Digital Services Act increases platform responsibilities to mitigate systemic risks such as misinformation. Against this regulatory backdrop, the doctrine analyses three vectors by which automated content generation, adversarial machine-learning techniques and compromised IoT endpoints are combined to magnify information sabotage and data exfiltration. Using two short case studies that illustrate (i) coordinated deepfake-driven manipulation amplified via compromised IoT endpoints, and (ii) supply-chain exploitation of edge devices to bypass detection, our research illustrates and assesses gaps in current operational practices and regulatory implementation. We conclude by proposing an actionable set of governance measures, including elevating cybersecurity to board-level oversight, designating and empowering a CISO function with clear reporting duties, integrating adversarial testing into security assurance for AI systems and IoT products, and harmonising incident reporting and platform mitigation playbooks with legal obligations. This approach aims to bridge technical controls, organisational accountability and regulatory compliance to reduce the tactical effectiveness of information sabotage, while preserving legitimate digital services. References to recent EU regulatory developments and implementation guidance will be provided during the paper presentation.

Keywords: Ai-driven disinformation, deepfakes, IoT security, cyber-resilience, digital supply-chain risk, data exfiltration.

1. Introduction

The issue of AI-generated disinformation can no longer be framed, in 2026, solely in the classical terms of freedom of expression or informational accuracy. The problem is equally one of technical infrastructure, the machinery that enables the fabrication, amplification and distribution of manipulative content: generative models, online platforms, social networks, connected devices, sensors, cameras, digital assistants, connected software products and third-party infrastructure providers. In this equation, “disinformation” is not merely a discursive product but also the outcome of a vulnerable technical architecture. This precise intersection is highlighted by the abstract provided, which proposes an integrated approach combining operational management, legal compliance and resilience strategies.

The working hypothesis of this study is that current administrative law must be read functionally, not sectorally. In other words, it is not sufficient to note that NIS2 regulates network security, that the DSA (Digital Services Act) addresses online intermediation, that DORA (Digital Operational Resilience Act) targets the financial sector, that the CRA (Cyber Resilience Act) covers products with digital elements, and that the AI Act introduces transparency requirements for synthetic content. The scientific relevance lies precisely in the way these instruments form a regulatory network designed to respond to a convergent risk: the convincing falsehood, its viral circulation and its technical vulnerability. [1]

On a theoretical level, AI-generated disinformation raises three specific problems. The first concerns factual truth and the criterion of manifest inaccuracy: how easily can synthetic content that mimics a statement, an image or an identity be challenged and removed. The second concerns the liability of platforms and intermediaries, especially where content is not necessarily illegal yet causes social harm. The third concerns the source of infrastructure risk, since many manipulation campaigns and many exfiltration or compromise operations exploit poorly secured digital products, IoT devices, peripheral endpoints or unaudited supply chains. Recent literature underscores precisely this shift in emphasis from simple “content moderation” to an integrated governance of digital risks. Chesney and Citron (2019) were early in demonstrating that deepfakes produce effects on privacy, security and democracy; Vandezande (2024) showed that NIS2 transforms cybersecurity into a governance and supply-chain security obligation; Buttigieg and Brunelli Zimmermann (2024) discussed the centrality of convergent oversight in DORA; Fathaigh (2025) demonstrated that the DSA regulates disinformation primarily through the paradigm of systemic risk rather than through a general prohibition of falsehood; and Łabuz (2024) and Romero-Moreno (2024; 2025) highlighted both the potential and the limits of the AI Act with respect to deepfakes and the protection of fundamental rights. [2]

On a normative level, the choice to focus the analysis on Romania is justified by two reasons. First, because Romanian administrative law offers very fertile ground for analysing the transposition and application of European norms: Law no. 50/2024 created the national enforcement mechanism for the DSA and designated ANCOM (the National Authority for Management and Regulation in Communications) as the digital services coordinator, while Government Emergency Ordinance (GEO) no. 155/2024, approved by Law no. 124/2025, fundamentally reconfigured domestic cybersecurity law. Second, empirical data reveal a significant Romanian paradox: high internet penetration, digital consumption and social use of connected devices, yet a low uptake of digital public services and still numerous institutional and operational vulnerabilities. This gap lends particular value to the administrative question: how does one legally and managerially organise resilience in a society that is digitalising faster than it is being governed? [3]

The key terms also require a conceptual clarification. “Disinformation” does not always coincide with “illegal content”. Some false or misleading content may fall within the scope of rules on fraud, defamation, identity theft, incitement speech or data protection; another part, however, remains in the realm of harmful content without being automatically

unlawful. It is precisely for this reason that the DSA addresses the problem largely through transparency, risk assessment, complaint mechanisms and procedural obligations, rather than solely through content suppression. Correspondingly, the AI Act does not promise the “truth” of synthetic content, but rather imposes transparency primarily regarding interaction with AI and the labelling of certain generated or manipulated content. It follows that contemporary digital administrative law is, to a large extent, a law of risk procedures and organisational responsibilities. [4]

For public administration, this shift is decisive. ENISA (the European Union Agency for Cybersecurity) indicates that the public administration sector is newly covered by NIS2, is still in early stages of alignment and exhibits only a moderate level of maturity, while simultaneously being one of the sectors most exposed to cyber incidents. In other words, digital administration simultaneously becomes a service provider and an object of legal protection. When a public service depends on information systems, databases, connected digital products and external communication platforms, disinformation and technical weakness are no longer mere “collateral events” but threats to good administration, service continuity, data security and the legitimate trust of those administered. [5]

Within this framework, the article seeks to answer four fundamental questions. The first: what is the relevant normative architecture, at European and Romanian level, for the combined treatment of AI disinformation and IoT vulnerabilities? The second: what do official data reveal about objective exposure and institutional response capacity? The third: what principles can be drawn from European case law on intermediary liability, the correction of inaccurate information and the proportionality of measures? The fourth: what governance model must be proposed, in concrete administrative terms, to prevent legal obligations from remaining purely formal? The answer I advance is that the only coherent model is one of integrated compliance, based on the triad “leadership – infrastructure – procedure”, rather than on fragmented interventions. [6]

2. Methodology

The research employs a legal-doctrinal methodology, supplemented by comparative analysis, public policy analysis and a contextual reading of official statistical data. In legal terms, the hierarchy of sources was established as follows: first, primary and secondary legislation of the European Union and Romania, official administrative reports and documents, European case law and statistical data published by authorities; second, peer-reviewed scientific literature and relevant Romanian legal doctrine; third, doctrinal or institutional explanatory materials used exclusively for the clarification of metadata and context. This hierarchy is consistent both with the requirements of legal research and with the nature of the subject, in which the validity of conclusions depends decisively on normative precision and administrative competence. [7]

From the perspective of the normative corpus, the principal analysis was built on the basis of the NIS2 Directive, the DORA Regulation, the Digital Services Act, the Cyber Resilience Act, the AI Act, the GDPR (General Data Protection Regulation), GEO no. 155/2024 and Law no. 124/2025, as well as Law no. 50/2024 and the ANCOM decisions

adopted for the application of the DSA in Romania. For the identification of institutional roles and concrete administrative mechanisms, use was made of ANCOM's annual report on DSA implementation in Romania, the DNSC (National Directorate of Cyber Security) annual report for 2024, the official DORA materials published by financial supervisory authorities and the ENISA reports on maturity and the threat landscape in the public administration and financial sectors. [8]

On an empirical level, the selection of indicators aimed to highlight the relationship between social exposure, administrative maturity and technical risk. Five data groups were therefore chosen: connectivity and internet access in Romania; use of digital public services; use of connected devices by individuals and enterprises; citizens' perception of disinformation and the role of authorities; and the dynamics of cyber incidents and threats facing public administration. This set of indicators is not accidental: it enables the connection of legal norms with the factual terrain on which they operate. Ultimately, a good legal-administrative article is not limited to the exegesis of statutory text but must also show why that text is necessary, where it produces effects and what gaps it still leaves uncovered. [9]

Regarding the case studies, situations were selected that illustrate the composite risk of the subject: the ransomware attack on the Hipocrate platform, which affected 26 hospitals and highlights vendor dependency and the propagation effect through infrastructure; the official guidance on deepfakes and the example of a deepfake using the image of Mugur Isărescu employed for investment fraud, which illustrates the bridge between synthetic content and economic deception; and European case law on the delisting of manifestly inaccurate information and intermediary obligations, which provides standards of proportionality and due diligence. The selection criterion was legal representativeness, not media spectacle. [10]

From an analytical standpoint, the study operates with the abstract around three risk vectors. The first is the vector of "synthetic content and deception", in which the AI Act, the DSA, the GDPR and case law on inaccuracy and content removal are relevant. The second is the vector of "infrastructure and supply chain", where NIS2, the CRA and ENISA documents on IoT and digital product security become central. The third is the vector of "operational continuity and sectoral resilience", where DORA is the paradigmatic instrument and public administration and healthcare provide examples with demonstrative value. [11] This framework does not artificially simplify reality but renders it legally intelligible, as it allows the mapping of obligations onto institutional actors and risk categories. [12]

Methodologically, the limitations of the approach were also taken into account. Some national texts or official reports are not easily accessible in a citation-friendly format, and Romanian public judicial practice specifically concerning deepfakes, content removal orders or the direct correlation between IoT and disinformation is still in a formative stage. For this reason, in the discussion section, certain conclusions are explicitly formulated as doctrinal inferences grounded in legislation, administrative reports and European case law,

rather than as absolute empirical generalisations. This methodological caution is, however, precisely consonant with the rigour required by serious legal research. [13]

3. Results

The factual premise of the research is one of convergence: Romanian society is intensely digitalised at the level of access and everyday use, yet not equally mature with regard to the governance of public services and the associated risks. In 2025, 89.1% of households had internet at home, while only 24% of individuals aged 16–74 had used public authority websites or applications in the previous year; simultaneously, 62% of Romanian internet users were using connected devices in 2024, and only 11% of Romanian enterprises were using IoT systems in 2021. [14] This statistical profile is particularly relevant from a legal standpoint: it indicates a high social readiness for digital tools, combined with an administrative and organisational asymmetry that can amplify the effects of technical vulnerabilities and informational manipulation. [15]

The applicable normative architecture can be summarised as follows:

Table 1. Comparative Overview of Key EU Digital Governance and Cybersecurity Instruments

Instrument	Main Legal Object	Actors Concerned	Obligations Relevant to the Article's Topic	Dominant Administrative Function
NIS2 / Government Emergency Ordinance No. 155/2024, approved by Law No. 124/2025	Security of networks and information systems for essential and important entities	Public administration, critical infrastructures, digital service providers	Risk management, incident reporting, informing management, designation of responsible persons, supervision and sanctions	Risk governance and administrative control
DORA (Digital Operational Resilience Act)	Digital operational resilience in the financial sector	Banks, insurers, investment firms, other financial actors and ICT dependencies	ICT risk management framework, resilience testing, incident reporting, supplier and third-party registers	Sectoral supervision and operational continuity
CRA (Cyber Resilience Act)	Security of products with digital elements	Manufacturers, importers, distributors	Security by design and by default, vulnerability management, incident and vulnerability reporting, CE marking	Market regulation and lifecycle security management
DSA / Law No. 50/2024	Regime of online intermediary services and procedural liability online	Online service providers, platforms, search engines	Complaints mechanisms, orders regarding illegal content, transparency notifications, procedural mechanisms, systemic risk assessment for Very Large Online Platforms (VLOPs)	Administrative coordination and user protection
AI Act	Harmonized rules for artificial intelligence systems	Providers and professional users/deployers of certain AI systems	Transparency obligations for generated/manipulated content, labeling of deepfakes, governance and risk-based compliance	Risk-based compliance supervision
GDPR (General Data Protection Regulation)	Protection of personal data	Controllers and processors	Lawfulness, security, impact assessment, rights of data subjects	Oversight of data processing and individual remedies

Source: Author's own elaboration based on EU legislation and official regulatory documents.

This mapping is supported by official texts and implementation documents at both European and national level. NIS2 pursues a common framework for regulating cybersecurity at EU level; in Romania, Law no. 124/2025, approving GEO no. 155/2024, expressly sets out the obligations of governing bodies, their training requirements and the limits of administrative sanctions. DORA has been applicable since 17 January 2025 in the financial sector. The DSA, through Law no. 50/2024 and the ANCOM report, acquires a clear national procedural mechanism. The CRA shifts the focus towards the inherently secure digital product, while the AI Act provides for a phased application schedule, including for the transparency obligations under Art. 50, applicable from 2 August 2026. [16]

Regarding the core of NIS2 obligations in Romanian law, the conclusion is clear: cybersecurity is no longer conceived as an exclusively technical matter. Law no. 124/2025,

approving GEO no. 155/2024, provides that members of the governing bodies of essential and important entities must complete accredited professional training, ensure the allocation of necessary resources, designate security officers and support the implementation of risk management measures. Furthermore, the sanctioning regime may reach, for certain infringements committed by essential entities, 10 million euros or 2% of total annual worldwide turnover, whichever is higher. From an administrative perspective, this represents a paradigm shift: managerial accountability and internal control become components of administrative legality, not merely good practices. [17]

For public administration, these obligations are layered onto a still modest maturity landscape. ENISA indicates that the public administration sector is among the least mature under NIS2, that only 27% of the public administrations surveyed were aware of the general scope of the directive, and that 76% of critical entities in the sector did not participate in collaboration or information-sharing mechanisms. ENISA also shows that public administration accounted for 19% of all events recorded in the reporting period July 2023–June 2024 and 33% of DDoS (Distributed Denial of Service) incidents. [18] The relevance of these figures for the present subject is twofold: they justify the emphasis placed by the abstract on governance and confirm that institutional vulnerability is not a doctrinal hypothesis but an officially documented fact. [19]

In the area of digital services and online content, ANCOM's 2024 annual report provides a very precise picture of the national DSA enforcement mechanism. Law no. 50/2024, which entered into force in March 2024, is not limited to designating ANCOM as the digital services coordinator but also establishes [20] the sanctioning regime, the mechanism for issuing orders against illegal content and the framework for cooperation with sectoral authorities. The report explains that the DSA aims, among other things, at more effective protection of consumers and fundamental rights, at defining clear responsibilities for platforms and at addressing illegal content, hate speech and disinformation. In addition, ANCOM adopted in 2024 three normative decisions concerning the complaints procedure, trusted flaggers and out-of-court dispute resolution bodies. This is essential for a legal-administrative approach to disinformation: the state operates not only through prohibitions but also through procedural infrastructure. [21]

An important observation emerges here from combining official sources with the specialist literature. The DSA does not automatically render every piece of false content illegal. As Fathaigh (2025) demonstrates, the regulation of disinformation under the DSA operates predominantly through the logic of systemic risk and due diligence instruments, rather than through the introduction of a general criminalisation of “online falsehood”. This explains why the administrative law of platforms is procedural and preventive in nature: complaints, traceability, audits, trusted flaggers, information requests, risk assessments and mitigation measures. For the present article, the consequence is significant: the fight against deepfakes and AI manipulation cannot rest exclusively on the notion of illegal content but must also be anchored in the organisational and technical obligations of digital actors. [22]

The AI Act regime completes this picture but does not exhaust it. According to official Commission materials, the transparency obligations under Art. 50 became applicable on 2 August 2026, and they concern, among other things, the labelling of artificially generated or manipulated content and the facilitation of its identification in a machine-readable manner compatible with detection mechanisms. The Commission has, for precisely this reason, initiated the drafting of a code of practice for the marking and labelling of AI-generated content. From an administrative perspective, this means that the period analysed by the present study is one of transition: the transparency obligation will very soon become justiciable and subject to administrative review, yet at the time of writing this article, the system is still in the operational preparation phase. Legal literature warns, however, that mere labelling will not eliminate the phenomenon but will only raise the threshold of caution and verifiability. [23]

Regarding the CRA, its importance for the subject of this article derives from the fact that many manipulation and exfiltration operations rely on insecure or insufficiently updated digital products. The Regulation aims to create the conditions for the development of secure hardware and software in the Union, to raise the level of security across the entire product lifecycle and to provide buyers and users with adequate information. The principal obligations apply from 11 December 2027, while the obligations to report actively exploited vulnerabilities and severe incidents begin from 11 September 2026. [24] In doctrinal terms, Teichmann (2025/2026) and van 't Schip (2025) have observed that this regulation shifts the paradigm from post-facto remediation to security embedded in the product and its supply chain. For our subject, the implication is direct: without security by design for cameras, sensors, edge devices and connected software products, any anti-disinformation strategy remains defensive and incomplete. [25]

DORA provides an even clearer example of the transformation of a technical concern into an administrative governance obligation. Official documents show that DORA has applied since 17 January 2025 and imposes a harmonised framework for ICT risk management, major incident reporting, third-party risk management and resilience testing. In Romania, the ASF (Financial Supervisory Authority) page dedicated to DORA confirms applicability from 17 January 2025. From a doctrinal standpoint, Buttigieg and Brunelli Zimmermann (2024) observe that the real challenge lies not in the existence of obligations but in the coordination of supervision and the avoidance of fragmentation. For the present article, DORA is relevant not only as a financial *lex specialis* but also as an organisational model of “operational compliance”: mapping dependencies, testing, auditability, crisis scenarios and the strategic accountability of leadership. This model can, *mutatis mutandis*, be adapted to other administrative sectors as well. [26]

To better understand the temporal relationship between the instruments, the following schema is useful:

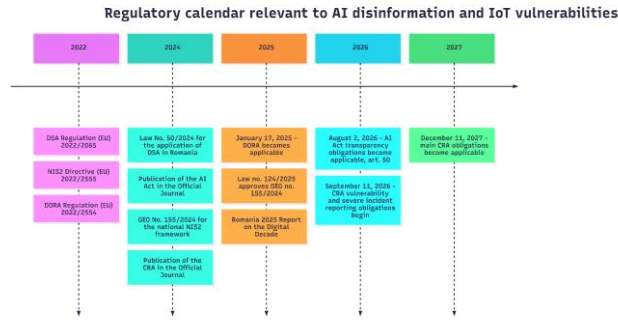


Fig. 1. Regulatory Timeline of Key European Union Instruments Relevant to AI-Driven Disinformation and IoT Vulnerabilities

Source: Author’s own elaboration based on European Union legislative instruments, including the Digital Services Act, NIS2 Directive, Digital Operational Resilience Act (DORA), Cyber Resilience Act (CRA), and Artificial Intelligence Act.

The timeline above derives from official European and national texts and explains why the subject of this article is one “in motion”: after 17 January 2025, DORA is already applicable to positive law; in 2025, Romanian NIS2 law was consolidated through Law no. 124/2025; and from 2 August 2026, Art. 50 of the AI Act will transform the transparency obligation regarding synthetic content into a legal standard directly relevant for public administration, platforms and digital markets. [27]

The empirical dimension of the risk is summarised in the following table:

Table 2. Key Digitalization and Cybersecurity Indicators Relevant to Public Administration and Digital Risk Governance

Official Indicator	Value	Legal-Administrative Significance
Households in Romania with internet access, 2025	89.1%	Digital administrative services operate within an almost fully connected society
Use of e-government in Romania, 2025	24%	Gap between connectivity and the actual use of digital administrative tools
Internet users in Romania who use connected devices, 2024	62%	Expansion of the social risk surface associated with IoT
Romanian enterprises using IoT, 2021	11%	Selective organizational adoption, with risks concentrated in specific sectors
Romanian citizens who believe it is important for authorities to combat online disinformation, 2025	78%	Explicit normative expectation toward public administration
EU respondents who were exposed to online disinformation in the last 7 days, 2025	66%	High prevalence of the phenomenon in the European digital space
Reported online fraud in Romania, 2024 vs. 2023	+40.2%	Intensification of digital fraud and exploitation of public trust
Malware incidents in Romania, 2024 vs. 2023	+286.8%	Aggravation of the technical component of cyber threats
Ransomware incidents managed by the National Cyber Security Directorate (DNSC) in 2024	101	Real operational pressure on public and private entities
Public administration share of ENISA-reported incidents, July 2023 – June 2024	19%	The public sector remains a primary target for attackers

Source: Author's own compilation based on data from Eurostat, the National Institute of Statistics of Romania (INS), the National Cyber Security Directorate (DNSC), the European Union Agency for Cybersecurity (ENISA), and the European Commission (Eurobarometer).

These figures carry two cumulative meanings. On the one hand, they justify the adoption of an integrated approach: AI-assisted disinformation must not be analysed in isolation from the broader ecosystem of fraud, malware and supply-chain breaches. On the other hand, they refute a thesis still present in some administrative practices, according to which disinformation is merely a matter of public communication or media literacy. In reality, the DNSC and ENISA data point to a structural association between informational manipulation, technical security and operational continuity. [28]

The case of the Hipocrate platform is, from this perspective, paradigmatic. According to official communications and reports, the Backmydata/Phobos-type attack disrupted the operations of 26 hospitals in Romania, and the DNSC annual report indicates that the service was affected for approximately one week. The legally relevant phenomenon is not merely the existence of the malware or the ransom demand, but the fact that a software or managed services provider becomes the single point of vulnerability for an entire group of healthcare facilities. From an administrative perspective, this lends new weight to the obligations concerning third-party assessment, contractual clauses, continuity plans, logging and the right of audit. In other words, supply-chain vulnerability is not a peripheral matter but forms part of the legality of public service organisation. [29]

The second case study, this time along the axis of synthetic content, is provided by the official materials of the DNSC and the Romanian Police concerning deepfakes and investment fraud. The DNSC guidance expressly identifies a deepfake using the image of the NBR (National Bank of Romania) Governor, while the Romanian Police indicates that in 2025 deepfakes and artificially generated images became a preferred instrument in trading scam and investment fraud schemes. [30] From a legal standpoint, this example is more valuable than a mere media illustration. It shows that the boundary between “disinformation” and “deception” is porous: synthetic content does not merely persuade the public of a general untruth but can also induce concrete acts of financial disposition. Consequently, the AI Act transparency obligations, the DSA procedures and common law remedies must be understood together, not in isolation. [31]

The relationship between the technical source of the risk and its social effect can be summarised as follows:

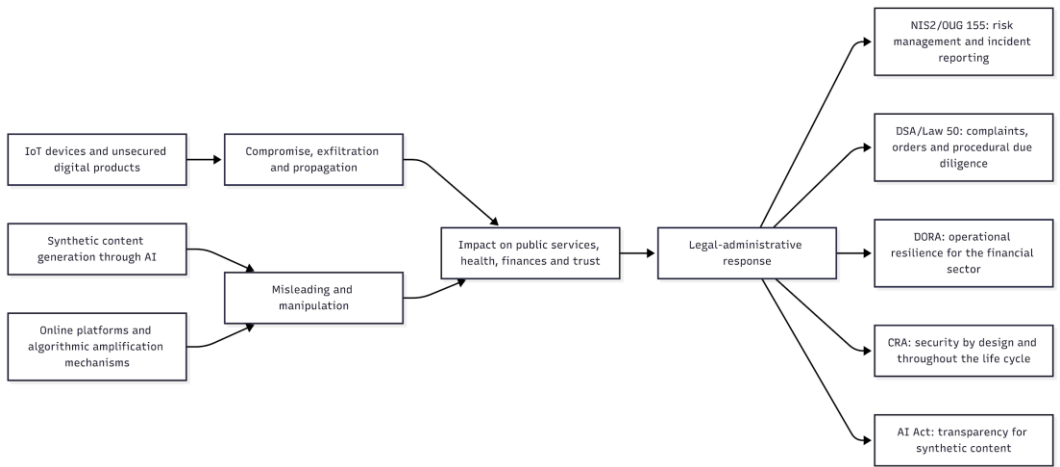


Fig. 2. Conceptual Model of Legal-Administrative Response to AI-Driven Disinformation and IoT Security Vulnerabilities
 Source: Author’s own elaboration based on European Union cybersecurity and digital governance legislation.

The diagram highlights the central idea of the study: AI disinformation and IoT vulnerabilities are not two juxtaposed subjects but two segments of the same chain of risk. This chain begins in the technical production of the falsehood or in the compromise of infrastructure, continues through socio-digital amplification and concludes, legally, only through a combination of ex ante and ex post obligations. This is precisely where the abstract provided converges with the recent literature on deepfake regulation, supply-chain security and digital product security. [32]

From the perspective of case law, the results can be summarised as follows:

Table 3. Key European Case Law on Online Content Moderation, Platform Liability and Digital Rights

Case	Court	Established Principle	Relevance for the Article
C-18/18, Glawischnig-Piesczek v Facebook Ireland	CJEU (Court of Justice of the European Union)	A platform may be required to remove identical content and, under certain conditions, equivalent content declared unlawful	Establishes mechanisms for content removal and the extension of remedies
C-460/20, Google (dereferencing inaccurate content)	CJEU (Court of Justice of the European Union)	Dereferencing is necessary when the data subject demonstrates the manifest inaccuracy of the information	Relevant for deepfakes, factual falsity, and protection of the individual
Delfi AS v Estonia	ECtHR (European Court of Human Rights)	The liability of an intermediary for manifestly unlawful comments may be compatible with Article 10 of the European Convention on Human Rights	Confirms the heightened duty of diligence in content moderation
Sanchez v France	ECtHR (European Court of Human Rights)	Sanctioning the failure to promptly remove unlawful comments from a public account during an electoral campaign may be proportionate	Highlights the requirement for active management of public content and interaction spaces

Source: Author's own elaboration based on case law of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR).

The common significance of this case law lies in the fact that European law adheres neither to the thesis of absolute intermediary neutrality nor to that of automatic liability for any third-party content. The standard is one of the juridification of due diligence: the manifestly unlawful or manifestly inaccurate character of content, the technical possibility of intervention, the context of publication and the protected interest all become criteria of assessment. For the subject of deepfakes and AI disinformation, this orientation is particularly important, as it suggests that transparency and procedural promptness will matter as much as the material truth of the content. [33]

The specialist literature, examined in parallel with official sources, confirms several robust doctrinal trends. Vandezande (2024) insists that NIS2 is, in essence, an upgrade of the European security strategy, with emphasis on supply-chain and managerial accountability. Buttigieg and Brunelli Zimmermann (2024) show that DORA places the quality of the supervisory architecture and the coherence of implementation at its centre. Teichmann

(2025/2026) explains the CRA as a form of hybrid regulation, in which mandatory obligations are complemented by standardisation and lifecycle compliance. Fathaigh (2025) demonstrates that the DSA addresses disinformation deliberately through the lens of systemic risk and public-order governance. Łabuz (2024), Veale and Zuiderveen Borgesius (2021) and Romero-Moreno (2024; 2025) converge on the idea that the AI Act is necessary but insufficient unless complemented by other legal regimes and genuine administrative capacity. Recent Romanian doctrine points in the same direction: Ungureanu (2025) discusses the “European legal antidotes” to online manipulation, while Târnavăan (2025) places deepfakes and social engineering directly within the sphere of critical infrastructures and algorithmic objectivism.

The synthetic result of this entire section is as follows: the abstract provided can be developed, rigorously and convincingly, into a substantial legal-administrative article precisely because there already exists a critical mass of positive law, official data and doctrine that permits the demonstration of a strong thesis. That thesis is that resilience against AI disinformation cannot be conceived separately from infrastructure resilience; and infrastructure resilience, in turn, cannot be left exclusively to technical specialists, because it has become a leadership obligation and an object of administrative control. [34]

4. Discussions

The first conclusion of the discussion concerns the inadequacy of fragmented approaches. In many organisations, including public administration, disinformation is still handled by communications departments, while cybersecurity is managed by IT departments; procurement of digital products is left to public procurement or logistics management, and legal compliance remains the responsibility of legal advisers. Yet the very sources analysed show that this bureaucratic division is counterproductive. [35] NIS2 requires governing bodies to approve and oversee risk measures; DORA requires a serious mapping of ICT dependencies; the CRA requires security across the entire lifecycle; the DSA requires procedures and maps the relationship between platforms, users and authorities; the AI Act requires transparency for synthetic content. It follows that public administration and regulated organisations need a single “internal constitution of resilience”, not multiple parallel regimes without functional interfaces. [36]

The second conclusion concerns the shift from formal compliance to effective governance. In the classical sense, legal compliance could be reduced to the existence of internal policies, standard procedures and bureaucratic registers. In the matter under analysis, such compliance is insufficient. The ENISA data on public administration with a low level of participation in information sharing, modest awareness of the NIS2 scope and high exposure to attacks suggest that the real problem is not the absence of texts but the capacity to translate them into organisational practices. [37] In legal-administrative terms, this means that formal legality must be complemented by functional legality: the effective existence of responsibilities, traceability, exercises, training, documentation and the decision-making chain. [38]

From this perspective, the central recommendation for the article and for any public policies arising from it is the institutionalisation of cybersecurity at leadership level. The abstract explicitly invokes elevating security to board level and strengthening the CISO role. This proposal is fully compatible with the European normative evolution and with post-NIS2 Romanian law. In public administration, its implementation does not mean the mechanical importation of corporate structures, but the designation of an internal command nucleus capable of integrating the functions of IT, legal, procurement, data protection, business continuity and crisis communication. In the absence of such an integrating level, the organisation responds to incidents in a reactive and desynchronised manner. [39]

Second, the article must insist on the contractual and procurement dimension of resilience. The Hipocrate case and the logic of the CRA show that risk no longer resides solely within the entity itself but also in the ecosystem of suppliers, updates, licences, patches, managed services and edge products. In Romanian administrative law, this has direct implications for terms of reference, clauses concerning security updates, the right of audit, notification deadlines, logging, log export, access to indicators of compromise and post-incident assistance obligations. In other words, the legal security of digital administration must be built pre-contractually as well, not only post-incident through liability and sanctions. [40]

Third, the analysis must emphasise that “transparency” is not equivalent to “solving” the deepfake problem. The AI Act and the code of practice currently being drafted pursue labelling and detectability, but doctrine is nearly unanimous in observing that malicious actors will not self-label, and that signatures or watermarks can be circumvented or removed. [41] It is precisely for this reason that these measures must be viewed as part of a broader package: institutional education, escalation procedures, coordination with platforms, rapid contestation mechanisms, rules on digital evidence and, where appropriate, the use of existing pathways for delisting, removal or rectification. Transparency reduces the evidentiary burden and accelerates the response; it does not, however, substitute the remedy. [42]

A point to be discussed separately is the tension between combating disinformation and protecting freedom of expression. Here, European case law has an essential methodological function. The cases of Glawischnig-Piesczek, Google C-460/20, Delfi and Sanchez show that intervention on content or on its accessibility can be legitimate if it is sufficiently foreseeable, proportionate and focused on unlawfulness, manifest inaccuracy or the reasonable due diligence of the intermediary actor. For a Romanian academic article, the discussion should not be framed in the simplistic terms of “censorship” versus “absolute freedom”, but in terms of correct procedure and standards of justification. In matters of deepfake and synthetic manipulation, the risk of administrative arbitrariness is reduced not through inaction but through clear regulation of competences, deadlines, evidence and avenues for contestation. [43]

From this derives a broader thesis of doctrinal value. Digital administrative law tends to become a law of “organisational prudence”. It no longer exhausts the control of legality exclusively through the verification of the form of the administrative act or of classical

competence, but also through the verification of the institution's capacity to anticipate, document and absorb technological risks with effects on rights, public services and markets. In this sense, NIS2, DORA, the DSA, the CRA and the AI Act are not merely sectoral regulations but expressions of the same model of preventive administration, assisted by technical standards and oriented towards resilience. Consequently, the article derived from the abstract can contribute meaningfully to Romanian doctrine precisely by emphasising the unity of this model. [44]

On a practical level, the model I propose derives from all the sources examined and can be formulated in seven coordinates, expressed here in summary form but developed analytically in the body of the section. First, the governing body must receive an express competence and an obligation of effective exercise, not merely a nominal role. Second, an operational security leadership function must be designated, with technical autonomy and a direct reporting line. Third, the management of suppliers and products with digital elements must be integrated into legal and contractual obligations. Fourth, the organisation must have distinct procedures for technical incidents, fraudulent synthetic content and requests addressed to platforms or authorities. Fifth, the preservation and management of digital evidence must be standardised. Sixth, a culture of periodic training is required, including for non-technical staff. Seventh, compliance assessment must become continuous and scenario-based, not annual and purely declaratory. Each of these coordinates is supported, in various forms, by the legislative and doctrinal corpus analysed. [45]

A final observation concerns the Romanian specificity. Romania does not start from zero: it already has a significant normative infrastructure, an active national cybersecurity authority, a digital services coordinator with a clear legal basis, a central bank, and a financial supervisory authority operating in compliance with DORA, as well as a high level of social awareness regarding the need to combat disinformation. [46] The critical problem is therefore not the total absence of norms but the capacity to integrate norms, statistics, and management. From the standpoint of the research outlined in the abstract, this is precisely where the stakes lie: to show that the future of Romanian digital administrative law depends not only on new texts but also on institutions' capacity to translate European normative convergence into internal practice convergence. [47]

5. Conclusions

The analysis carried out in the present study has systematically demonstrated that the intersection between disinformation generated by artificial intelligence systems and the vulnerabilities of infrastructures based on interconnected devices constitutes, at present, one of the most complex challenges for contemporary public law and modern public administration. This reality can no longer be treated exclusively as a technological or cybersecurity problem but must be approached as a legal-administrative phenomenon with direct implications for digital public order, the functioning of public services and the protection of individuals' fundamental rights.

As emerges from the recent analysis of the European normative framework, consolidated through instruments such as the revised Network and Information Security Directive, the

Digital Operational Resilience Act, the Cyber Resilience Act and the Digital Services Act, the European legislator has effected a fundamental conceptual shift: from a reactive approach to cyber risks to a preventive one, based on organisational accountability, institutional governance and the systematic assessment of risks. These normative instruments implicitly enshrine the idea that digital security constitutes an essential component of good administration and the exercise of public functions, under conditions of legality and efficiency.

In particular, the research has demonstrated that the use of automatic content generation technologies, combined with the exploitation of existing vulnerabilities in IoT infrastructures, can produce significant legal and administrative effects, including the disruption of public services, the compromise of administrative data integrity and the erosion of citizens' trust in state institutions. The examples analysed, including cases of informational manipulation through falsified video materials and the use of connected devices for data exfiltration, confirm that these threats are not hypothetical but represent real, internationally documented risks.

Furthermore, the doctrinal and normative analysis has revealed the existence of operational gaps in the implementation of legal obligations concerning cybersecurity and the management of digital incidents. In numerous situations, public institutions and economic operators lack adequate organisational structures for monitoring technological risks, and the information security function is not effectively integrated into strategic decision-making mechanisms. This situation contravenes the principle of professional due diligence and may give rise to legal liability, including administrative, contravention or civil liability, in the event of harm.

A central element of the conclusions of the present study is the necessity of institutionalising a culture of digital resilience within public administration and private organisations that provide essential services. This culture cannot be achieved exclusively through the adoption of advanced technologies but must be grounded in clear legal norms, standardised administrative procedures and efficient control and audit mechanisms. In this regard, it is imperative to strengthen the role of executive leadership in overseeing cyber risks, as well as to establish explicit responsibilities for the information security function at the level of governing structures.

The study has also highlighted the importance of integrating digital risk assessment into the process of developing and implementing public policies. Public administration must adopt a proactive approach, based on the systematic analysis of vulnerabilities and the periodic testing of institutional capacity to respond to incidents. In this context, the use of resilience tests and operational simulations constitutes an essential instrument for verifying the effectiveness of security measures and for identifying procedural deficiencies.

From a legal perspective, the research findings confirm that responsibility for digital security can no longer be limited to the technical or operational level but must be extended to the level of institutional leadership. In accordance with modern principles of

administrative governance, the heads of public institutions have an obligation to ensure the operation of information systems under conditions of safety and to prevent the occurrence of harm caused by the improper use of digital technologies. Failure to comply with these obligations may constitute a breach of the principle of legality and may entail the legal liability of the competent authorities.

Another relevant aspect identified in the study is the necessity of harmonising security incident reporting procedures with the legal obligations laid down by European and national legislation. Late or incomplete reporting of incidents can affect the capacity of authorities to manage crisis situations effectively and may generate significant legal consequences. Accordingly, public institutions and economic operators must develop internal mechanisms for rapid and transparent reporting, based on clear criteria and well-defined responsibilities.

At the same time, the study has underlined the essential role of institutional cooperation in the prevention and combating of disinformation phenomena and cyber attacks. In a digital environment characterised by technological interdependence and informational mobility, no institution can manage in isolation the risks associated with the use of digital technologies. Cooperation between administrative authorities, regulatory bodies, digital service providers and the academic community represents an indispensable condition for ensuring the security and stability of information systems.

Last but not least, the research has highlighted the necessity of developing continuous professional training programmes for public administration personnel and for specialists in the field of information security. Technical and legal competences must be permanently updated in order to keep pace with the rapid evolution of digital technologies and the methods employed by malicious actors. Investment in professional training represents, in this sense, an essential preventive measure for reducing operational risks and for increasing institutional response capacity.

In conclusion, the present study confirms that protection against disinformation generated by artificial intelligence and against the vulnerabilities of digital infrastructures cannot be achieved exclusively through technical instruments but requires an integrated approach combining legal norms, administrative procedures and institutional governance mechanisms. This integrated approach must be grounded in the principles of legality, accountability and transparency, which constitute the essential pillars of modern public administration.

Consequently, the development of a coherent legal-administrative framework, adapted to contemporary technological realities, represents an indispensable condition for ensuring digital security and for protecting the public interest in the information society. Only through the strengthening of institutional accountability and the implementation of efficient prevention and control mechanisms can the maintenance of citizens' trust in state institutions and the stable functioning of public services in the digital environment be assured.

References

- [1] E. Union, "Cybersecurity of network and information systems," EUR-Lex, 20 April 2026. [Online]. Available: <https://eur-lex.europa.eu/EN/legal-content/summary/cybersecurity-of-network-and-information-systems.html>.
- [2] Bestavros, Azer; Dogan, Stacey; Ohm, Paul; Sellars, Andrew, "Bridging the Computer Science – Law Divide," in *CSLAW '22: Symposium on Computer Science and Law*, 2022.
- [3] ANCOM, "Raport anual privind aplicarea Digital Services Act (DSA) în România," Autoritatea Națională pentru Administrare și Reglementare în Comunicații, București, 2024.
- [4] ANCOM, "Raport anual privind aplicarea Digital Services Act (DSA) în România," Autoritatea Națională pentru Administrare și Reglementare în Comunicații, București, 2024.
- [5] European Union Agency for Cybersecurity (ENISA), "ENISA NIS360 2024 – Cybersecurity maturity and criticality of NIS2 sectors," European Union Agency for Cybersecurity, Heraklion, 2025.
- [6] Court of Justice of the European Union, "Press Release No 128/19 – Judgment in Case C-18/18 Glawischmig-Piesczek v Facebook Ireland Limited," Court of Justice of the European Union, Luxembourg, 2019.
- [7] European Union, "Cybersecurity of network and information systems," EUR-Lex, 14 December 2022. [Online]. Available: <https://eur-lex.europa.eu/EN/legal-content/summary/cybersecurity-of-network-and-information-systems.html>. [Accessed 20 April 2026].
- [8] ANCOM, "Raport anual privind aplicarea Regulamentului privind serviciile digitale (DSA) în România," Autoritatea Națională pentru Administrare și Reglementare în Comunicații, București, 2024.
- [9] Institutul Național de Statistică, "Accesul populației la tehnologia informației și comunicațiilor în anul 2025," Institutul Național de Statistică, București, 2025.
- [10] Directoratul Național de Securitate Cibernetică, "Alertă: Backmydata Ransomware," Directoratul Național de Securitate Cibernetică, București, 2024.
- [11] SecurityToday, "Cybersecurity Regulation in Europe: NIS2, DORA, CRA, and AI Act Overview," SecurityToday, 12 December 2024. [Online]. Available: <https://www.securitytoday.de/en/2024/12/12/cybersecurity-regulation-in-europe-nis2-dora-cra-and-ai-act-overview/>. [Accessed 20 April 2026].
- [12] European Commission, "Navigating the AI Act," Shaping Europe's digital future, 28 January 2026. [Online]. Available: 20. [Accessed April 2026 <https://digital-strategy.ec.europa.eu/en/faqs/navigating-ai-act>].
- [13] ANCOM, "Raport anual conform art. 55 din Regulamentul privind serviciile digitale," Autoritatea Națională pentru Administrare și Reglementare în Comunicații, București, 2024.
- [14] Trading Economics, "Romania – Level of internet access," Trading Economics, 2026. [Online]. Available: <https://tradingeconomics.com/romania/level-of-internet-access-eurostat-data.html>. [Accessed 20 April 2026].
- [15] Institutul Național de Statistică, "Accesul populației la tehnologia informației și comunicațiilor în anul 2025," Institutul Național de Statistică, București, 2025.
- [16] European Commission, "NIS2 Directive: securing network and information systems," Shaping Europe's digital future, 20 January 2026. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>. [Accessed 20 April 2026].
- [17] Parlamentul României, "Legea privind dreptul de autor și drepturile conexe," Portal Legislativ, 1996. [Online]. Available: <https://legislatie.just.ro/Public/FormaPrintabila/00000G2W4JLR489ZMOA327XB328GIAAA>. [Accessed 20 April 2026].
- [18] European Union Agency for Cybersecurity (ENISA), "Public administration increasingly targeted by DDoS attacks," ENISA, 6 November 2025. [Online]. Available:

- <https://www.enisa.europa.eu/news/public-administration-increasingly-targeted-by-ddos-attacks>. [Accessed 20 April 2026].
- [19] European Union Agency for Cybersecurity (ENISA), "ENISA NIS360 2024 – Cybersecurity maturity and criticality of NIS2 sectors," European Union Agency for Cybersecurity, Heraklion, 2025.
 - [20] ANCOM, "What is ANCOM's role as coordinator of digital services?," ANCOM, 26 September 2024. [Online]. Available: <https://www.ancom.ro/en/about-us/media-en/press-releases/what-is-ancoms-role-as-coordinator-of-digital-services/>. [Accessed 20 April 2026].
 - [21] ANCOM, "Raport anual conform art. 55 din Regulamentul privind serviciile digitale," Autoritatea Națională pentru Administrare și Reglementare în Comunicații, București, 2024.
 - [22] R. Ó Fathaigh, D. Buijs and J. van Hoboken, "The Regulation of Disinformation Under the Digital Services Act," *Media and Communication*, vol. 13, 2025.
 - [23] European Commission, "Navigating the AI Act," Shaping Europe's digital future, 28 January 2026. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/faqs/navigating-ai-act>. [Accessed 20 April 2026].
 - [24] European Commission, "NIS2 Directive: securing network and information systems," Shaping Europe's digital future, 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>. [Accessed 20 April 2026].
 - [25] European Commission, "Cyber Resilience Act – Summary of the legislative text," Shaping Europe's digital future, 3 2025 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/cra-summary>. [Accessed 20 April 2026].
 - [26] European Insurance and Occupational Pensions Authority (EIOPA), "Digital Operational Resilience Act (DORA)," EIOPA, 2025. [Online]. Available: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en. [Accessed 20 April 2026].
 - [27] European Insurance and Occupational Pensions Authority (EIOPA), "Digital Operational Resilience Act (DORA)," EIOPA, 2025. [Online]. Available: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en. [Accessed 20 April 2026].
 - [28] Institutul Național de Statistică, "Accesul populației la tehnologia informației și comunicațiilor în anul 2025," Institutul Național de Statistică, București, 2025.
 - [29] Directoratul Național de Securitate Cibernetică, "Alertă: Backmydata Ransomware," DNSC, 15 February 2024. [Online]. Available: <https://www.dnsc.ro/citeste/alert-backmydata-ransomware-spitale-romania>. [Accessed 20 April 2026].
 - [30] OECD.AI, "AI Incident – 2025-02-14-e2d1," OECD AI Incidents Monitor, 14 February 2025. [Online]. Available: <https://oecd.ai/en/incidents/2025-02-14-e2d1>. [Accessed 20 April 2026].
 - [31] Directoratul Național de Securitate Cibernetică, "Ghid privind identificarea materialelor de tip Deepfake," Directoratul Național de Securitate Cibernetică, București, 2024.
 - [32] R. Ó Fathaigh, D. Buijs and J. van Hoboken, "The Regulation of Disinformation Under the Digital Services Act," *Media and Communication*, p. 13, 2025.
 - [33] Court of Justice of the European Union, "Press Release No 128/19 – Judgment in Case C-18/18 Glawischnig-Piesczek v Facebook Ireland Limited," Court of Justice of the European Union, Luxembourg, 2019.
 - [34] Parlamentul României, "Legea nr. 124/2025 privind aprobarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică," Portal Legislativ, 7 July 2025. [Online]. Available: <https://legislatie.just.ro/Public/FormaPrintabila/00000G2W4JLR489ZMOA327XB328GIAAA>. [Accessed 20 April 2026].
 - [35] European Parliament, "Interplay between the AI Act and the EU digital legislative framework," European Parliamentary Research Service, Brussels, 2025.
 - [36] Parlamentul României, "Legea nr. 124 din 7 iulie 2025 pentru aprobarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică," Portal Legislativ, 7 July 2025. [Online]. Available:

- <https://legislatie.just.ro/Public/FormaPrintabila/00000G2W4JLR489ZMOA327XB328GIAAA>. [Accessed 20 April 2026].
- [37] European Union Agency for Cybersecurity (ENISA), "Public administration increasingly targeted by DDoS attacks," ENISA, 6 November 2025. [Online]. Available: <https://www.enisa.europa.eu/news/public-administration-increasingly-targeted-by-ddos-attacks>. [Accessed 20 April 2026].
- [38] European Union Agency for Cybersecurity (ENISA), "ENISA NIS360 2024 – Cybersecurity maturity and criticality of NIS2 sectors," European Union Agency for Cybersecurity, Heraklion, 2025.
- [39] Parlamentul României, "Legea nr. 124 din 7 iulie 2025 pentru aprobarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică," Portal Legislativ, 7 July 2025. [Online]. Available: <https://legislatie.just.ro/Public/FormaPrintabila/00000G2W4JLR489ZMOA327XB328GIAAA>. [Accessed 20 April 2026].
- [40] Directoratul Național de Securitate Cibernetică, "Raport anual de activitate 2024," Directoratul Național de Securitate Cibernetică, București, 2025.
- [41] Council on Foreign Relations, "Beyond Watermarks: Content Integrity Through Tiered Defense," Council on Foreign Relations, 8 May 2024. [Online]. Available: <https://www.cfr.org/blog/beyond-watermarks-content-integrity-through-tiered-defense>. [Accessed 20 April 2026].
- [42] European Commission, "Code of Practice on marking and labelling of AI-generated content," Shaping Europe's digital future, 2025. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content>. [Accessed 20 April 2026].
- [43] Court of Justice of the European Union, "Press Release No 128/19 – Judgment in Case C-18/18 Glawischnig-Piesczek v Facebook Ireland Limited," Court of Justice of the European Union, Luxembourg, 2019.
- [44] European Union, "Cybersecurity of network and information systems," EUR-Lex, 14 December 2022. [Online]. Available: <https://eur-lex.europa.eu/EN/legal-content/summary/cybersecurity-of-network-and-information-systems.html>. [Accessed 14 December 2022].
- [45] Parlamentul României, "Legea nr. 124 din 7 iulie 2025 pentru aprobarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică," Portal Legislativ, 7 July 2025. [Online]. Available: <https://legislatie.just.ro/Public/FormaPrintabila/00000G2W4JLR489ZMOA327XB328GIAAA>. [Accessed 20 April 2026].
- [46] Țuca Zbârcea & Asociații, "Establishing a framework for cybersecurity of networks and IT systems in the civilian national cyberspace," Țuca Zbârcea & Asociații, 2025. [Online]. Available: <https://www.tuca.ro/knowledge/publications/establishing-a-framework-for-cybersecurity-of-networks-and-it-systems-in-the-civilian-national-cyberspace.html>. [Accessed 20 April 2026].
- [47] European Commission, "Romania 2025 Digital Decade Country Report," European Commission, Brussels, 2025.

Voluntary IT Specialist Involvement in Romanian City Digital Strategies

Elena CIGU

*Alexandru Ioan Cuza University of Iasi, Faculty of Economics and Business Administration Iasi, Romania
elenacigu@yahoo.com*

Doru-Constantin MOCANU

*Alexandru Ioan Cuza University of Iasi, Romania, Doctoral School of Economics and Business Administration
mocanudoru@yahoo.com*

Abstract

The rapid evolution of new technologies offers public administration the opportunity to streamline its activities and the services it offers to the community. Most of the time, however, administrative institutions do not have the financial, technical and human resources necessary to implement modern digital solutions. In this context, our study analyzes the impact of the voluntary involvement of Information Technology specialists on the development of digital development strategies of cities in Romania recognized as IT centers. Starting from the premise that civic involvement is no longer limited to isolated initiatives, but has become an important resource for transferring expertise in the process of co-creating public policies in Romania, we will review the forms of participation of IT specialists in the efforts to digitize local administration in major university centers in Romania, the resources of this form of civic activism, as well as the effects of these collaborations, having as a benchmark the components of the digital development strategies of the respective cities. Our research is based on the analysis of official documents available to the public in the cities of Bucharest, Cluj-Napoca, Iași and Timișoara, as well as on reports from other civic or state organizations in the field of technology. Being limited to the four mentioned cities, the results of our study cannot be considered relevant for all urban centers in Romania, but by identifying collaboration mechanisms between local authorities and IT volunteer communities, we can hope that this expertise transfer system will expand and lead to the dynamization of the digital transformation of local administration in our country.

Keywords: digitalisation, public administration, digital governance, transfer of expertise, Romania

1. Introduction

Digital transformation has become one of the fundamental directions of public administration modernization and urban development. The adoption of the United Nations 2030 Agenda for Sustainable Development in 2015 included the strengthening of information technology utilization, as well as the enhancement of efficiency and transparency in public institutions, among the major governance objectives [1]. Subsequently, the European Union incorporated these objectives into its strategic framework through the document “Next Steps for a Sustainable European Future: European Action for Sustainability”, which reinforced the political consensus for promoting digital public administration, smart cities, and citizen-centered public services [2]. Within this framework, the digitalization of public administration has emerged as an institutional instrument for improving efficiency, accessibility, transparency, and civic participation.

Recent European initiatives, particularly the strategic framework of Europe’s Digital Decade, emphasize the need to develop resilient digital ecosystems based on interoperability, innovation, and cooperation among public institutions, the private sector,

and civil society [3]. These strategic orientations have also influenced the public policies adopted by Romania in the fields of public administration digitalization and smart urban development. National strategies on digital transformation and policy documents developed by the authorities responsible for digitalization aim to modernize public services, enhance digital skills, and stimulate technological innovation at both national and local levels [4]. Consequently, digitalization is integrated into a broader vision of sustainable development, aligned with objectives concerning sustainable cities, participatory governance, and the strengthening of institutional partnerships.

In this context, the involvement of IT specialist communities in the design and implementation of urban digital strategies may be interpreted as an expression of the convergence between European sustainability priorities and national strategic directions regarding digital transformation. In Romania, pressure to digitalize public services, increase administrative transparency, and improve the relationship between citizens and local administrations has intensified in recent years, particularly following the COVID-19 pandemic and in the context of European funding opportunities dedicated to the development of digital competencies.

Nevertheless, many local administrations continue to face constraints related to internal technical capacity, deficits in digital skills, and institutional limitations that hinder the implementation of coherent and sustainable digital strategies. Therefore, IT communities may constitute a strategically relevant resource for smart city development and for strengthening local administrative capacity. The voluntary participation of these professionals in consultation, planning, and co-creation processes can facilitate collaborative governance models based on expertise, civic engagement, and open innovation.

The concept of collaborative governance refers to the coordinated participation of public, private, and civic actors in the formulation and implementation of public policies [5]. In the digitalization of public administration, this model is particularly relevant because digital infrastructures and services depend not only on technological investments but also on the capacity of institutions to develop stable relationships of cooperation, trust, and knowledge exchange among multiple stakeholders. In Romanian cities such as Bucharest, Cluj-Napoca, Iași, and Timișoara, where local IT ecosystems have developed rapidly, significant opportunities have emerged for formal and informal partnerships among public administrations, universities, technology companies, and professional communities.

Despite this potential, the voluntary involvement of IT specialists in urban digital strategies remains insufficiently explored in the academic literature and only weakly institutionalized within local public administration in Romania. Important questions persist regarding the motivations for voluntary participation, the mechanisms through which technical expertise can be integrated into administrative processes, and the institutional conditions required for effective digital co-governance. This study addresses this gap by examining the role of the voluntary involvement of IT specialists in the design and implementation of digital strategies in Bucharest, Cluj-Napoca, Iași, and Timișoara.

2. Literature Review

The scholarly literature on urban digital transformation highlights a gradual transition from traditional models of administrative governance, characterized by hierarchical structures and centralized bureaucratic mechanisms, toward collaborative, participatory, and co-creative approaches to governance. In this context, the concept of the smart city has evolved beyond its initial focus on technological infrastructure and digital solutions. Smart cities are increasingly understood as complex socio-technical ecosystems in which administrative performance and innovation capacity result from the interaction between technology, institutions, human capital, and citizen participation [6], [7].

The development of smart cities is frequently associated in the literature with the paradigm of smart governance, understood as the use of digital technologies to optimize decision-making processes, enhance administrative transparency, and facilitate citizen participation in public policy formulation [8]. From this perspective, the digitalization of public administration extends beyond a purely technological dimension and is conceptualized as a process of structural transformation in the relationships between public institutions and local communities.

Consequently, the development of smart city strategies depends not only on digital infrastructure but also on the capacity of local administrations to establish effective mechanisms of collaboration among the public sector, the private sector, academia, and civil society [9]. In the scholarly literature, the concept of the smart city is analyzed both from a structural perspective, emphasizing the interaction between technology, institutions, and human capital [9], [10], and from an evolutionary perspective, describing the transition from traditional models of urban governance toward approaches based on data, connectivity, and real-time decision-making processes [6], [7]. These perspectives converge on the idea that the success of smart city strategies depends on the existence of robust collaborative governance mechanisms and the ability to establish partnerships among relevant institutional and societal actors.

Collaborative governance therefore represents an essential condition for the functioning of intelligent urban ecosystems. Within this approach, public administration is no longer perceived as the sole actor responsible for policy formulation and implementation but rather as a facilitator of cooperation among multiple stakeholders. The integration of digital tools into this system generates efficiency and contributes to strengthening trust in the public sector [6], [11]. Collaborative governance models involve the coordinated participation of public institutions, private-sector organizations, civic groups, and professional communities in the planning, implementation, and evaluation of urban policies. The literature indicates that such models are associated with enhanced innovation capacity and greater institutional adaptability in the context of digital transformation [12].

Researchers have also devoted increasing attention to co-creation and open innovation in local public administration as mechanisms for supporting digital transformation and collaborative urban governance. Co-creation refers to the direct involvement of citizens

and non-state actors in the design, development, and testing of public services [13]. Urban policies are therefore no longer viewed as the exclusive product of administrative apparatuses but rather as outcomes of continuous interaction between public institutions and local innovation ecosystems. These processes are supported by digital infrastructures, open data, and participatory mechanisms. Recent studies demonstrate that initiatives such as urban living labs and co-creation platforms facilitate the experimentation of innovative solutions and the engagement of local actors in urban governance processes [14], [15]. These approaches contribute to strengthening the innovation capacity of public administrations and improving policymaking processes through the integration of knowledge distributed across communities and urban ecosystems.

At the same time, the literature identifies significant limitations and vulnerabilities within current models of urban digital governance. Although digital participation initiatives and open governance platforms are increasingly employed to engage local stakeholders in urban planning, many of these mechanisms remain consultative and do not necessarily lead to a genuine redistribution of decision-making power [16]. In many cases, the participation of citizens and professional communities is formalized in a symbolic manner, without the effective integration of their contributions into final public policies.

Another important research direction concerns the relationship between digitalization, smart governance, and local administrative capacity. Analyses of smart governance instruments indicate that the implementation of digital transformation initiatives within local administrations is significantly influenced by organizational capacity. Institutional structures and the digital competencies of public-sector personnel can generate substantial differences among cities regarding the adoption of digital technologies [17].

In this context, human capital and urban innovation ecosystems play a crucial role in cities' innovation capacity. The literature highlights that complex and knowledge-intensive economic activities tend to concentrate in large urban environments, where advanced skills resources and innovation infrastructures are available, thereby strengthening these cities' capacity to generate and absorb innovation [18]. At the same time, research on open innovation emphasizes the importance of collaboration among organizational actors in the processes of generating, combining, and transferring the knowledge necessary for the development of innovative technological solutions [19]. From the perspective of digital governance, the literature underscores the potential of leveraging distributed expertise and involving non-institutional actors in improving decision-making processes. However, most studies focus on institutionalized forms of collaboration and pay comparatively less attention to the direct involvement of technological communities in the formulation of urban strategies [20].

The approaches discussed above highlight both the potential of collaboration among diverse actors in generating innovative solutions and the current limitations of mechanisms designed to involve non-institutional actors in urban decision-making processes. In this context, the present research is positioned at the intersection of these debates by examining

voluntary IT expertise as a distinct and underexplored resource for collaborative urban digital governance.

3. Research Methodology

This study employs a comparative qualitative approach based on the analysis of smart city strategies, institutional documents, and civic-tech initiatives developed in the municipalities of Bucharest, Cluj-Napoca, Iași, and Timișoara. These cases were selected according to several criteria: the existence of developed IT ecosystems, a high concentration of technology companies, the presence of universities specializing in engineering and computer science, the existence of urban digitalization initiatives, and the availability of public documents related to local digital strategies.

The research design is based on the comparative case study method and seeks to identify the mechanisms through which IT communities participate in urban digital transformation processes. In the absence of a standardized national indicator measuring the degree of urban digitalization, the comparative analysis was conducted through the examination of smart city strategies, institutional structures responsible for digital coordination, implemented projects, and mechanisms of collaboration between local administrations and technological ecosystems.

The primary research method employed is document analysis, applied to urban digitalization strategies, smart city strategies, integrated urban development plans, institutional reports, official communications, and publicly available information from the platforms of local administrations and organizations involved in urban digital transformation. Documents produced by professional organizations, technology communities, business associations, and civic initiatives were also analyzed. The purpose was to identify forms of voluntary involvement in the IT sector, mechanisms of institutional cooperation, and the main objectives and instruments employed within urban digital transformation strategies.

4. Data Sources

The study utilizes data derived from official documents, institutional platforms, and public sources relevant to the analysis of urban digital transformation and collaboration mechanisms between public administrations and local technological communities. The primary data sources consist of digitalization strategies and policy documents developed by the local administrations of Cluj-Napoca, Timișoara, and Iași. These documents include smart city strategies, integrated urban development strategies, digital transformation plans, implementation reports, and documentation related to projects financed through European funds [21], [22], [23]. In the case of Bucharest, no integrated digital transformation strategy was identified; instead, the involvement of IT volunteers in urban digitalization processes appears predominantly within a fragmented ecosystem of institutional initiatives and isolated civic projects.

European and national policy documents were also utilized, including European Commission documents on digital transformation and smart urban development, reports on

the implementation of the European Digital Decade, and Romania's national digitalization strategies [3], [4]. These sources were used to contextualize the institutional and regulatory framework within which local digitalization policies are developed.

Another category of sources consists of public platforms and databases related to European projects and indicators of urban digital development. Information from European Commission platforms, cohesion policy implementation reports, and documentation related to European funding programs for digitalization and urban innovation was analyzed. These sources contributed to the identification of smart city projects implemented in the cities under study and the financial frameworks supporting local digital transformation.

The research also draws upon publicly available information from reports and materials produced by professional organizations, IT industry associations, technology clusters, and local innovation communities. These sources were necessary to identify forms of voluntary participation and mechanisms of collaboration between local administrations and technological ecosystems [24], [25], [26].

5. Analysis of the Voluntary Involvement of IT Specialists in Urban Digital Strategies in Romania

According to official statistics published by the European Commission [27], Romania continues to rank below the European Union average in terms of digital skills and the use of digital public services. Only 28% of Romanian citizens possess basic digital skills, compared to the European average of 54%. Although Romania's connectivity infrastructure is among the most advanced in the European Union, the level of digital skills and the use of digital public services remain relatively low. In this context, local public administrations are required to identify additional mechanisms for strengthening digital administrative capacity, and collaboration with local innovation ecosystems and IT communities has become a strategically important resource.

The comparative analysis of Bucharest, Cluj-Napoca, Iași, and Timișoara demonstrates that urban digital transformation processes increasingly depend on technological expertise originating outside public administration. In most of the cases examined, local administrations have developed formal or informal mechanisms of collaboration with universities, IT communities, and professional organizations, particularly during the design of digitalization strategies and the implementation of smart city projects.

The involvement of IT specialists is expressed primarily through flexible and only partially institutionalized forms of collaboration, including thematic public consultations, informal working groups, civic hackathons, urban innovation laboratories, project-based partnerships for digital applications, open governance and open data platforms, as well as voluntary mentoring and technical advisory initiatives. These mechanisms provide local administrations with access to expertise and innovative solutions developed outside traditional bureaucratic structures.

5.1. Bucharest

In the absence of a unified digital transformation strategy at the level of the Municipality of Bucharest, the involvement of IT specialists in urban governance processes is manifested predominantly through civic initiatives, project-based interventions, and autonomous technological communities.

Although it is difficult to establish comprehensive statistics for such initiatives, the involvement of IT specialists within Bucharest's digital ecosystem occurs primarily through hackathon and GovTech events, which function as mechanisms of open innovation and temporary co-creation of digital solutions. The Code for Romania community represents a central actor within this ecosystem, mobilizing IT volunteers to develop civic applications and digital solutions for the public sector through collaborative and open-source approaches [24]. Complementing these efforts, the DevHacks hackathon provides a "24-hour hackathon" format in which software developers, students, and designers collaborate to generate digital solutions to social and urban challenges, explicitly focusing on the intersection between technology and society [25]. Similarly, VibeHack Bucharest promotes the rapid development of digital prototypes through the use of emerging technologies, including artificial intelligence and no-code tools, bringing together participants from diverse fields within a collaborative environment oriented toward experimentation and applied innovation [26]. These initiatives illustrate an emerging model of distributed urban innovation characterized by voluntary participation, co-creation, and interdisciplinary collaboration outside formal administrative structures.

5.2. Cluj-Napoca

The involvement of IT volunteers in Cluj-Napoca is manifested through a hybrid innovation ecosystem composed of civic hackathons, university initiatives, and informal technological communities. One example is Cluj Hackathon, which brings together software developers, students, and industry specialists to develop digital solutions aimed at public service digitalization and the resolution of urban challenges in areas such as digital administration, healthcare, and urban mobility [28]. Similarly, DevHacks functions as an intensive 24-hour hackathon focused on developing technological solutions for social and urban challenges, including smart cities and digital transformation, engaging interdisciplinary teams of programmers and designers within a civic-tech collaborative framework [29]. VibeHack also represents a digital innovation format focused on rapid prototyping, where participants—including developers, designers, and entrepreneurs—use AI-based tools and low-code platforms to develop experimental solutions emphasizing applied and iterative innovation [30].

In parallel, this ecosystem is supported by a collaborative governance model in which actors from the IT sector, academia, and public administration interact through institutionalized structures such as Cluj IT Cluster and dedicated working groups focused on smart city development [31], [32].

5.3. Iași

The involvement of IT specialists in urban digitalization initiatives in Iași is manifested through a collaborative ecosystem composed of technological communities, innovation initiatives, and projects associated with the smart city concept. A central element of this ecosystem is Iași Smart City, a platform that promotes urban digitalization projects and collaboration among local administration, academia, and the IT sector [33]. Complementing these efforts, the regional innovation ecosystem is supported by initiatives such as Fab Lab Iași, which brings together technological communities, civic organizations, entrepreneurs, and students through collaborative projects, hackathons, and open innovation initiatives [34].

5.4. Timișoara

In the municipality of Timișoara, the involvement of IT specialists in digital transformation processes is closely linked to the development of the Smart City and Digital Transformation Strategy of the Municipality of Timișoara [22]. The strategy development process included public consultation mechanisms and collaboration with actors from the local ecosystem, including IT companies, professional organizations, universities, and independent experts [35]. These initiatives indicate the existence of a consultative participatory framework in which local technical expertise contributes to shaping strategic directions for urban digitalization, without, however, involving institutionalized mechanisms of co-decision.

At the same time, the local innovation ecosystem is supported by initiatives such as HackTM and IT community networks, which facilitate collaboration among software developers, students, and entrepreneurs through hackathon events focused on developing digital solutions to urban and social challenges [36], [37]. These initiatives contribute to strengthening local innovation capital and mobilizing IT competencies within experimental civic-tech environments, yet they remain largely external to formal administrative mechanisms of urban governance.

5.5. Discussion

The study demonstrates that forms of participation and the degree of institutionalization of collaboration differ significantly among cities. Cluj-Napoca illustrates the most consolidated model of collaborative digital governance, whereas Bucharest remains characterized by fragmented civic-tech initiatives that operate largely outside formal institutional structures. Iași and Timișoara occupy intermediate positions, combining ecosystem-based innovation with strategic consultative collaboration.

This analysis does not seek to provide a comparative assessment of the level of digital transformation in Romania, a task made even more challenging by the absence of a standardized national framework for measuring the digital maturity of local administrations. Rather, the research highlights the growing importance of collaborative governance mechanisms in the context of urban digital transformation. In the Romanian cities examined, digital governance no longer depends exclusively on administrative apparatuses or internally available institutional expertise. Instead, local digital transformation increasingly relies on distributed forms of technological knowledge

generated within civic-tech communities, universities, innovation clusters, and professional networks.

6. Conclusions

This study examined the role of voluntary IT expertise in the development of urban digital transformation strategies in four major Romanian cities: Bucharest, Cluj-Napoca, Iași, and Timișoara. The comparative analysis demonstrates that local digital transformation processes increasingly depend on collaborative governance mechanisms involving public administrations, civic-tech communities, universities, and innovation ecosystems.

The analysis also indicates that the institutionalization of collaboration constitutes a critical factor influencing the sustainability and effectiveness of digital governance initiatives. Cities characterized by more structured forms of cooperation between administrations and technological ecosystems, such as Cluj-Napoca, exhibit greater continuity and coherence in the implementation of smart city strategies. By contrast, cities that rely predominantly on fragmented and informal civic-tech participation may generate innovative digital initiatives but encounter difficulties in ensuring long-term strategic integration.

At the same time, limitations associated with volunteer-based digital governance models must also be acknowledged. Although voluntary participation contributes to innovation and administrative flexibility, excessive dependence on informal expertise may generate institutional vulnerabilities. Volunteer initiatives are often project-oriented, temporary, and dependent upon fluctuating levels of civic engagement, which may reduce the predictability and continuity of public digital transformation processes. Furthermore, participation mechanisms may remain selective, primarily involving technologically skilled actors while limiting broader forms of civic inclusion.

The findings therefore support the argument that urban digital transformation requires not only technological modernization but also the development of institutional capacities capable of integrating collaborative expertise into stable governance frameworks. In this context, distributed digital governance emerges as a relevant conceptual perspective for understanding the evolving relationship among local administrations, technological communities, and urban innovation ecosystems.

From a theoretical perspective, this article contributes to the literature on collaborative governance and smart cities by providing an analysis of civic-tech participation mechanisms in urban governance in Romania. Building on the finding that voluntary IT expertise constitutes an important strategic resource for strengthening local administrative capacity and accelerating digital transformation processes, we argue that local administrations should develop more stable institutional frameworks for cooperation with technological communities, universities, and innovation actors.

Future research could extend the comparative analysis to other Romanian cities and investigate the perceptions of public officials, civic-tech actors, and citizens regarding the effectiveness and legitimacy of collaborative digital governance mechanisms.

References

- [1] United Nations, *Transforming Our World: The 2030 Agenda for Sustainable Development*, A/RES/70/1. New York, NY, USA: United Nations, 2015.
- [2] European Commission, *Next Steps for a Sustainable European Future: European Action for Sustainability*, COM(2016) 739 final. Brussels, Belgium: European Commission, 2016.
- [3] European Commission, *2030 Digital Compass: The European Way for the Digital Decade*, COM(2021) 118 final. Brussels, Belgium: European Commission, 2021.
- [4] Government of Romania, *National Action Plan for the Digital Decade for Romania*. Bucharest, Romania: Ministry of Research, Innovation and Digitalization, 2024. [Online]. Available: <https://www.mcid.gov.ro/wp-content/uploads/2024/04/Plan-national-de-actiune-roadmap-pentru-publicare.pdf>. Accessed: May 26, 2026.
- [5] C. Ansell and A. Gash, "Collaborative governance in theory and practice," *Journal of Public Administration Research and Theory*, vol. 18, no. 4, pp. 543–571, 2008.
- [6] R. Kitchin, "The real-time city? Big data and smart urbanism," *GeoJournal*, vol. 79, no. 1, pp. 1–14, 2014, doi: 10.1007/s10708-013-9516-8.
- [7] M. Deakin and H. Al Waer, "From intelligent to smart cities," *Intelligent Buildings International*, vol. 3, no. 3, pp. 140–152, 2011, doi: 10.1080/17508975.2011.586671.
- [8] M. P. Rodríguez Bolívar, Ed., *Smart Technologies for Smart Governments: Transparency, Efficiency and Organizational Issues*. Cham, Switzerland: Springer, 2018, doi: 10.1007/978-3-319-58577-2.
- [9] R. P. Dameri, "Searching for Smart City definition: A comprehensive proposal," *International Journal of Computers & Technology*, vol. 11, no. 5, pp. 2544–2551, 2013, doi: 10.24297/ijct.v11i5.1142.
- [10] T. Nam and T. A. Pardo, "Conceptualizing smart city with dimensions of technology, people, and institutions," in *Proc. 12th Annual International Digital Government Research Conference*, 2011, pp. 282–291.
- [11] S. Goldsmith and S. Crawford, *The Responsive City: Engaging Communities Through Data-Smart Governance*. San Francisco, CA, USA: Jossey-Bass, 2014.
- [12] S. A. M. Dolmans, W. P. L. van Galen, B. Walrave, E. den Ouden, R. Valkenburg, and A. G. L. Romme, "A dynamic perspective on collaborative innovation for smart city development: The role of uncertainty, governance, and institutional logics," 2023. doi: 10.1177/01708406231169422.
- [13] J. Alford, *Engaging Public Sector Clients: From Service Delivery to Co-production*. London, UK: Palgrave Macmillan, 2009.
- [14] N. Haug and I. Mergel, "Public value co-creation in living labs—Results from three case studies," *Administrative Sciences*, vol. 11, no. 3, Art. no. 74, 2021, doi: 10.3390/admsci11030074.
- [15] I. H. Mahmoud, E. Morello, D. Ludlow, and G. Salvia, "Co-creation pathways to inform shared governance of urban living labs in practice: Lessons from three European projects," *Frontiers in Sustainable Cities*, vol. 3, Art. no. 690458, pp. 1–17, 2021, doi: 10.3389/frsc.2021.690458.
- [16] E. M. Leclercq and E. A. Rijshouwer, "Enabling citizens' Right to the Smart City through the co-creation of digital platforms," *Urban Transformations*, vol. 4, Art. no. 2, 2022, doi: 10.1186/s42854-022-00030-y.
- [17] M. Gascó-Hernandez, G. Nasi, M. Cucciniello, and A. M. Hiedemann, "The role of organizational capacity to foster digital transformation in local governments: The case of three European smart cities," *Urban Governance*, vol. 2, no. 2, pp. 236–246, 2022, doi: 10.1016/j.ugj.2022.09.005.
- [18] P.-A. Balland, C. Jara-Figueroa, S. G. Petralia, M. P. A. Steijn, D. L. Rigby, and C. A. Hidalgo, "Complex economic activities concentrate in large cities," *Nature Human Behaviour*, vol. 4, no. 3, pp. 248–254, 2020, doi: 10.1038/s41562-019-0803-3.
- [19] H. W. Chesbrough, *Open Innovation: The New Imperative for Creating and Profiting from Technology*. Boston, MA, USA: Harvard Business School Press, 2003.
- [20] B. S. Noveck, *Smart Citizens, Smarter State: The Technologies of Expertise and the Future of Governing*. Cambridge, MA, USA: Harvard University Press, 2015.
- [21] Cluj-Napoca City Hall, *Cluj-Napoca Digital Transformation and Smart City Strategy 2021–2030*. Cluj-Napoca, Romania, 2021.
- [22] Timișoara City Hall, *Timișoara Smart City and Digital Transformation Strategy*. Timișoara, Romania, 2022.

- [23] Iași Smart City, *Iași Smart City Digital Transformation Strategy*. [Online]. Available: <https://iasismartcity.ro/>. Accessed: May 27, 2026.
- [24] Code for Romania, *The Infrastructure for Good*. [Online]. Available: <https://code4.ro/ro/>. Accessed: May 31, 2026.
- [25] DevHacks Romania, “About DevHacks – 24h Hackathon.” [Online]. Available: <https://devhacks.devtalks.ro/about>. Accessed: May 27, 2026.
- [26] VibeHack, “Bucharest Hackathon – AI & Innovation Event.” [Online]. Available: <https://vibehack.eu/>. Accessed: May 27, 2026.
- [27] European Commission, *Country Reports – Digital Decade Report 2023*. Brussels, Belgium: European Commission, 2023. [Online]. Available: <https://digital-strategy.ec.europa.eu/en/library/country-reports-digital-decade-report-2023>. Accessed: May 28, 2026.
- [28] Cluj Hackathon, “Digital Romania / Smart City Innovation Challenge.” [Online]. Available: <https://www.clujhackathon.ro/>. Accessed: May 28, 2026.
- [29] DevHacks Romania, “24h Coding Challenge for Social Impact.” [Online]. Available: <https://devhacks.devtalks.ro/>. Accessed: May 28, 2026.
- [30] VibeHack, “AI-Powered Hackathon for Rapid Prototyping and Innovation.” [Online]. Available: <https://vibehack.eu/>. Accessed: May 28, 2026.
- [31] Cluj IT Cluster, “Innovation Ecosystem in IT&C.” [Online]. Available: <https://www.clujit.ro/>. Accessed: May 28, 2026.
- [32] Cluj IT Cluster, “Working Groups – Smart City.” [Online]. Available: <https://www.clujit.ro/working-groups/>. Accessed: May 28, 2026.
- [33] Iași Smart City, “Iași Smart City.” [Online]. Available: <https://iasismartcity.ro/>. Accessed: May 26, 2026.
- [34] Fab Lab Iași, “Ecosystem.” [Online]. Available: <https://fablabiasi.ro/ecosystem/>. Accessed: May 26, 2026.
- [35] Timișoara City Hall, *Timișoara Smart City and Digital Transformation Strategy 2022–2027*, approved by Local Council Decision No. 302/30.06.2022. [Online]. Available: <https://hcl.usr.ro/timisoara/2022/h302>. Accessed: May 29, 2026.
- [36] HackTM, “HackTM.” [Online]. Available: <https://hacktm.ro/>. Accessed: May 29, 2026.
- [37] Banat IT, “HackTM Project.” [Online]. Available: <https://banatit.ro/projects/hacktm/>. Accessed: May 29, 2026.

Enhancing Decision-Making Transparency through E-Participation

Florentina Pană-Micu

Faculty of Public Administration,

National University of Political Studies and Public Administration

Bucharest, Romania

florentina.micu@snspp.ro

Abstract

This article explores how e-participation platforms enhance transparency in public administration decision-making. With the ongoing digitalization of public institutions, these platforms enable citizens to participate actively in the decision-making process, from policy implementation to practical application. Consequently, citizens become engaged stakeholders, influencing how decisions are made at the administrative level. The research focuses on studying the main tools of citizen participation, assessing the level of digital engagement among citizens, and identifying the barriers encountered during implementation. Furthermore, the study analyses the concepts of decision-making transparency and e-participation. It evaluates the relationship between citizens' digital participation in decision-making and the overall transparency of public institutions.

Keywords: e-participation, transparency, decision-making, public administration, digital governance.

1. Introduction

Nowadays, amid discussions about digitalization and artificial intelligence, public administration is undergoing a paradigm shift towards open and participatory governance. Thus, the citizen becomes an active actor in the decision-making process. Transparency and e-participation are complementary concepts, both closely linked to administrative democracy.

The shift towards participatory governance is based on two fundamental dimensions: transparency in decision-making and citizen involvement. In the past, transparency was often limited to formal procedural obligations, and public access to relevant information was restricted. In the digital era, these limitations can be overcome through technological tools that facilitate direct communication between citizens and authorities, reducing information gaps and strengthening public trust in state institutions.

The main objective of this research is to highlight how e-participation can be used as an effective mechanism for increasing transparency in public administration, through an analysis of best practices at the European level and their applicability in Romania.

E-governance involves more than just implementing information systems; it requires transforming the way public administration thinks and acts. Institutions must adopt a proactive approach, be open to citizen feedback, ensure easy access to public data, and create mechanisms to integrate citizens' opinions and suggestions into decision-making effectively. This change also requires the development of digital skills at both the

institutional and citizen levels, so that electronic participation becomes relevant and efficient.

2. Literature review

Transparency in the decision-making process can be effectively achieved only when participatory and deliberative forms of democracy operate together within the institutional framework of representative democracy. [1] Even in representative systems, democratic deficits may persist, particularly when deliberative processes lack consistency or transparency, and opportunities for public involvement are limited.

On the other hand, Tero Erkkila, in the paper “Transparency in Public Administration”, considers that transparency is one of the keywords of contemporary governance. [2]

Public authorities and institutions are obliged to inform citizens, consult them, and involve them in public debates regarding draft normative acts, as well as to provide access to the administrative decision-making process and public-interest data and information, within the limits established by law. [1]

Deepak Kumar, in the article “The Making of Smart Citizenry: Decoding ‘Smart Citizen’”, argues that digital participation cannot achieve real decision-making transparency without creating a social and institutional environment that encourages informed engagement. Kumar highlights that a “smart citizen” results from access to clear, understandable, and up-to-date public data as an essential condition for increasing transparency and administrative accountability. [3]

Transparency in public administration has a significant impact on the reform process of public governance. It contributes to increasing efficiency, effectiveness, and responsiveness, core components of the concept of “good administration”. In this regard, transparency in public administration is strengthened through the use of modern information and communication technologies. Thus, the modernization and digitalization of public administration are considered essential factors in governmental transformation, guiding institutions toward greater transparency and open access to information. [4]

E-participation refers to the use of information and communication technologies (ICT) to facilitate citizen involvement in public decision-making processes. This concept lies at the intersection of transparency, civic participation, and good governance, offering modern tools that enable public administration to become more open and accountable.

According to the literature, e-participation can be analysed across three essential levels:

- Information (citizens are granted access to relevant information regarding policies, legislative proposals, and administrative decisions. This includes publishing

documents, reports, statistics, and standardized government data, enabling the public to understand decision-making processes.

- Consultation (public authorities seek opinions, suggestions, or comments from citizens on proposed decisions or policies. Consultation can take place through digital feedback platforms, online surveys, public debates, or specialized forums.
- Active engagement (citizens effectively participate in the formulation and evaluation of public policies, influencing final decisions through mechanisms such as digital participatory budgeting, co-creation of regulatory proposals, or electronic voting for public policy priorities). [5]

E-participation not only enhances transparency in decision-making but also strengthens public trust in the administration. Studies show that providing clear, accessible information, combined with consultation mechanisms, increases citizens' perceptions of transparency and performance.

On the other hand, Portal and Fabrègue show that decision-making transparency is directly proportional to the level of citizen involvement in defining public priorities, and that digital technologies can transform these processes only if they are designed to facilitate participation and enhance the accountability of public authorities. [6]

For example, the study "Transparency and Trust in Government: Evidence from a Survey Experiment" by Alessandro et al. [7] shows that active information provision increases citizens' perceptions of government transparency by approximately eight percentage points. The content of the message matters more than its presentation: citizens place greater trust in government when its performance exceeds expectations, regardless of whether the message emphasizes efficiency or empathy.

The OECD Public Integrity Indicators on government information transparency assess both the normative framework and its practical implementation. On average, OECD countries comply with 66% of the criteria related to the normative framework and 62% of those related to implementation. For instance, almost all OECD governments publish the national budget and consolidated primary legislation, but fewer than half publish ministers' agendas or asset declarations of senior officials. [55]

According to Romanian legislation, transparency in public administration entails the obligation to publicly communicate administrative decisions, ensuring easy access to information for interested members of the public and facilitating the participation of all stakeholders, including through inclusive measures where necessary. [1]

These studies highlight the importance of combining transparency in decision-making with e-participation mechanisms to strengthen citizens' trust and improve governance effectiveness. Digital public consultation platforms enable citizens to influence decision-making and monitor its implementation, thereby contributing to an open and accountable administration.

Moreover, implementing e-participation requires a cultural and organizational shift within public institutions that promotes collaboration and values citizens' contributions.

In conclusion, e-participation is a key instrument of modern governance, integrating transparency, accountability, and civic participation into a digital framework. Its effective adoption contributes to a more open, accountable, and efficient public administration, reinforcing the relationship between authorities and citizens.

3. E-Participation and Transparency in Public Administration: International Indicators and Romania's Progress

To grasp how countries perform in this digital transition, analysts and policymakers rely on robust indicators. Among the most important are the Digital Economy and Society Index (DESI), the United Nations (UN) E-Government Development Index (EGDI), and the digital government metrics used by the Organisation for Economic Co-operation and Development (OECD). These indicators offer a comprehensive view of how well public services have been digitalized, how capable citizens are of using digital tools, and to what extent governments are open and responsive.

According to the European Commission's 2024 Digital Decade Country Report, Romania has achieved significant progress in the digitalization of public services and in supporting SMEs through digital tools. However, challenges remain in enhancing citizens' basic digital skills and in deploying 5G networks. At the same time, Romania demonstrates strong performance in implementing fibre-to-the-premises (FTTP) infrastructure, ensuring high-speed broadband access to a large part of the population. This progress highlights the potential for increased digital engagement and e-participation, although gaps in digital literacy and mobile connectivity still limit the full use of online public services. [9]

On the other hand, according to the UN E-Government Knowledgebase, Romania's 2024 E-Government Development Index (EGDI) stands at 0.7636, while its E-Participation Index (EPART) is 0.6849, placing the country in the 'Very High EGDI' class, subgroup V1. However, despite this structural readiness, the downward shift in ranking compared to 2022 suggests that the pace of e-governance adoption and citizen engagement remains uneven. [57]

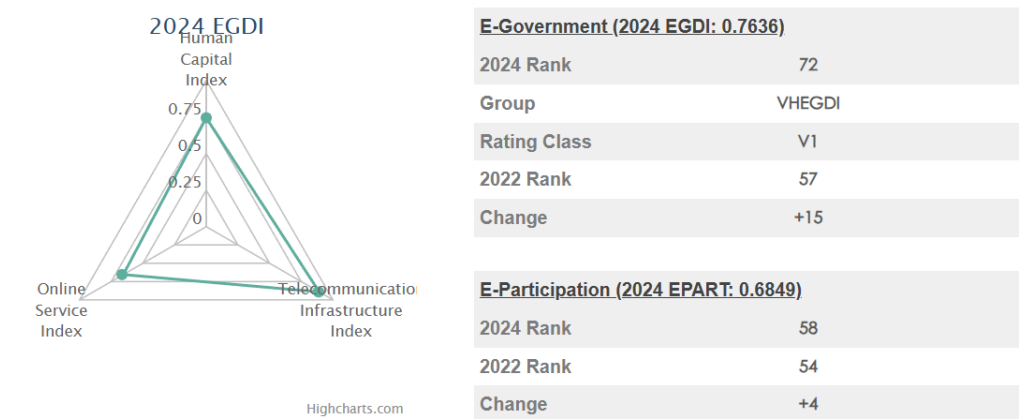


Fig.1. E-Government Development Index (EGDI) și E-Participation Index (EPART) pentru România, 2024

Source: [57]

E-Government Development Index	2024	2022	2020	2018	2016	2014	2012	2010	2008	2005	2004	2003
Romania (Rank)	72	57	55	67	75	64	62	47	51	44	38	50
Romania (Value)	0.76364	0.76190	0.76050	0.66710	0.56114	0.56315	0.60595	0.54791	0.53830	0.57040	0.55035	0.48278

Fig.2. E-Government Development Index over time

Source: [57]

OECD’s recent analysis, compiled in the 2023 Digital Government Review of Romania, reveals that connectivity and basic digital infrastructure in many parts of the country are improving. Still, citizen use of digital public services lags. The report highlights a significant digital skills deficit: only a fraction of the population possesses the basic competencies needed to navigate e-services effectively. [58]

As observed from various indicators, Romania needs to take intermediate steps to strengthen e-participation. Transforming it from a passive technological convenience into an active democratic mechanism requires more than just technology. Efforts should focus on improving digital literacy across all segments of the population, designing intuitive, accessible, user-friendly platforms, and fostering a participatory culture where citizen feedback is genuinely considered, and results are communicated, ensuring meaningful engagement and reinforcing trust in institutions.

Despite these challenges, Romania has established vital infrastructure to support e-participation. To fully harness the potential of e-participation in Romania, several strategic measures are recommended:

- Promotional campaigns for e-governance platforms should be implemented at both local and national levels to increase awareness and encourage citizen participation;

- Digital literacy programs must target vulnerable groups to ensure that all citizens have the necessary skills to engage effectively with e-government services;
- Institutional feedback mechanisms should be developed to gather citizen input and continuously improve public services;
- Expanding access to high-speed internet and digital devices, especially in underserved regions, is essential to create equitable opportunities for e-participation;
- Platforms must be intuitive, accessible on multiple devices, and inclusive;
- Authorities should monitor participation rates, evaluate the impact of citizen input, and report any legislative or policy changes resulting from consultations to assess effectiveness;
- Public institutions must foster a participatory culture in which citizen contributions are valued and incorporated into decision-making;
- E-participation should not operate as a standalone initiative but should be integrated into broader governance reforms, connecting digital services, civic engagement, and open government objectives.

By implementing these measures, Romania can transform e-participation from a theoretical concept into a practical tool that strengthens transparency, accountability, and efficiency in public administration. Over time, a combination of digital infrastructure, literacy, institutional commitment, and active citizen engagement can foster a modern, responsive, and inclusive governance model, one where citizens are genuinely empowered to shape the policies that affect their lives.

4. Conclusions

E-participation represents a transformative approach to governance, enabling citizens to move from passive recipients of public services to active participants in decision-making. As this study has highlighted, transparency and citizen engagement are inseparable components of modern public administration. While Romania has made progress in developing digital platforms, real citizen involvement remains limited due to barriers including digital skill gaps, uneven infrastructure, cultural perceptions of formal consultations, and insufficient promotion of participatory tools.

Despite these challenges, the potential of e-participation to enhance transparency, accountability, and public trust is significant. When citizen feedback is genuinely considered and institutional responses are consistent, digital platforms provide mechanisms for monitoring legislative initiatives, reporting discrepancies, and fostering a culture of public oversight. The effective combination of digital literacy programs, infrastructure development, the promotion of participatory platforms, and institutional commitment can transform e-participation into a powerful mechanism for democratic engagement.

Strategically, Romania must focus on several key areas to realize this potential. These include actively promoting digital platforms, investing in digital skills, ensuring user-friendly and inclusive tool design, integrating citizen feedback into decision-making, monitoring participation and outcomes, and embedding e-participation within broader governance reforms. A cultural and organizational shift is essential, where public institutions recognize the value of citizen contributions and leadership commits to sustained engagement.

In conclusion, e-participation is not merely a technical innovation but a pathway to open, accountable, and responsive governance. By addressing structural, cultural, and technological barriers, Romania can foster a digital environment in which citizens are empowered, institutions are more transparent, and decision-making is more participatory and legitimate.

References

- [1] A. Androniceanu, "Transparency in public administration as a challenge for a good," *Administratie si Management Public*, vol. 36, 2021.
- [2] T. Erkkila, "Transparency in Public Administration," 2020.
- [3] D. Kumar, "The Making of Smart Citizenry: Decoding 'Smart Citizen'," *Smart Cities and Regional Development (SCRD)*, vol. 7, no. 2, 2023.
- [4] M. Jashari and I. Pepaj, "The Role of Transparency in Public Administration Reform: Enhancing Efficiency, Effectiveness and Responsiveness through ICT," *Journal of Public Administration and Governance*, vol. 8, no. 2, p. 45–58, 2018.
- [5] OECD, "The e-Government Imperative," OECD Publishing, 2003.
- [6] L. Portal and B. Fabregue, "Establishing participative Smart Cities: theory and practice," *Smart Cities and Regional Development (SCRD)*, vol. 6, no. 2, 2022.
- [7] B. C. L. C. S. J. S. ş. J. T. M. Alessandro, "Transparency and Trust in Government: Evidence from a Survey Experiment," *World Development*, vol. 138, 2021.
- [8] OECD, "Government at a Glance 2021: Public Integrity Indicators," OECD Publishing, 2021.
- [9] European Commission, "Romania 2024 Digital Decade Country Report," 2024.
- [10] United Nations, "Country Information: Romania, UN E-Government Knowledgebase," 2024.
- [11] OECD, "Digital Government Review," OECD Publishing, 2023.

The role of artificial intelligence in ensuring cyber security in the concept of smart cities of Ukraine

Olha Naumenko

*Kyiv National Economic University Named After Vadym Hetman, Kyiv, Ukraine
naumenko.olha@kneu.edu.ua*

Abstract

Objectives: To explore opportunities and challenges regarding the role of artificial intelligence in ensuring cyber security in the concept of Smart Cities of Ukraine with the aim of their further improvement. The tasks of the research relate to the definition and essence of artificial intelligence as an element of cyber security of Smart Cities of Ukraine for the purpose of automating threats; description of the main Ukrainian cities regarding the development of Smart technologies, such as: Kyiv, Dnipro, Lviv, Kharkiv and others; systematization of the main directions of Smart Cities in Ukraine. The development of artificial intelligence in cyber security is important for Ukraine to strengthen security measures to protect against various cyber threats and improve the support of Ukraine's Smart Cities both during the war and during the recovery of the country. **Prior work:** The research is focused the study on the concept of Smart Cities in the context of the role of artificial intelligence in ensuring cyber security in Ukraine; research by Ukrainian and foreign scientists on the concept of Smart Cities and the application of foreign experience in providing effective artificial intelligence algorithms in ensuring cyber security for Ukraine. **Approach:** To collect practical evidence, such approaches as observations on the artificial intelligence in ensuring cyber security for the concept of Smart Cities are used to collect practical evidence. For the evidence of the research, a comparative approach is used regarding such areas of Smart Cities in Ukraine as e-democracy and e-governance to collect and analyze qualitative data based on case studies. **Results:** An analysis and generalization of the role of artificial intelligence in ensuring cyber security in the concept of Smart Cities of Ukraine, comparing the best practices of e-democracy and e-governance abroad with their introduction in Ukraine and the application of foreign experience in Ukrainian realities. **Implications:** The study has practical and theoretical significance regarding the role of artificial intelligence in ensuring cyber security in the concept of Smart Cities of Ukraine for academics, researchers and practitioners. **Value:** It consists in the original experience of the development of artificial intelligence in ensuring cyber security in the concept of Smart Cities of Ukraine before the war and during the legal regime of martial law.

Keywords: artificial intelligence, cyber security, the concept of «Smart City», e-democracy, e-governance.

1. Introduction

Today, the significant development of digital technologies is combined with new opportunities for society and new threats. A significant place among the threats is occupied by cyber threats, which create risks not only for individual users, but also for strategic sectors of the economy, defense and public administration. Currently, the significant weight of cyber threats is growing, and this trend will increase with the development of information technologies and their convergence with artificial intelligence technologies in the coming decades. In the aspect of combating threats, the role of artificial intelligence is growing, which makes it possible to: automate data analysis processes, detect anomalies, predict and respond to cyber attacks. According to experts, the importance of artificial intelligence in cyber security will increase significantly in the future [1].

Under the conditions of digital transformation, artificial intelligence plays a key role in the management processes of local communities. The use of intelligent systems stimulates the improvement of the efficiency of decision-making, optimization of administrative processes, improvement of communication between the authorities and citizens, and

ensuring the transparency of management. As world experience shows, the digitization of city management is a necessary condition for the sustainable growth of territorial communities. At the same time, the integration of artificial intelligence into management processes is associated with a number of challenges, such as ethical aspects, the database and the readiness of local authorities to use the latest technologies.

Despite the great potential of artificial intelligence in the field of local community management, there are a number of unresolved issues regarding the insufficient development of mechanisms for adapting artificial intelligence to the specifics of local government, the presence of problems with digital infrastructure and the level of digital literacy of local government personnel. Issues of security, data privacy and legal regulation of the use of artificial intelligence in local systems are relevant [2].

2. Research methodology

Approaches such as observing the process of artificial intelligence in ensuring cyber security for the concept of Smart Cities are used to collect practical evidence. For the evidence of the research, a comparative approach is used regarding such areas of Smart Cities in Ukraine as e-democracy and e-governance to collect and analyze qualitative data based on case studies.

3. The role of artificial intelligence in ensuring cyber security in the concept of Smart Cities of Ukraine

3.1. Smart technologies in the concept "Smart City"

The use of artificial intelligence in the management of local communities shows a significant interest in studying the use of the latest technologies to increase efficiency and transparency in management processes at the local level.

An important research is the integration of artificial intelligence into the e-government system, namely: the development of chatbots for communication with residents, the automation of the processing of citizen requests, the introduction of forecasting systems for the management of urban transport, waste processing and energy resources [2].

The rapid development of electronic means, the reduction of their cost and their distribution in an increasing number of different spheres, has formed the hope that they will be able to solve existing urban problems.

The British Standards Institution (BSI) describes a Smart City as "the effective integration of physical, digital and human systems in an artificially created environment to ensure a sustainable, prosperous and inclusive future for citizens".

The experience of using smart technologies has formed a conditional "Smart City standard", the implementation of which involves the implementation of the following programs: electronic government (city management); a favorable environment for innovative activity; intelligent systems of public security and control; development of the infrastructure of networks and means of communication; intelligent housing and communal

management; Smart City transport; intelligent environmental safety systems; clean (green) energy; zero level of waste; promotion of tourism and service.

At the same time, it is planned to increase management capabilities, reduce unproductive costs and free up residents' time [3].

Romanian scientist C. Sirbu defines cyber security as a set of rules, technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks. Noting that cyber security plays an important role in the field of information technology, where the protection of information has become one of the biggest challenges of today [4].

As noted by Moldovan scientists A. Babin, S. Tutunaru, I. Covalenko, in the context of rapid digital transformation, both urban and rural communities are revising their development strategies by implementing intelligent technologies aimed at increasing sustainability, engagement and security. Considers a comprehensive framework for promoting Smart Cities and Smart Villages, with a special emphasis on cyber security as a fundamental basis for socio-technical sustainability [5].

Moroccan scientists H. Ait Bakader, N. I. Bedoui point out that the integration of artificial intelligence (AI) into Smart Cities and human resource management (HRM) significantly changes the process of organizational decision-making, creating both significant opportunities and complex ethical issues [6].

3.2. The essence of artificial intelligence as an element of cyber security of Smart Cities of Ukraine

In accordance with the Cybersecurity Strategy of Ukraine dated August 26, 2021 №. 447, it is stated regarding cyber security in the global context that "ensuring cyber security is one of the priorities in the national security system of Ukraine. The implementation of the specified priority will be carried out by strengthening the capabilities of the national cyber security system to counter cyber threats in the modern security environment. The 21st century is marked by the active formation of the sixth technological order and the risks that civilization faces as a result of the introduction of the latest technologies."

It is noted that the threats to Ukraine's cyber security are: hybrid aggression of the Russian Federation against Ukraine in cyberspace; cybercrime, which damages information resources, social processes, and individual citizens, reduces public trust in information technologies and leads to significant material losses; cyberattacks organized and sponsored by the governments of other states, related to the theft of sensitive information for political, economic or military purposes (cyberespionage) and the implementation of intelligence and subversive activities; use of cyberspace by terrorist organizations to commit acts of cyberterrorism, financial and other support for terrorist activities.

In particular, with regard to the hybrid aggression of the Russian Federation, the aggressor state is constantly expanding its arsenal of offensive cyber weapons, the use of which can have irreparable and irreversible destructive consequences. Cyberattacks of the aggressor country are aimed at the information and communication systems of state bodies of Ukraine

and critical infrastructure objects with the aim of disabling them, and the use of cyberattacks by the aggressor state as an element of special information operations for the purpose of manipulative influence on the population, interference in election processes and discrediting Ukrainian statehood [7].

In the field of cyber security, artificial intelligence is used to: detect anomalies in network traffic; automatic analysis of events in cyberspace; protection against unauthorized access to information resources; analysis and structuring of information about cyber threats; responding to cyber incidents in real time; prediction of cyber attacks based on the analysis of large data sets; development of advanced algorithms that help detect cyberattacks and prevent their negative manifestations; machine learning according to acquired experience.

To detect anomalies in network traffic, artificial intelligence uses neural networks to analyze the network and detect malware. These systems are able to quickly identify abnormal actions in network traffic, which can indicate attempts to invade or infect the system with viruses. Neural networks help identify threats in large information systems and provide real-time response.

Detection of anomalous behavior consists in the formation of signs according to which user actions are malicious for normal protection systems. When some of these signs coincide, the system registers an intrusion, while artificial intelligence is able to identify parameters that were not taken into account before. This provides an opportunity to form a more effective predicative model. Artificial intelligence is used to create models capable of identifying suspicious activity on the network.

As for the detection of unauthorized research of an information resource, artificial intelligence systems automatically detect malicious code or unspecified Internet traffic and react to unusual user behavior, for which malicious software is actively used.

Risk identification is key to predicting AI in cybersecurity. Artificial intelligence is capable of analyzing network changes and applying these patterns to predict potential cyber attack vectors based on historical data, primarily the methods and ways that cyber attackers can use to access the system or networks.

The use of artificial intelligence has the following advantages: high data processing speed; the ability to simultaneously analyze a large number of factors; autonomous response to threats without human intervention; availability of self-learning mechanisms; forecasting cyber risks.

The significance of the risks of using artificial intelligence is determined by: a high dependence on the quality of training data; manipulation and other criminal actions by hackers (adversarial attacks); problems with explaining artificial intelligence solutions (black box problem); violation of the right to privacy and protection of personal data; ethical issues related to autonomous systems [1].

Ukrainian scientist R. A. Krytskyi provides the main directions of using artificial intelligence in the management of local communities: automation of administrative processes, smart urban planning and infrastructure management, improvement of communication with citizens, support for decision-making, security and crisis management, development of electronic governance [2].

The main directions of Smart Cities in Ukraine are: electronic democracy: the use of electronic petitions and participatory budgets (public budget); mobility and transport: "smart" stops with scoreboards and cashless fare payment; electronic governance: creation of Centers for the provision of administrative services, automation of document processing and transfer of references online; energy efficiency: modernization of street lighting, automated heating points in residential buildings and resource consumption monitoring systems.

With the support of Switzerland, 12 Ukrainian cities were given the opportunity to improve the quality of life of their residents, making the Cities Smart and comfortable for everyone: Kovel, Volodymyr, Novovolynsk, Nizhyn, Pryluky, Romny, Starokostyantyniv, Kamianets-Podilskyi, Samar, Zhovti Vody, Podilsk, Chornomorsk. These cities will be able to implement "smart" lighting systems, digital services for utility payments, video surveillance, environmental monitoring and "smart" public transport.

Financing of this program in Ukraine is carried out with the support of Switzerland through the Eastern Europe Fund, in cooperation with the Ministry of Digital Transformation of Ukraine and the Innovabridge Fund.

The implementation of IoT (Internet of Things), AI (Artificial Intelligence), and Big Data is expected to manage urban infrastructure, which will help reduce costs, make cities comfortable to live in, and improve the quality of services [8].

For Ukraine, the introduction of Smart City consists in educating local self-government leaders in the skills of designing and implementing digital initiatives. The purpose of Smart City is to promote the improvement of the quality of life and optimization of the processes of obtaining, distributing, using and utilizing resources. The tasks of Smart City are: improving the quality of public space; coordination of group spaces within the framework of public space; improving the quality of group spaces depending on their specifics.

The concept of Smart City is a model of the city with the use of digital technologies to solve the current problems of the city, its sustainable development and the comfortable life of citizens [3].

The idea of a Smart City combines various innovative tools, with the help of which each city can choose an individual solution to problems, which is helped by the "Internet of Things" technology, which is able to monitor various objects and analyze their condition.

The Internet of Things (IoT) is a network of physical objects that have built-in technologies and enable interaction with the external environment, transmitting information about their

state and receiving data from the outside. These sensors help control lighting in the city by turning on street lights automatically when it gets dark outside.

In Ukraine, 2015 was the beginning of the introduction of Smart City in Kyiv. Until 2021, such digital services as: signature of electronic petitions, registration of a child for kindergarten, appointment to a family doctor, participation budget, video surveillance system and determination of license plates of cars that violate traffic rules were introduced in Kyiv.

Residents of Kyiv receive a free municipal "Card of a Kyivan", which entitles them to benefits, access to electronic services through an electronic cabinet, and online payment of utility bills. There is an application "Kyiv Digital" through which you can pay for parking, receive notifications about road repairs and utility services. Kyiv public transport is equipped with GPS trackers.

Thanks to the capabilities of mobile operators, such smart innovations are also available in other cities of Ukraine. In Mariupol: SmartTicketCity automated fare payment was launched in public transport even before the full-scale war [9].

In some cities, the "Safe City" system functions as video surveillance cameras with recognition of license plates and faces. In Kyiv, Vinnytsia, and Lviv, the Smart Lighting system (LED lamps with motion sensors) is operating, and Smart Grid pilot projects have been launched to distribute electricity and connect renewable sources.

The application "Diia" has been a significant success in Ukraine, which has made most public services available online, allowing you to vote, sign petitions and interact with the state.

The full implementation of the concept is held back by the following factors: lack of a strategic vision regarding clearly defined plans for the development of Smart solutions; lack of financing, which also depends on business and investors; lack of specialists; cyberattacks and security issues, the risk of which increases due to war, threatening the digital infrastructure of cities [10].

Dnipro: the city platform "eDnipro" for solving communal issues and appeals, and the system "Safe Dnipro", which is based on video surveillance cameras, are functioning.

Lviv: the project "Data-Driven Governance" made it to the finals of the prestigious World Smart City Award 2025. This award is given to cities that use technology to improve the lives of residents [11].

Kharkiv: despite its proximity to the front, it is developing the concept of Smart City, including the security direction of law and order control.

3.3. Best practices of e-democracy and e-governance: foreign experience of digital technologies

The application of foreign experience of electronic democracy and electronic governance in Ukrainian realities is carried out taking into account the foreign experience of digital technologies.

The main problems of the development of artificial intelligence in Ukraine reasonably include: low level of digital literacy, awareness of the population regarding the main aspects, opportunities, risks and safety of the use of artificial intelligence; lack or imperfection of legal regulation of artificial intelligence (in the spheres of public administration, economy, education, defense, cyber security), and imperfection of legislation on the protection of personal data; low level of investment in the development of artificial intelligence technologies; insufficient level of information security and data protection in the information and telecommunication systems of state bodies due to outdated automatic systems for detecting and assessing information threats; an increase in the number of attempts at unauthorized intervention in the operation of automated systems and computer networks; the presence of risks of an increase in the level of unemployment associated with the use of artificial intelligence technologies [1].

An example of a successful introduction of e-government at the local level of the Smart City concept is the experience of the large cities of the United Arab Emirates – Abu Dhabi and Dubai. For example, citizens in Abu Dhabi can access the local government's online portal to use various electronic services. Some additional services are provided through the Abu Dhabi Portal, including viewing and changing personal profile information such as address and number plate [8; 3].

A positive example of the successful introduction of electronic democracy is the experience of Denmark, where the following services were launched: Internet conferences, electronic appeals, online blogs of heads of public authorities. Denmark's experience is useful for the introduction of e-democracy in Ukraine.

It is advisable to take into account the peculiarities and methods of introducing electronic democracy in Great Britain, Spain, Italy, Finland, Switzerland, Belgium, the Netherlands, Estonia, Poland [12].

4. Conclusion

The study has practical and theoretical implications for the development of e-government and digital technologies for scholars and practitioners.

War is a catalyst for innovation. Restoration of destroyed cities helps to build them anew, taking into account modern technologies. This approach will make Ukraine more competitive and attractive for investors. The concept of a Smart City is not only a convenience, but a strategic need that will help Ukraine to be a leader in the field of innovation on a global scale. As for development prospects, it is the development of security solutions, such as automated shelters, autonomous warning systems [10].

The cyber security of Smart Cities must take into account and control the available risks. Therefore, a real Smart City must be safe.

References

- [1] O.S. Fedorchenko, “The role of artificial intelligence in ensuring cyber security of Ukraine: current state and development prospects.,” *Information and law*, no. 3 (54), 2025. pp. 139–146. [Online]. Available: ORCID: <https://orcid.org/0009-0007-7358-7753>
- [2] R. A. Krytskiy, “The role of artificial intelligence in the conditions of digital transformation of local community management.,” *Electronic magazine “Public administration: improvement and development”*, no. 6, 2025. pp. 1–21. [Online]. Available: <http://doi.org/10.32702/2307-2156.2025.6.10>
- [3] “What is a Smart City?,” *Public space*. [Online]. Available: <https://www.prostir.ua/?news=scho-take-smart-city#:~:text=%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D1%96%D1%8F%20%D1%81%D0%BC%D0%B0%D1%80%D1%82%2D%D1%81%D1%96%D1%82%D1%96%20%D1%94%20%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D0%BB%D1%8E,%D1%80%D0%BE%D0%B7%D0%B2%D0%B8%D1%82%D0%BA%D1%83%20%D1%82%D0%B0%20%D0%BA%D0%BE%D0%BC%D1%84%D0%BE%D1%80%D1%82%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%B6%D0%B8%D1%82%D1%82%D1%8F%20%D0%B3%D1%80%D0%BE%D0%BC%D0%B0%D0%B4%D1%8F%D0%BD>. [Accessed 01 June 2026].
- [4] C. Sirbu, “Cybersecurity, the challenge of the present.,” *Machine Intelligence & Security for Smart Cities (TRUST). Ensuring Trust and Security in Intelligent Urban Ecosystems*, vol. 2 (2025). pp. 25–28. [Online]. Available: <https://scrd.eu/index.php/trust/article/view/740/772>. [Accessed 01 June 2026].
- [5] A. Babin, S. Tutunaru, I. Covalenko, “Cybersecurity and smart innovation for rural resilience: Moldova’s strategic transition to green and digital villages.,” *Machine Intelligence & Security for Smart Cities (TRUST). Ensuring Trust and Security in Intelligent Urban Ecosystems*, vol. 2 (2025). pp. 75–95. [Online]. Available: <https://www.scrd.eu/index.php/trust/article/view/745/777>. [Accessed 01 June 2026].
- [6] H. Ait Bakader, N. I. Bedoui, “Smart cities, smarter decisions: The algorithmic governance of human resource management.,” *Machine Intelligence & Security for Smart Cities (TRUST). Ensuring Trust and Security in Intelligent Urban Ecosystems*, vol. 2 (2025). pp. 211–217. [Online]. Available: <https://www.scrd.eu/index.php/trust/article/view/757/789>. [Accessed 01 June 2026].
- [7] Cybersecurity Strategy of Ukraine: Decree of the President of Ukraine dated August 26, 2021 №. 447. [Online]. Available: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>. [Accessed 29 May 2026].
- [8] O. Gaponchuk, “12 cities in Ukraine are switching to «intelligent» Smart City management: what will change for residents.,” March 22, 2025. YSC. [Online]. Available: https://ysc.kiev.ua/tehnika/tech_news/12-mist-v-ukrayini-perehodyat-na-rozumne-upravlinnya-smart-city-shho-zminytsya-dlya-meshkantsiv. [Accessed 01 June 2026].
- [9] “Global smart trends in the development of "smart cities" and Ukrainian realities.,” December 8, 2021, *Kyivstar Business Hub*. [Online]. Available: <https://hub.kyivstar.ua/articles/svitovi-smart-tendenciyi-u-rozvytku-rozumnyh-mist-ta-ukrayinski-realiyi>. [Accessed 01 June 2026].
- [10] “The current state of Smart City in Ukraine and the world.,” *Clear Energy Group*, June 12, 2025. [Online]. Available: <https://clearenergy.ua/uk/?view=article&id=56:potochnij-stan-smart-city-v-ukrajini-ta-sviti&catid=11>. [Accessed 01 June 2026].
- [11] “Lviv in the finals of the world award for transparent electronic city management.,” *Press service of the Lviv City Council*. October 30, 2025. [Online]. Available: <https://city-adm.lviv.ua/news/city/lviv-changes/lviv-u-finali-svitovoi-vidznaky-za-prozore-elektronne-upravlinnia-mistom/>. [Accessed 01 June 2026].
- [12] O. O. Yurikov, “Analysis of foreign experience in the implementation of electronic democracy.,” *Electron. Journal. Public management and administration in Ukraine: science. magazine*, no. 46, 2025. pp. 85–88. [Online]. Available: DOI <https://doi.org/10.32782/pma2663-5240-2025.46.14>

Ethical governance, compliance and systemic performance in public health services in Romania

Doina – Monica Agheorghiesei
Alexandru Ioan Cuza University of Iasi
Iasi, Romania
agheorghiesei.doina@feaa.uaic.ro

Ana-Maria Bercu
Alexandru Ioan Cuza University of Iasi
Iasi, Romania
bercu@uaic.ro

Abstract

The accelerated transformations generated by the COVID-19 pandemic, the digitalization of public services and the process of harmonization with European norms have highlighted structural vulnerabilities of the Romanian healthcare system and the limits of traditional administrative governance mechanisms. Although the period 2020–2025 was marked by the expansion of the regulatory framework and compliance tools, systemic performance, the quality of medical care, and the level of public trust remained below expectations. In this context, the study analyses the relationship between administrative compliance and ethical governance, starting from the premise that formal compliance with regulations is not sufficient to ensure institutional efficiency. Based on the Donabedian model and the literature on organizational culture, transparency and institutional accountability, the research highlights that dysfunctions such as communication deficit, punitive culture and underreporting affect the efficiency of compliance mechanisms and institutional response capacity. The methodology used is a qualitative, integrative one, based on the analysis of legislation, institutional reports and specialized literature relevant to the analysed period. The results indicate the need to overcome the paradigm of formal compliance and consolidate an ethical governance model oriented towards accountability, transparency and the patient's interest.

Keywords: ethical governance, administrative compliance, systemic performance, public health services, institutional reform

JEL classification: I18, H83, H11, K23

Introduction

In recent years, public health services in Romania have undergone profound transformations. The health crisis generated by the COVID-19 pandemic, together with the need for accelerated digitalization and alignment with European standards, has required rapid institutional adaptation. However, these external factors have highlighted dysfunctions in the governance sphere: although formal regulations were multiple, systemic performance remained below expectations. The efficiency and quality of medical care, as well as the trust of citizens, are correlated not only with legal compliance (compliance), but also with the way in which ethical values are integrated into the decision-making process. In this context, the relationship between administrative compliance and ethical governance becomes an essential study objective.

The literature emphasizes that the performance of health systems depends on structural factors, management processes and outcomes associated with care (the Donabedian model) [1]. However, simple compliance with laws and formal procedures (“paper” compliance)

does not automatically guarantee quality services. Communication problems, punitive organizational culture and lack of transparency can generate underreporting or avoidance of responsibility even in the presence of clear norms [2] [3]. Thus, it is necessary to explore how ethical governance can be strengthened – that is, the institutional framework that ensures decisions and behaviors based on moral values, responsibility and patient orientation.

This paper analyzes how these dimensions are reflected in the Romanian healthcare system, during the period 2020–2025. Based on an integrative qualitative methodology (legislative analysis, literature studies, institutional reports), we assess whether formal compliance with regulations is sufficient to improve systemic performance. We will show that addressing chronic problems of underfunding and inefficiency requires, in addition to technical norms, strengthening institutional capacity and an ethical culture. The study identifies as directions for reform the institutionalization of the "compliance advisor" function in healthcare organizations and the codification of healthcare regulations for clarity and coherence. These proposals are exemplified by policies or good practices, and the analysis is based on recent data and academic sources.

1. Theoretical framework: ethics in public governance and health service performance

Ethical governance refers to the integration of moral principles (transparency, accountability, and common good) into decision-making processes and institutional culture. In public health administration, this involves orienting policies and practices towards the interest of the patient and the community, not just towards the formal fulfillment of indicators. An ethical organizational culture encourages reporting problems and taking responsibility; while a "blame-free" (non-punitive) culture encourages continuous improvement. Research shows that, in the absence of such a culture, institutions tend to protect their image and minimize the reporting of adverse events [1]. For example, the underreporting of nosocomial infections (HAI – Hospital-Associated Infections) in Romania has been linked to the fear of sanctions, not just the lack of reporting infrastructure [2] [3]. In conclusion, ethical governance involves creating an environment in which rules are respected not only mechanically, but also out of conviction, by assuming ethical values.

Administrative compliance means rigorous compliance with laws and regulations. Although essential for legality and fairness, formal compliance has limits if it is not accompanied by institutional accountability. Comparative studies show that a system with complex rules, but rigid enforcement, can create a culture of fear, where true reporting (e.g., of medical errors) is minimized to avoid consequences [2]. In Romania, evidence suggests that a state has been reached in which the proposal of (legislative) measures is advancing rapidly, but their implementation remains weak. Systemic outcomes (health indicators, patient satisfaction, and financial sustainability) are affected by this gap.

The systemic performance of public health services is a concept that encompasses the efficiency of resource use, the quality of care and equity of access. Relevant indicators include avoidable mortality, immunization coverage or patient satisfaction. For example, preventable mortality in Romania remained high compared to the EU average, and access

to essential services (consultations, hospitalizations, medicines) is often conditional on direct patient payment (over 20% of total expenses) [62]. An OECD report notes that the Romanian healthcare system “aims to be efficient and people-centered, but primary care, prevention and data use need to be strengthened” and emphasizes that “efforts to combat resource waste and increase efficiency and transparency require additional effort” [62]. In this framework, supporting ethics and compliance becomes an integral part of the performance solution: transparency of measures and managerial accountability can reduce inefficiencies and quality-cost discrepancies.

2. Methodology

This study adopts an integrative qualitative approach. Key legislative documents (laws, ordinances and ministerial orders); institutional reports (annual reports of the Ministry of Health, CNAS – National House of Health Assurance, international reports such as OECD, WHO, etc.) and specialized literature (academic articles, case studies) were analyzed. In addition, operational reports and studies were included to highlight good practices or problems identified in the field (e.g., patient satisfaction or infection reporting studies). Citations from the relevant literature (Coman et al.'s work on infection legislation, Mirescu's study on patient satisfaction, Popescu et al.'s analysis on digital services) illustrate concrete examples. Also, updated official sources (ITA USA report on Romania's digital strategy, OECD 2025 study) were used to support the statements. Through this synthesis, a holistic perspective is pursued: not only quantifying performance, but also the organizational and cultural factors that influence it.

Research question

How does the integration of ethical governance mechanisms influence the relationship between administrative compliance and systemic performance in public health services in Romania according to the literature from the last 5 years?

Hypotheses

H1. The integration of ethical governance mechanisms, such as ethics committees, transparency procedures and organizational accountability practices, contributes to improving systemic performance and institutional trust in public health services in Romania.

H2. The existence of administrative compliance mechanisms and health regulations does not have a significant influence on the quality, transparency or systemic performance of public health services in Romania.

3. Evolution of the legislative framework and performance in Romanian public health

3.1. Legislative progress and limits (2020–2025)

Over the past decade, Romanian health legislation has been continuously enriched. The basic regulatory framework remains Law no. 95/2006 on health reform, but numerous orders and decisions have detailed diagnostic criteria, prevention measures and reporting procedures [5]. An illustrative example is the field of healthcare-associated infections (HAIs). In 2004, there were no uniform surveillance criteria in Romania, and HAI reporting

was sporadic. Between 2006 and 2015, successive norms were adopted that expanded definitions, introduced mandatory reporting and, recently, digitized the national infection registry. Thus, according to official legislation, the existence of a computerized registry and the HAI notification law should lead to increased transparency.

However, the effective implementation of these rules has proven problematic. Recent studies reveal that the officially reported prevalence of HAI in Romania is only 4.1%, well below the European average (7.1%) [2]. The main factors: insufficient and untrained human resources, old infrastructure, but also “underreporting for fear of sanctions” [2]. The authors Coman et al. (2025) conclude that “strictly punitive barbarism” persists, and a non-punitive organizational culture is necessary to improve transparency. In other words, legislative changes have existed, but in the absence of a moral environment of trust they do not give the expected results.

In the field of digitalization, notable steps have been taken: the introduction of electronic prescriptions, the national health card, teleconsultation systems or scheduling platforms. However, progress has been heterogeneous. A recent report shows that Romania still lacks interoperability of healthcare systems: healthcare data is fragmented and updated haphazardly [6]. According to the International Trade Administration (2026), Romania’s healthcare digitalization strategy aims to modernize healthcare infrastructure, specifically “overcoming persistent challenges” such as fragmented data and insufficient digital skills, through the development of electronic records, telemedicine platforms, and professional training. In other words, the strategy recognizes that information performance is deficient, and that digitalization, although legally required, needs to be strengthened in practice [6].

Patient satisfaction studies (a proxy indicator of perceived quality) confirm the theory that simple modernization is not enough. In a study conducted at Craiova County Clinical Hospital, Mirescu et al. (2024) show that after the pandemic, patients have become more critical and service evaluations are “more polarized” than before [1]. Although accommodation conditions have improved (modernization of rooms, equipment, protocols), post-2022 patients give more variable and lower marks to the medical staff - a sign that the perception of quality also depends on emotional and organizational experiences, not just on facilities [1]. In conclusion, even technical measures (renovations, procedures) do not fully achieve systemic performance if they are not accompanied by improvements in communication, staff attitude, and institutional culture.

3.2. Beyond compliance: the need for ethical governance

Legislative transformations and technical investments must be accompanied by changes in managerial mindsets. As Coman et al. show, “promoting a non-punitive organizational culture, combined with training, is essential for correct reporting of events and infection prevention” [2]. This quote clearly highlights the fact that legal provisions (reporting, instruction) need an “ethical support framework” (culture, continuing education). Otherwise, a hospital may formally meet the accreditation checklist, but remain marked by fear and avoid communicating problems.

Therefore, the turning point is the integrated approach: formal compliance + ethical governance. Compliance ensures predictability and legality, ethics in governance ensures coherence and adaptability to new challenges. An OECD report highlights that Romania needs to overcome waste in the system and increase its transparency, in order to become efficient and focused on patients' needs [62]. This involves resource management measures (relating to finances and payroll) as well as open communication and institutional integrity (ethical aspects). Integrated ethical governance could, for example, reduce the informality of payments (although a predominantly financial problem, but also reflected in patient trust) and increase public trust in the system. Thus, in the analysis of systemic performance, not only the quantity of allocated resources (classical health indicators) but also the quality of the human and decision-making factor must be taken into account.

3.3. Digitalization of health services and ethical governance

An essential subchapter is the digitalization of public health services, as it intersects interests of efficiency, access and governance. In Romania, digitalization efforts have been progressive: from telemedicine platforms and electronic signatures to national strategies. However, the adoption of digital public services still remains low. According to the European Commission's DESI index, Romania ranks last in Europe in terms of the expansion of digital public services [7]. Recent analyses show that the population is aware of the benefits of digitalization (simplicity, speed, transparency), but faces significant obstacles: lack of information and technical support, fears about data security, low digital literacy and the complexity of government platforms [7]. In other words, the role of ethical governance here is twofold: to ensure adequate legislative frameworks (protecting personal data, for example) and to promote social inclusion and digital education so that citizens truly benefit from the new services.

A positive example is the digital strategy developed in 2025–2026: The Romanian Government has prepared the National Health Digitalization Strategy 2026–2030, which aims precisely to remedy the deficiencies discovered. The document explicitly recognizes that "health data is fragmented," "systems are not interoperable," and healthcare professionals lack sufficient digital skills [6]. The plan emphasizes the development of integrated electronic medical records, the modernization of telemedicine platforms, and the training of specialists. It is a necessary step to increase information transparency and operational efficiency. At the same time, its implementation should be accompanied by clear ethical policies: for example, the protection of patient data must be guaranteed to the population, and the way in which platforms are used must be transparent. These measures generate trust, an element highlighted by the study by Popescu et al. (2024), which shows that in Romania citizens want "reliable and accessible" digital solutions and demand from the government an approach that takes into account the cultural values of the population [7]. Simply put, successful digitalization of healthcare requires respect for both technical regulations and the moral needs and expectations of users.

4. Examples of good practices and public policies in Romania

In recent years, the Romanian healthcare system has gradually begun to integrate compliance mechanisms, digitalization and organizational ethics, in an attempt to respond to both European requirements and internal structural issues related to transparency, patient

safety and managerial responsibility. Although many of these initiatives are still in a consolidation stage, they indicate a gradual paradigm shift, oriented towards health governance based on quality, monitoring and institutional accountability.

A relevant example is the strengthening of surveillance and reporting mechanisms for healthcare-associated infections (HAI). Currently, the applicable regulatory framework is mainly represented by the Order of the Minister of Health no. 1101/2016 on the approval of the Norms for the surveillance, prevention and limitation of healthcare-associated infections in healthcare units, a regulatory act still in force and successively updated. It establishes the obligation of all public and private healthcare facilities to identify record and report healthcare-associated infections, as well as to implement their own prevention and control programs [8].

The digitalization of these processes represented an important step towards increasing the traceability and transparency of epidemiological data. The introduction of electronic registers and the centralization of reporting at the Ministry of Health level reduced the risk of information loss and facilitated comparative analysis between institutions. Although practical application is still uneven between hospitals, these mechanisms contribute to the development of an organizational culture based on real reporting and prevention, in line with European standards on patient safety. The study conducted by Coman et al. (2025) highlights the fact that the evolution of Romanian legislation in the field of HAI reflects a progressive orientation towards systematic monitoring, institutional responsibility and harmonisation with European public health policies.

Another relevant example of good practice is the national hospital accreditation system coordinated by the National Authority for Quality Management in Health (ANMCS). The accreditation process involves the periodic assessment of healthcare facilities against complex standards regarding service quality, patient safety, risk management and respect for beneficiaries' rights. Beyond the formal and administrative component, accreditation stimulates the development of an institutional culture oriented towards accountability and continuous improvement. In practice, hospitals are required to implement clear procedures regarding informed consent, patient communication, incident reporting and ethical management of medical activities. The importance of these mechanisms is also supported by international assessments. OECD (2025) shows that the Romanian healthcare system aims to become "efficient and people-centered", but emphasizes the need to strengthen primary medicine, prevention and the use of data in the decision-making process. The report also emphasizes that measures aimed at reducing waste of resources and increasing administrative transparency require additional efforts [62]. In this context, accreditation can be interpreted not only as a bureaucratic compliance tool, but also as a mechanism for organizational transformation and managerial professionalization. The development of internal ethics and compliance structures represents another important direction in the modernization of hospital governance. In many healthcare facilities, ethics committees and internal mechanisms for analyzing conflicts of interest, patient complaints and professional misconduct are in place. These structures are supported by the provisions of Law No. 95/2006 on healthcare reform and by secondary regulations on the organization of public hospitals. Their role goes beyond simple legal compliance, contributing to the

consolidation of an organizational culture based on integrity, accountability and the protection of patient rights.

In parallel, the Ministry of Health and other public institutions have promoted in recent years guiding documents on ethical conduct and professional integrity in the medical system. Even if their application differs between institutions, the existence of codes of ethics and internal compliance procedures indicates a trend towards European models of clinical and administrative governance. In the specialized literature, Agheorghiesei (Corodeanu) and Poroș (2016) argue that ethical auditing represents an essential element of the "third generation of organizational ethics", through which medical institutions move from simple formal compliance with norms to the integration of ethical values into the managerial and decision-making culture. At the same time, civic participation and patient feedback mechanisms have begun to play an increasingly important role in assessing the quality of medical services. Some public hospitals implement periodic patient satisfaction surveys and publish their results in order to increase transparency and managerial accountability. These tools contribute to introducing a patient-centered perspective and allow the identification of vulnerabilities related to communication, accessibility, or perception of the medical act. The results of the research conducted by Mirescu et al. (2024) demonstrate that patient satisfaction is influenced not only by medical competence, but also by the quality of human interaction, response time, hospitalization conditions, and the level of information provided to the patient.

At the same time, the digitalization of public administration and medical services creates the premises for a more transparent relationship between the citizen and healthcare institutions. The national health digitization strategy for the period 2026–2030 promotes the development of medical data interoperability, the expansion of the electronic health record and the increase of the population's access to integrated digital services [6]. These objectives are consistent with the conclusions formulated by Popescu et al. (2024), according to which citizens' perception of digital public services directly depends on the level of transparency, accessibility and institutional trust.

Overall, these initiatives demonstrate that health policies in Romania are beginning to be formulated in logic of ethical and participatory governance, in which legal compliance is complemented by mechanisms of mutual control, transparency and civic engagement. However, significant challenges remain related to administrative capacity, specialized human resources, digital infrastructure and uniform application of standards at national level. Consolidating these reforms requires continued investments in professional training, organizational culture, and opening up the decision-making process to civil society and beneficiaries of health services.

These examples illustrate how health policies can be thought of in terms of ethical governance: not just rules imposed from above, but also mechanisms of participation and mutual control. However, much work remains to be done to increase institutional capacity (training, resources) and to open up decisions to the public.

5. Discussions

The analysis of institutional practices and the regulatory framework in the Romanian healthcare system highlights the fact that the relationship between compliance and governance can no longer be reduced exclusively to formal compliance with legislation. Increasingly, institutional efficiency depends on the existence of internal mechanisms capable of ensuring continuity of monitoring, decision-making coherence and the integration of ethical values into current managerial activity. In this context, the importance of developing organizational structures dedicated to compliance supervision and institutional risk management is noted.

The experience of large hospitals and medical networks shows that the presence of ethics, quality or compliance offices contributes to increasing the institutional capacity for the coherent interpretation and application of regulations. Such structures facilitate communication between management, medical staff and control bodies, reduce the risk of non-unitary administrative practices and support the development of an organizational culture oriented towards accountability and transparency. From a governance perspective, the existence of permanent internal monitoring mechanisms allows overcoming the reactive approach, based exclusively on sanctions or external control, in favor of a preventive and formative logic.

At the same time, the analysis of the legislative framework reveals that one of the major difficulties of the Romanian healthcare system is regulatory fragmentation. Although there are fundamental legislative acts, such as Law no. 95/2006 on healthcare reform or Law no. 46/2003 on patient rights, numerous essential regulations are dispersed in ministerial orders, government decisions, protocols and successive methodological norms [9]. This legislative dispersion can generate difficulties in interpretation and application, especially at the level of institutions with limited administrative resources. Consequently, the predictability and coherence of the decision-making process depend not only on the existence of rules, but also on their accessibility and clarity.

From a good governance perspective, contemporary trends in public administration support the need to simplify and harmonize regulations, in accordance with the principles of "smart regulation". A more coherent regulatory framework facilitates both institutional compliance and the accountability of actors involved in the medical and administrative process. At the same time, reducing legislative overlaps and contradictions can contribute to increasing administrative efficiency and strengthening the trust of health professionals in regulatory mechanisms.

The analysis also highlights the fact that modern compliance mechanisms tend to go beyond the strictly legal dimension, integrating elements related to organizational ethics, whistleblower protection, transparency, and institutional participation. In this sense, ethical auditing, internal reporting procedures and professional counseling mechanisms contribute to building an institutional culture based on collective responsibility and decision-making. These tools become particularly relevant in contexts characterized by high administrative pressures, legislative complexity and the constant need to adapt to European standards.

Overall, the relationship between compliance and governance in the Romanian healthcare system indicates a gradual transition from a predominantly bureaucratic approach to one oriented towards integrated institutional management, transparency and ethical responsibility. The consolidation of this direction, however, depends on the development of administrative capacity, the professionalization of health management, and the creation of stable coordination mechanisms between legal norms, organizational practices, and public interests associated with health protection.

The results of our research show a complex picture: Romania has many regulations and technological initiatives at its disposal, but the implementation process is lagging. Ethical governance appears as a mediating factor between formalism and real results. In its absence, systemic performance suffers from rigidity and fear. For example, it was observed that the implementation of a ministerial code of ethics was ignored in many healthcare facilities because there was no oversight mechanism and clearly defined consequences. Similarly, the lack of a dedicated ethics auditor or compliance advisor meant that performance indicators (reporting of infections, patient satisfaction) were used partially, without exploring the social or cultural causes of low values. Another critical aspect is staff training. Promoting ethical behavior requires not only strict rules, but also the development of communication and teamwork skills. In hospitals that have invested in participatory management (internal feedback sessions, regular ethical training, multidisciplinary working groups), patient satisfaction indicators have improved compared to more traditionally managed units. Thus, performance is not improved only through written rules, but also through ethical leadership.

Digitalization can be a major catalyst if accompanied by appropriate strategies. The aforementioned national strategy foresees substantial investments in technology [6], which creates high expectations. But European experience shows that technology without organizational sustainability only generates additional administrative pressure. To be effective, the national digital platform for health (budgeted with 100 million EUR) should be implemented progressively, with user involvement and data protection at the center. (We recall that in Romania, in 2025, the registration of individuals did not yet allow the patient direct online access to their own medical record; the strategy attempts to correct this situation.)

6. Conclusions

The analysis of the literature from the last five years on the relationship between administrative compliance, ethical governance and systemic performance in public health services in Romania demonstrates that institutional efficiency cannot be achieved exclusively through the existence of extensive regulations or formal administrative control mechanisms. Although Romania has significantly expanded its legislative and regulatory framework regarding patient safety, hospital accreditation, reporting obligations and the digitalization of health services, the effectiveness of these measures depends largely on the extent to which they are integrated into the organizational culture and everyday institutional practices.

The results support the first hypothesis (H1), namely that the integration of ethical governance mechanisms contributes to improving systemic performance and strengthening institutional trust in public health services in Romania. The literature indicates that mechanisms such as ethics committees, ethics audits, transparency procedures, codes of conduct and organizational accountability practices facilitate the development of an institutional culture based on responsibility, prevention and professional integrity. In this context, ethical governance becomes an essential component of the modernization of the health system, as it encourages transparency, supports institutional learning and strengthens public trust in medical organizations. Agheorghiesei (Corodeanu) and Poroach (2016) emphasize that ethical audit represents an advanced form of organizational governance, capable of integrating moral values into managerial and administrative decision-making processes within medical institutions. Therefore, ethics should not be perceived separately from legal regulation, but rather as a complementary dimension that enhances both the legitimacy and effectiveness of administrative action.

At the same time, the analysis also confirms the second hypothesis (H2), according to which the existence of administrative compliance mechanisms and health regulations does not significantly influence the quality, transparency or systemic performance of public health services in Romania. The studies analyzed show that formal compliance, when disconnected from ethical organizational practices, often remains limited to bureaucratic obligations, without generating substantial structural improvements. The persistence of underreporting practices, institutional reluctance to recognize internal vulnerabilities and difficulties related to accountability continue to affect the health system's capacity to implement effective prevention and quality control policies. In this regard, Coman et al. (2025) demonstrate that deficiencies in reporting medical incidents and healthcare-associated infections remain significant obstacles to institutional transparency and organizational learning. Similarly, research conducted by Mirescu et al. (2024) emphasize that patient satisfaction and trust are influenced not only by clinical outcomes, but also by the quality of communication, institutional transparency, and the degree of respect shown to patients during interactions with healthcare.

Furthermore, the literature emphasizes the importance of strengthening institutional capacity and ensuring regulatory adaptability in the context of ongoing healthcare reforms and digital transformation. The increasing complexity of healthcare administration, combined with European requirements for data interoperability and transparency, requires administrative structures capable of efficiently managing compliance processes while upholding ethical governance principles. Continued investments in staff training, modernizing digital infrastructure, and simplifying legislative procedures are therefore necessary conditions for improving institutional performance. The National Strategy for the Digitalization of the Healthcare System for the Period 2026-2030 reflects this orientation towards a more integrated and data-driven healthcare administration system [6].

Another important conclusion concerns the negative effects generated by legislative fragmentation and overlapping regulations. Excessive bureaucracy and instability of the regulatory framework can reduce institutional predictability and hinder the coherent implementation of public health policies. Therefore, the performance of health institutions

depends not only on the quantity of regulations, but also on their clarity, accessibility and practical applicability. Effective health administration requires a coherent regulatory environment, capable of balancing administrative compliance with ethical responsibility and the public interest.

References

- [1] Mirescu, L., Popescu, A. C., & Dragomir, I. M. , "Degree of satisfaction among patients admitted to a public healthcare facility in Romania," *Current Health Sciences Journal*, vol. 50(5), no. <https://doi.org/10.12865/CHSJ.50.04.06>, p. 515–527, 2024.
- [2] Coman, A., Pop, D., Muresan, F., Oprescu, F., & Fjaagesund, S., "Surveillance and reporting of hospital-associated infections—A document analysis of Romanian healthcare legislation evolution over 20 years," *Healthcare*, vol. 13(3), no. <https://doi.org/10.3390/healthcare13030229>, p. 229, 2025.
- [3] Agheorghiesei (Corodeanu), D. T., & Poroch, V., "Ethical audit practice in hospital units – The pillar of the third generation of ethics," *Postmodern Openings*, vol. 137–147, no. <http://dx.doi.org/10.18662/po/2016.0702.09>, p. 7(2), 2016.
- [4] OECD, "OECD reviews of health systems: Romania 2025," OECD Publishing, <https://doi.org/10.1787/f52e4a98-en>, 2025.
- [5] Parliament of Romania, " Law no. 95/2006 on healthcare reform (republished)," *Official Gazette of Romania, Part I*, no. 652, 28 August 2015.
- [6] International Trade Administration., "Romania national health digitalization strategy 2026–2030. U.S. Department of Commerce.," 26 January 2026. [Online]. Available: <https://www.trade.gov/market-intelligence/romania-national-health-digitalization-strategy-2026-2030>. [Accessed 20 May 2026].
- [7] Popescu, M. A. M., Barbu, A., Moiceanu, G., Costea-Marcu, I.-C., Militaru, G., & Simion, P. C., "Citizens' perception of digital public services: A case study among Romanian citizens," *Administrative Sciences*, vol. 14(10), no. <https://doi.org/10.3390/admsci14100259>, p. 259, 2024.
- [8] Ministry of Health , "Ministry of Health Order no. 1101 of September 30, 2016 on the approval of the Norms for surveillance, prevention and limitation of healthcare-associated infections in health care facilities.," *Official Gazette of Romania*, no. 791, 7 October 2016.
- [9] Romanian Parliament, "Law no. 46 of January 21, 2003 on Patients' Rights," *Official Gazette of Romania, Part I*, no. 51,, 29 January 2003.

Digital product passport for the textile industry: ensuring transparency, circularity, and cyber resilience

Anatolie Babin

Academy of Economic Studies of Moldova, Chisinau, Republic of Moldova
anatolii.babin@ase.md

Andrey Mirza

Moldova State University, administrator of the SORINTEX cluster
sorintex.soroca@gmail.com

Sergiu Tutunaru

Academy of Economic Studies of Moldova, Chisinau, Republic of Moldova
tutunaru@ase.md

Ion Covalenco

National Scientific and Educational Network of Moldova, Chisinau, Republic of Moldova
ion.covalenco@renam.md

Abstract

The advancement of digital technologies offers opportunities to enhance transparency and security across industrial supply chains, particularly in sectors critical for sustainability. **Objectives:** This study examines the implementation of a Digital Product Passport (DPP) in the textile and fashion industry to improve transparency, traceability, circularity, and cybersecurity compliance. The goal is to secure lifecycle data from raw material sourcing to recycling, supporting sustainability and alignment with the EU Ecodesign for Sustainable Products Regulation (ESPR). **Prior Work:** Building on our research on *SME Integration to Industry 4.0 – Regional Innovation Platform*, which emphasized promoting SMEs' adoption of digital services, document digitization, and integration into digital value chains, previous studies in the textile sector have highlighted a gap between brand-level reporting and product-level traceability. The DPP framework leverages EU initiatives such as CIRPASS-2 and GS1 standards to ensure interoperability, secure data exchange, and enhanced visibility of product lifecycle information. **Approach:** A mixed-method approach was applied, including expert interviews, field surveys, and IT architecture analysis, integrating geolocation and production data. The DPP platform employs a decentralized, interoperable architecture with blockchain for data immutability, role-based access, PLM/PIM integration, and QR/NFC “Garment-to-Twin” interfaces. Key data encompass material composition, environmental performance, product origin, and circularity instructions. **Results:** Findings indicate that brand transparency is improving, but product-level traceability remains limited. Integration with the EU Cybersecurity Certification Framework (EUCCF) ensures secure handling of production and location data, supporting trusted information exchange and regulatory compliance. **Implications:** This research guides policymakers, practitioners, and researchers in deploying secure digital tools in global textile supply chains, demonstrating how DPPs advance circular economy objectives and cyber-resilience. **Value:** The study presents an original framework connecting digital product passports, territorial traceability, and cybersecurity compliance, offering a scalable model for improving accountability, transparency, and secure data governance in the European textile industry.

Keywords: digitalization; cybersecurity; supply chain traceability; circular economy; data management.

1. Introduction

The textile and fashion industry is one of the most complex and globally integrated industries, characterized by complex supply chains, diverse stakeholders, and significant environmental and social impacts. In recent years, growing consumer awareness,

increasing regulation, and sustainability demands have highlighted the need for increased transparency and traceability throughout the product life cycle (PLM) [1]. Traditional reporting methods, often limited to brand-level disclosure, do not provide detailed information at the product level, limiting accountability and opportunities for implementing circular economy practices. Digital Product Passports (DPPs) [2] represent a promising tool for addressing these challenges. They enable the recording, storage, and secure sharing of detailed product information - from raw material sourcing to lifecycle management, including disposal and recycling. This increases supply chain transparency, promotes material recycling and reuse, and ensures compliance with cybersecurity standards. This approach is consistent with the EU Ecodesign for Sustainable Products Regulation (ESPR) [3], which emphasizes product-level transparency, efficient resource use, and circular economy principles. For textile cluster managers, the digital product passport should be viewed not simply as a digital tool, but as a strategic element of digital transformation and integration into European innovation ecosystems. Its implementation will facilitate the development of circular production models, optimize resource use, reduce waste, and increase trust with consumers, partners, and regulators through standardized and secure data exchange. The objective of this study is to examine the implementation of the DPP at SORINTEX textile cluster companies, focusing on enhancing traceability, supporting circular economy goals, and ensuring data security. Building on previous research on the integration of small and medium-sized enterprises into Industry 4.0 [4] and digital value chains, the article proposes a scalable model for implementing a digital passport using blockchain technologies. Its integration with PLM/PIM, ERP, QR/NFC "Garment-to-Twin" interfaces and manufacturing platforms ensures synergy with the Industry 4.0 concept, enabling enterprises to move towards more sustainable and intelligent production and supply chain management models. For enterprises in the cluster, the implementation of the DPP is an important step towards sustainable, digital and cyber-resilient production that complies with European standards ESG [5], ESPR, NIS2 [6] and ISO/IEC 27001 [7]. Moldova's associated participation in the CoP S3 interregional platforms can provide access to EU innovation networks, knowledge sharing, and best practices in digitalization, sustainable production, and industrial ecosystem development. Interaction with the platform not only facilitates product traceability but also develops the scientific and entrepreneurial potential of the development regions where the cluster's enterprises are located. Since the use of a digital product passport requires training specialists in data analysis, cybersecurity, environmental assessment, and product lifecycle management, and facilitates the creation of new jobs at enterprises, including for scientific researchers, the participation of universities and their research centers as partner organizations simultaneously facilitates the participation of interested cluster producers in the Horizon Europe Framework Programme for Scientific Research and the Erasmus+ educational program. Thus, the study provides both a conceptual and practical plan for policymakers, specialists, and researchers seeking to create sustainable, evidence-based, and expert-based supply chains in the textile industry.

2. Digitalization of the textile industry and the role of the Digital Product Passport

The textile and fashion industries today face complex challenges that require the implementation of digital traceability tools such as the Digital Product Passport (DPP). These industries are known for their high resource intensity and significant environmental

impact. Clothing production requires enormous amounts of water, land, and non-renewable resources, resulting in high levels of pollution and greenhouse gas emissions. With the growth of the fast fashion segment, clothing production volumes today are more than double those of 2000. Furthermore, a significant portion of low-quality, non-recyclable products has a devastating impact on natural resources. These trends highlight the need for the textile industry to transition to more sustainable production and consumption models. Environmental risks are inextricably linked to economic ones. Even before the global crises, "business as usual" forecasts pointed to declining production and profits due to raw material shortages, rising energy and water prices, and rising labor costs. The COVID-19 pandemic has dramatically exacerbated these trends: supply chain disruptions, logistical disruptions, and restrictions on international trade have led to declining sales and the bankruptcy of several major companies. In 2023, many European fashion retailers, including Camaieu, Go Sport, Pimkie, and Kooka [8], filed for bankruptcy or underwent judicial reorganization, demonstrating the industry's high vulnerability to economic and logistical shocks.

The social dimension of the textile industry's challenges is also critical. Recent tragic events, such as the Rana Plaza factory collapse [9] and the use of forced labor in Uyghur cotton production, have exposed systemic labor rights violations in supply chains. The UN Guiding Principles on Human Rights in Business [10], including the provision of decent wages and safe working conditions, often remain formal requirements, as confirmed by data from the International Labor Organization. These facts highlight the need to implement control and transparency tools at the product level. In this environment, the digital product passport is becoming a key tool for addressing the industry's complex problems. It enables the recording, storage, and secure transfer of detailed information on the origin of materials, production conditions, environmental impact, and recyclability of products. Its use increases transparency, supports circular economy goals, and promotes compliance with social and environmental standards. The passport supports interregional and international cooperation and enables small and medium-sized enterprises to participate in global supply chains on an equal basis with large manufacturers, increasing export potential and competitiveness, capturing information on the origin of materials, their recycling and reuse, and creating the basis for service and recovery business models. At the same time, the expected benefits – business sustainability, access to international innovation platforms, and integration into the "European Research Area" [11] – significantly outweigh the costs. The textile industry is currently undergoing a profound transformation driven by the simultaneous development of digital, social, and environmental sustainability dimensions, as shown in Fig. 1. This triple transition [12] reflects how technology, social responsibility and environmental sustainability are interconnected and together shape the future of the industry. The Digital Product Passport (DPP) is a digital identification card for products, components, and materials, officially registered with a government agency, which stores relevant information to support product sustainability, promote circularity, and strengthen compliance. It is designed to increase transparency, facilitate recycling, and provide consumers with reliable product information in accordance with the EU ESPR regulation. It represents not only a transparency tool but also a complex distributed data management system, in which the so-called security paradox is a key challenge. On the one hand, the DPP must ensure open access to

information on product composition, environmental performance, and recycling capabilities in accordance with ESPR requirements. On the other hand, the system is obliged to protect commercially sensitive data, including supply chains, cost data, and production recipes.

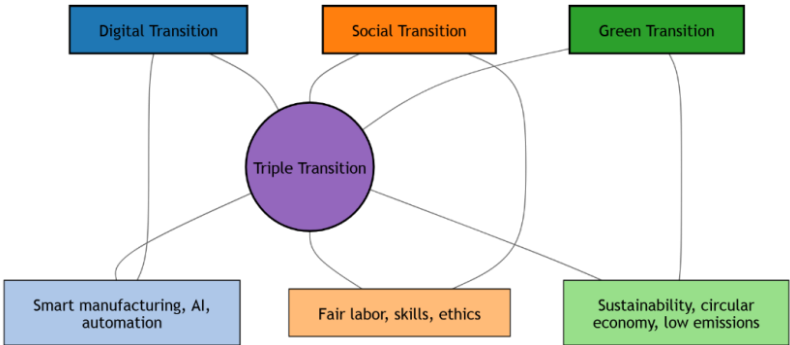


Fig. 1. Triple transition of the textile industry: digital, social and green dimensions.
 Source: Created by authors

Thus, a fundamental contradiction arises between transparency and privacy, which requires the implementation of a multi-layered cybersecurity architecture and differentiated access control. The clothing industry makes transparency and traceability particularly important. Materials can be sourced from dozens of countries, production stages are distributed across multiple factories, and logistics span global routes. This complexity complicates quality control, environmental compliance, and monitoring of labor conditions, increasing the industry's vulnerability to economic risks, consumer criticism, and regulatory demands. Transparency and traceability at the product level enable the tracking of every garment from raw material to the end consumer. This not only enhances environmental and social responsibility but also economic efficiency: companies can identify supply chain bottlenecks, optimize resources, and minimize the risk of reputational and financial losses.

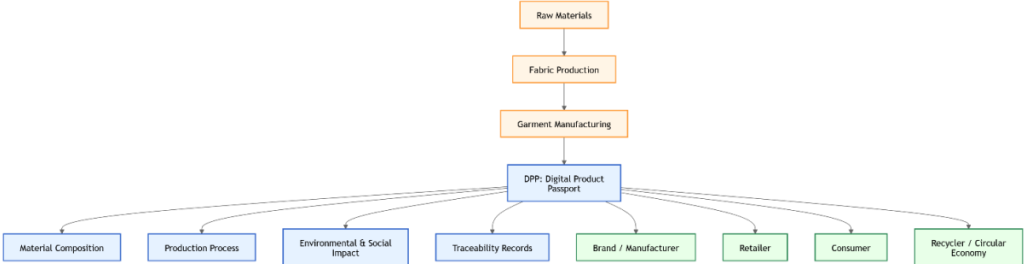


Fig. 2. The Role of DPP in Textile Supply Chain.
 Source: Created by authors

The figure shows how the DPP acts as a central hub, aggregating data from all supply chain participants and presenting it in a convenient and secure format. The platform enables tracking of material composition, environmental performance, and social standards at every stage, ensuring the trust of both consumers and regulators. This approach improves

monitoring efficiency, promotes sustainable production and the implementation of a circular economy, while minimizing the risks of non-compliance and supply chain abuse.

To systematically implement transparency and traceability, the EU developed the DPP, regulated by the Eco-Design for Sustainable Products Regulation (ESPR). The main goal is to ensure transparency and control over the product life cycle: from the composition of raw materials to instructions for recycling and reuse. In the textile industry, implementation is a priority, and requirements are planned [13] to be introduced in 2027–2028, making it a relevant tool for companies striving for sustainable and socially responsible production.

The platform architecture is to be decentralized, open, and compatible with GS1 standards [14] so that data can flow seamlessly between brands, suppliers, processors, and regulators. Each product receives a unique identifier (GTIN) [15], encoded in QR or NFC, through which complete product information can be accessed. The platform integrates the collection and aggregation of data from all supply chain participants, role-based access management, and integration with PLM systems.

The Garment-to-Twin application allows for the instant scanning of physical tags and the generation of a digital product passport. The integration of a product lifecycle management (PLM) system with the Garment-to-Twin application leverages 3D CAD platforms to create a single source of truth, significantly accelerating time-to-market and reducing the cost of physical samples. The experience of the Sust3DFashion project [16] can be used in conjunction with the Digital Product Passport to implement an innovative approach in the textile and fashion industry of the Republic of Moldova through collaboration with the technology and digital sectors, with a particular focus on 3D printing. The term Garment-to-Twin (G2T) is most often encountered in the context of 3D clothing modeling and virtual fashion and refers to the process of transferring physical clothing or its design into a digital twin. In other words, it is the creation of a virtual model of a real garment that accurately reproduces its shape, size, material, and movement behavior.

An important aspect of these innovations is ensuring compliance with European cybersecurity requirements, including the NIS2 directive, ISO/IEC 27001, and the GDPR. Since the DPP aggregates data on raw material origins, production processes, logistics, and ESG indicators, information security becomes critical to ensuring trust between supply chain participants. Therefore, the platform architecture must incorporate risk management mechanisms, network segmentation, data encryption, and secure interaction with external ERP, PLM, and PIM systems.

3. Methodology and architecture of the DPP and cyber security considerations

This study examines the architecture of digital product passports (DPPs) through the lens of a methodological approach to ensuring data security and privacy. The primary goal of the methodology is to ensure the availability, reliability, and security of data for all stakeholders, including consumers, regulators, and supply chain participants. Effective data protection begins with data classification, which determines which elements of information are public, restricted, or confidential. This classification forms the basis for implementing

access control systems and encryption strategies. In accordance with ESPR requirements, DPPs implement three access levels, as shown in Table 1.

Table 1. Data classification and access levels in the Digital Product Passport architecture

Access level	Description	Data examples
Public	Available to any user	Material composition, recycling instructions, environmental impact data
Authorized	Available to authorized parties only	Test reports, compliance documentation, supply chain traceability
Confidential	Trade secret, not available through DPP	Accurate supplier data, patented formulas, cost information

Source: Created by authors

Access control is implemented through an identity and access management (IAM) system. Public data is provided without authentication, authorized data requires credentials verification through a federated system, and sensitive data is not transferred via APIs but is available only as metadata with an indication of the legal basis for the request.

Data encryption is the foundation of DPP security. It is used both in transit between systems and at rest. Data transmission is protected using TLS 1.3 (or TLS 1.2 if necessary) with strong cipher suites and the inclusion of HSTS headers. Data at rest is encrypted using AES-256, with keys stored in hardware security modules (HSMs) or cloud-based KMS. Key rotation is performed automatically according to the security policy. Encryption is applied at the level of individual database fields, allowing simultaneous queries against publicly accessible data without decrypting sensitive fields.

Given the complexity of modern supply chains, the need to comply with environmental and social standards, and the growing role of digitalization, the study aims to ensure companies' strategic and operational effectiveness. To achieve this goal, the following specific objectives were identified:

- 1) Developing a DPP architecture with decentralization and blockchain in mind. The architecture must enable the collection of data from disparate sources, ensure its immutability, and support interoperability standards, including GS1 and ESPR requirements.
- 2) Integration with PLM/PIM systems and QR/NFC "Garment-to-Twin" interfaces (Fig. 3). This will allow data on material composition, product origin, production processes, and environmental performance to be combined into a single digital record accessible to all stakeholders.

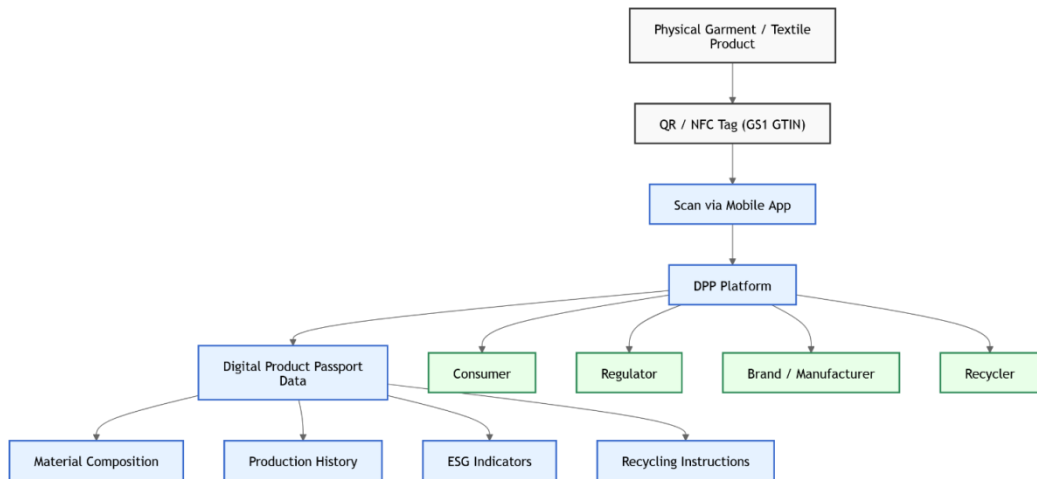


Fig. 3: The Garment-to-Twin Activation Flow
Source: Created by authors

3) Analysis of the impact of DPP on sustainability and the circular economy. The study assesses how DPP implementation impacts resource use, waste reduction, material recycling, and carbon footprint minimization.

4) Ensuring compliance with cybersecurity and EU standards. Particular attention is paid to data protection and the prevention of unauthorised access, including the use of role-based management and compliance with the EU Cybersecurity Certification Framework (EUCCF) [17].

The DPP may contain personal data, such as names of supply chain participants, IP addresses, email addresses, or unique identifiers. To comply with the GDPR, the following measures are taken:

- Data minimization: store only strictly necessary personal data.
- Purpose limitation: use data only for regulatory purposes, excluding marketing.
- Right to erasure: ensure that data is deleted or anonymised upon request by data subjects without compromising regulatory compliance.
- Data Processing Agreements (DPA): are concluded with all third-party data processors (cloud services, CDN, analytical platforms).

Ensuring the protection of companies' commercial information and minimizing the risks of unauthorized access, as well as supply chain transparency and protection of trade secrets, are achieved through: Data aggregation: reporting by region rather than by specific suppliers. Pseudonymization: replacing supplier identifiers with opaque codes. Selective disclosure: disclosing details only to authorized bodies. Zero-knowledge evidence: verifying product compliance with sustainability criteria without disclosing suppliers.

To ensure the sustainable operation and development of the digital product passport (DPP) ecosystem, a mixed-method study is proposed, combining qualitative and quantitative

approaches. This approach allows for the simultaneous consideration of organizational, technological, and cybersecurity aspects of DPP implementation, as well as assessing the impact of the digital passport on the transparency, traceability, and resilience of supply chains. The qualitative analysis includes expert interviews with representatives of brands, manufacturing companies, and technology consortia (e.g., CIRPASS-2[18]), which helps identify digital passport requirements, real-world supply chain challenges, and market participant expectations. The quantitative component includes the analysis of data on materials, production processes, logistics, geolocation, and circularity guidelines, which can be aggregated within the DPP architecture.

To formalize the digital product passport (DPP) architecture in accordance with ISO/IEC 42010 [19] requirements, a structured approach is used, based on dividing the system into viewpoints and corresponding views. This approach allows for the separation of interests between various stakeholders, including manufacturers, regulators, consumers, and IT infrastructure developers, while ensuring a transparent description of the functional, information, infrastructure, and cybersecurity aspects of the system. Based on this approach, a generalized DPP architecture is proposed, shown in Fig. 4.

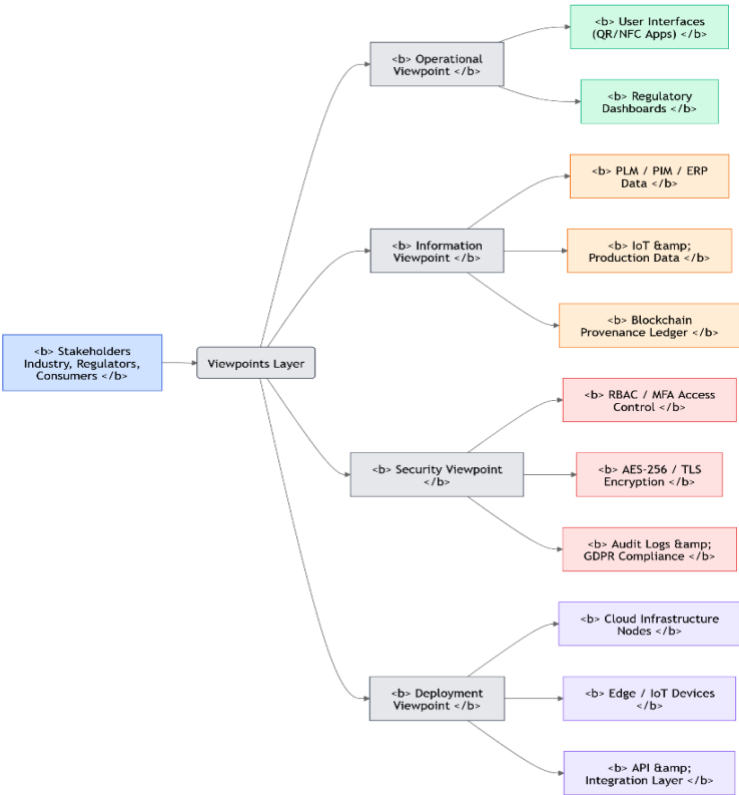


Fig. 4. ISO/IEC 42010 architecture model for the Digital Product Passport (DPP)
 Source: Created by authors

The presented architecture demonstrates the application of ISO/IEC 42010 principles to a digital product passport, providing a structured division of the system into presentation, data processing, cybersecurity, and deployment layers. The operational viewpoint reflects user interaction with the system through QR/NFC interfaces and regulatory panels. The information viewpoint integrates data from PLM, PIM, ERP systems, IoT sources, and a blockchain registry. The security viewpoint ensures the implementation of RBAC, MFA, encryption, and auditing mechanisms in accordance with GDPR and ISO/IEC 27001 requirements. The deployment viewpoint describes a distributed infrastructure including cloud and edge components. This approach ensures the interoperability, scalability, and cyber resilience of the DPP as part of the digital transformation of the textile industry. The platform enables material tracking, environmental performance, social standards, and recycling capabilities throughout the product lifecycle, increasing trust among all market participants and facilitating the adoption of circular production models.

The DPP security architecture [20] must include multi-layered cryptographic protection:

1) *Data transfer*: TLS 1.3 (or minimum TLS 1.2); HTTPS for all API interactions.

2) *Data storage*: AES-256 for protecting sensitive information; the use of hardware security modules (HSMs) or key management systems (KMS); and regular rotation of cryptographic keys. This ecosystem provides protection from both external attacks and storage infrastructure compromise. Field-level encryption is of particular importance in the DPP architecture-encrypting individual data attributes instead of protecting the entire database. This ensures: maintaining the availability of public data without delay; protecting sensitive information even if the database is compromised; and the ability to selectively decrypt only for authorized requests. This balances system performance and security. In the context of DPP, it is necessary to consider the possible presence of personal data, including:

- employee identification data;
- data from quality inspectors;
- electronic contacts;
- access logs;
- user identifiers.

Therefore, the system must comply with the GDPR requirements and ensure:

- minimization of collected data;
- limitation of the purposes of information processing;
- exercise of the right to erasure;
- availability of data processing agreements (DPA).

An important aspect of the digital product passport architecture is balancing data transparency with the protection of commercially sensitive information, which is defined in the literature as the "security paradox" of DPP. On the one hand, the system must ensure the availability of information for consumers and regulators in accordance with ESPR requirements, while protecting data on suppliers, production costs, and processes. To address this challenge, a multi-tiered access model is used, including public, authorized, and confidential data levels, where each type of user is provided with a strictly limited set of information. Since DPP operates through digital interfaces, the API becomes a key point

of cyber risk. To protect the API, the following are used: OAuth 2.0 and JWT tokens; strict input validation; protection against SQL injection attacks; rate limiting to prevent overload; logging of all user actions; IP allow listing; Content Security Policy (CSP). Summarizing the findings of this phase of research (outlined in sections two and three), it can be concluded that the Digital Product Passport (DPP), mandated by the EU Ecodesign Regulation for Sustainable Products (ESPR), represents a digital fingerprint of textile products, enabling the traceability of the origin of materials, chemical composition, and environmental impact of clothing. Protecting supply chain data is crucial to preventing counterfeiting, protecting confidential business information (CBI), and complying with strict data protection laws. Key cybersecurity threats and challenges include:

- Data falsification and fraud: Fraudsters may alter environmental performance, material balances or certification data to circumvent EU regulations or market surveillance authorities.
- Supply Chain Disruptions: Fragmented supply chains - from Tier 4 fiber producers to Tier 1 apparel brands—present numerous weak points where hackers can intercept unencrypted data.
- Disclosure of confidential information: Manufacturers risk disclosing proprietary color formulas, chemical compositions, or supplier lists when sharing data throughout the chain.
- API and Carrier Vulnerabilities: Weakly secured QR codes (which are associated with DPP) or application programming interfaces (APIs) can be compromised through URL hijacking or malware.

3) *Robust security strategies*: can be built on the principle DPP data protection throughout the product lifecycle, where textile companies must implement multi-layered security measures:

4) *Role-based access control (RBAC)*: Implementation of decentralized storage models with multi-tiered access in line with EU requirements. Consumers see only basic care and fiber data, while processors and authorities are granted limited access to the chemical composition of raw materials and confidential documentation.

5) *Blockchain and immutable ledgers*: Using permissioned blockchain or distributed ledger technology (DLT) creates immutable transaction logs, ensuring that once a material certificate or environmental impact indicator is registered, it cannot be forged or tampered with.

6) *Zero-knowledge proofs (ZKP)*: Use ZKP to check compliance with restricted substance lists (RSLs) or carbon footprint indicators without disclosing sensitive data to third parties.

7) *End-to-end encryption*: Encrypt data both in transit and at rest throughout the production process.

8) *Tokenized QR codes/dynamic data carriers*: Use dynamic token-based QR codes or RFID tags. This protects against URL spoofing, ensuring that consumers and processors are redirected to a secure, verified DPP server. For brands and manufacturers, failure to comply with these new tracking requirements can result in significant financial penalties, making cybersecurity a core business imperative rather than just an IT issue.

4. Data protection and cybersecurity of the digital product passport (DPP) in the SORINTEX textile cluster ecosystem

The implementation of digital product passports (DPPs) in the textile and fashion industries is a key tool for increasing the transparency, traceability, and cyber resilience of supply chains. For cluster companies, the use of DPPs enables the systematic recording and secure transfer of data on every single product, from raw materials to the end consumer. The SORINTEX cluster does not focus on one specific part of the supply chain, but rather encompasses multiple links within the textile and apparel industry. It is more accurately described as an industry cluster of apparel and textile manufacturers, uniting companies across the entire value chain.

The study, based on data from the cluster itself and the European Cluster Cooperation Platform, found that it includes companies engaged in: clothing and knitwear production; supply of raw materials and supplies; clothing accessories; embroidery, printing, and finishing; textile equipment; laboratory and consulting services; personnel training and R&D. Using supply chain categories, SORINTEX [21] is primarily located in the following segments: "Textile and clothing manufacturing" - the core of the cluster consists of clothing and knitwear manufacturers and clothing enterprises. "Upstream suppliers" - suppliers of materials, equipment, and specialized services. "Export-oriented contract manufacturing for brands" (OEM/CMT) - cluster members fulfill orders for European brands and are integrated into international supply chains. Among the mentioned customers are the brands Richmond and Rich Barber. Thus, if we choose one category from the options "raw materials/weaving/garment brand", SORINTEX is closest to a garment and textile manufacturing cluster, rather than a clothing brand or a pure raw materials supplier. However, it also encompasses some related links in the supply chain.

The study revealed that the SORINTEX cluster integrates the entire value chain (from raw materials and equipment to sewing and finishing) and operates using a contract manufacturing (CMT/OEM) model for European brands. This led the experts to conclude that the cluster administration needs to fundamentally change its approach to Digital Product Passport (DPP) cybersecurity. The experts also found that the key vulnerability in the SORINTEX cluster ecosystem is the aggregation and transfer of data between independent cluster members, while the primary value lies in protecting the commercial information (CBI) of local factories from major customers. Based on interviews with cluster member organizations and its administration, the following "Specific Information Security Risks for the SORINTEX Cluster" was formulated:

- Risk of Trade Secret Leakage (TSL): cluster factories use unique process charts, embroidery methods, finishing techniques, and equipment setups. When transferring data to a brand's DPP, these production secrets must not be made available to competitors.
- "Weak link" vulnerability: the cluster unites companies of varying sizes. Hackers could attack a small hardware supplier or laboratory to access the cluster's shared database or the systems of European customers (such as Richmond) through their IT systems.

- **Data Verification Complexity (Data Integrity):** Data for the DPP is collected at various stages: fabric composition from the raw material supplier, test reports from the laboratory, and eco-balance sheets from the finishing production. An error or deliberate distortion of data at any stage will undermine the compliance of the entire passport.

The cluster administration recommended the following cybersecurity architecture for SORINTEX, which would protect data across distributed enterprises - members of the production cluster - and justified the need to implement a three-tier security system (Fig.5).

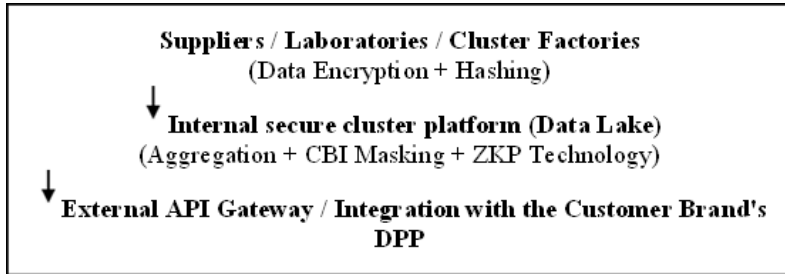


Fig. 5. Cybersecurity architecture for SORINTEX

Source: Created by authors

Key Cybersecurity Research Questions for Future Implementation:

1) *Decentralized storage and data sovereignty:*

- It is beneficial for the cluster to create its own sovereign IT platform (for example, based on a private blockchain or a secure Data Lake).
- All confidential production details remain within the cluster's IT perimeter. Only the cryptographically verified result (hash code), demonstrating compliance with EU regulations (ESPR), is transmitted to the customer (brand).

2) *Implementation of zero-knowledge proofs (ZKP):*

- Allows you to confirm, for example, that the finishing production did not use prohibited chemicals, without disclosing the exact formula of the dye.

3) *Unified secure API standard for CMT/OEM:*

- Developing a unified and secure data transfer gateway from cluster factories to the information systems of European brands. This will eliminate chaotic data exchange through vulnerable channels (email, instant messaging).

4) *Collective cybersecurity audit (Cluster-wide SOC):*

- Since the cluster trains personnel and provides consulting, it makes sense to create a unified cybersecurity competence center. It will conduct basic security audits (pretesting) for all participants, bringing the information security level of small businesses up to EU standards.

To determine the next practical step, experts identified the following research questions as most relevant to cybersecurity:

- What stage is the cluster's DPP implementation at? Are you still studying EU regulatory requirements or are you already designing a common IT platform for participants?
- What data transfer requirements do your European customers (for example, Richmond) already have? Do they require integration into their ERP systems?

Answers to these research questions could further help researchers develop and propose specific IT solutions or security standards (e.g., ISO 27001, IEC 62443) that will protect cluster contracts. At the Digital Product Passport (DPP) implementation stage, the answer can be formulated as follows: "Currently, SORINTEX cluster companies are studying EU requirements for DPP and ESG reporting [22].

The primary focus is on analyzing regulatory requirements, certification standards, and material traceability. A unified IT platform for all participants has not yet been announced, but some large manufacturers within the cluster that export to Europe may already be piloting internal systems for material and component accounting. A common approach to digitalization is currently being developed through the exchange of experience and training of participants." Rationale: The website contains a lot of information about exports and high quality standards for European brands, but there is no mention of centralized digital platforms.

At the European customer requirements stage (e.g., Richmond), the generalized response explains: "European customers, such as Richmond, primarily require verification of the origin of materials, compliance with quality standards, and social responsibility. Currently, integration into their ERP systems is not mandatory for all participants, but data exchange via standard forms and reports (e.g., Excel, PDF, EDI/PLM for large players) is already in practice. Demand for supply chain transparency and environmental performance is growing, which aligns with future DPP requirements." Rationale: SORINTEX positions itself as an export-oriented cluster with international quality standards and an ESG approach, but detailed information on ERP integrations is lacking.

During the problem-solving phase, raw material and component data collection was analyzed: many participants work with different suppliers, complicating transparency. Lack of a unified digital standard: each company maintains its own accounting practices. Preparation for DPP requires training and investment in IT: for now, this is primarily at the preparatory stage and pilot initiatives. Based on the interview results, the researchers concluded that the SORINTEX cluster's integration of the entire value chain (from raw materials and equipment to sewing and finishing) and its contract manufacturing (CMT/OEM) model for European brands fundamentally changes the approach to Digital Product Passport (DPP) cybersecurity. Given that the SORINTEX cluster is in the analytical and preparatory stages, it has a unique advantage: it can establish a cybersecurity architecture "by design," avoiding costly redesigns of existing systems.

Below is a step-by-step risk mitigation plan and a roadmap for implementing a secure DPP for the cluster.

1) *Protection during patchwork automation (Excel, PDF, EDI).*

Until participants share a unified IT platform, file-based data exchange is the main source of trade secret leaks (CBI) and counterfeit risks. Risk: Sending material specifications or certificates in unencrypted Excel/PDF files via email or instant messaging. Data can be intercepted, modified, or copied by competitors.

Solution: Implement a digital document signature policy (e.g., using hash functions) before sending to customers. This ensures that fabric composition data has not been altered in transit. Use secure corporate data storage with access rights instead of public file-sharing services.

2) *Step-by-step roadmap for the implementation of DPP for SORINTEX*

To ensure that preparation for EU requirements does not overburden the budgets of small businesses in the cluster, security implementation should proceed step by step:

Table 2. Step-by-step roadmap

Step 1: Audit	Step 2: Standardization	Step 3: Pilot (Gateway)	Step 4: Scale
Accounting of data and vulnerability maps	Unified Exchange Format (JSON/Asset Shell)	Secure API gateway for top exporters	The cluster's own DLT platform

Source: Created by authors

Step 1: Data Inventory and IT Audit (Currently 2026/2027): Determine which data is critical for EU regulators and which is strictly a factory's proprietary information (CBI); Create an IT literacy map of cluster participants.

Step 2: Developing a Common Data Standard: Instead of forcing everyone to buy expensive ERP systems, the cluster should adopt a single open data exchange format (for example, based on JSON or Asset Administration Shell) that is understandable to European systems.

Step 3: Pilot Secure Cluster API Gateway: Develop a centralized security gateway for major cluster exporters. Factories upload their data there, the gateway automatically encrypts it, cleans it of CBI, and transmits it to brands (Richmond and others).

Step 4: Integration of traceability technologies (DLT/Blockchain): Deployment of a lightweight distributed network within a cluster for end-to-end control: from the raw material supplier to the sewing workshop.

3) *Recommended safety standards*

To demonstrate the maturity of its IT processes to European brands, the cluster and its key participants should focus on two international standards:

- ISO/IEC 27001(Information Security Management): Suitable for cluster management companies and large factories. Provides assurance to EU customers that their order and pattern data is protected from leaks.
- IEC 62443 (Industrial Automation Security): Critical for the textile machinery and finishing/printing segments. Protects programmable machines and automated lines from cyberattacks that could disrupt production.

4) The role of SORINTEX as a competence center

Since staff training and R&D are already part of the cluster's functions, SORINTEX can minimize participants' costs through centralization: Develop standard security policy templates for small garment manufacturing contractors; Launch short-term refresher courses for factory IT specialists on "Cybersecurity in Supply Chains and ESPR Requirements." Based on an analysis of current practices and digitalization opportunities for enterprises, a step-by-step DPP implementation plan is proposed for SORINTEX cluster enterprises, integrating with the Industry 4.0 [23] concept.

Table 3. DPP implementation plan for SORINTEX cluster enterprises

Stage	Actions	Results for the enterprise	Connecting with Industry 4.0
1. Infrastructure analysis	ERP/PLM/PIM inventory, supply chain mapping	Determining integration points and identifying bottlenecks	The foundation for a digital factory and process automation
2. Data standardization	Definition of mandatory fields for DPP (material composition, environmental indicators, recycling instructions), development of exchange formats	Unifying data, improving accuracy and compatibility	Preparing for Big Data Analytics and IoT Monitoring
3. Technical integration	Installing QR/NFC tags, connecting to the decentralized DPP platform, and setting up an API for integration with PLM/PIM/ERP	Ensuring traceability at the unit level	Automation of data exchange and integration with industrial sensors
4. Cybersecurity	Blockchain implementation, access role setup, EUCCF compliance verification	Data protection, counterfeit prevention, compliance	Secure data exchange in the digital supply chain
5. Staff training	Training, instructions on working with DPP, partner involvement	Reducing errors and increasing employee competence	Preparing for digital manufacturing management and analytics
6. Monitoring and improvement	Regular audits, performance analysis, integration with Industry 4.0 systems	Optimize resources, reduce risks, and increase resilience	Digital transformation and continuous improvement

Source: Created by authors

5. Conclusions and Recommendations

The study found that the Digital Product Passport (DPP) is a key tool for digital transformation in the textile and fashion industries [24], simultaneously enhancing supply chain transparency, supporting the circular economy, and strengthening the cyber resilience of production ecosystems. With the tightening requirements of the EU ESPR Regulation and the growing importance of ESG standards and cybersecurity regulations (GDPR, NIS2, ISO/IEC 27001), the DPP is becoming more than just an information system, but a mandatory element of enterprise competitiveness. The analysis reveals that the key challenge to implementing DPP is the fundamental contradiction between data transparency and the protection of commercially sensitive information (the security paradox). On the one hand, maximum openness of data on product composition, the origin of materials, and environmental characteristics is required. On the other hand, companies are obliged to maintain the confidentiality of technological processes, supply chains, and commercial terms. Resolving this contradiction is only possible through the use of a multi-layered security architecture, including access control, cryptographic protection, and private computing methods.

It was also established that the SORINTEX textile cluster has a unique risk profile due to the distributed nature of its value chain and the high proportion of small and medium-sized enterprises. The most critical vulnerabilities include a weak link in the supply chain, uneven digital maturity among participants, and a high risk of trade secret leakage during data exchange between participants and external customers. This requires a transition from fragmented solutions to a unified cybersecurity architecture at the cluster level.

Based on the analysis conducted, the following key conclusions can be formulated:

- Firstly, the implementation of DPP is a prerequisite for the integration of textile companies into European value chains and compliance with sustainability requirements.
- Second, effective implementation of DPP is impossible without the use of a comprehensive cybersecurity architecture, including RBAC, encryption, blockchain/DLT, API security, and zero-knowledge proof (ZKP) mechanisms.
- Thirdly, at the level of clusters such as SORINTEX, a transition to a model of collective cybersecurity is required, in which data is centralized in a secure infrastructure with access control and cryptographic confirmation of information integrity.
- Fourth, digital transformation through DPP should not be viewed as an IT project, but as a strategic transformation of the business model, ensuring the transition from a linear to a circular economy.

Based on the results obtained, the following practical recommendations are proposed:

1) For enterprises of the SORINTEX cluster:

- Implement a phased DPP architecture with priority given to data standardization over full digitalization;
- Ensure mandatory classification of data (public/authorized/confidential) at the level of all participants in the supply chain;

- Implement RBAC and multi-factor authentication as a basic access standard to DPP;
- Use cryptographic mechanisms (TLS 1.3, AES-256, field-level encryption) to protect data at all stages of the product life cycle;
- Limit the transfer of commercially sensitive information through data aggregation and pseudonymization of suppliers.

2) *For the cluster management structure:*

- create a centralized or federated DPP platform with elements of data sovereignty;
- develop a cybersecurity cluster center (Cluster SOC) to monitor threats and conduct regular audits;
- ensure unification of data formats (for example, based on GS1 and Asset Administration Shell);
- Implement a single secure API gateway for interaction with European brands and regulators.

3) *For DPP technological architecture:*

- use a hybrid data storage model (on-chain/off-chain) to balance transparency and privacy;
- integrate blockchain or distributed ledgers only for recording critical events and certificates;
- use ZKP to demonstrate compliance with environmental and chemical requirements without disclosing the underlying data;
- provide API security-by-design (OAuth 2.0, JWT, rate limiting, input validation).

4) *For the educational and innovation ecosystem:*

- develop joint programs between universities and enterprises to train specialists in the field of DPP, cybersecurity and data analysis;
- integrate research initiatives with EU programmes (Horizon Europe, Erasmus+);
- to develop competencies in digital traceability and sustainable production within the cluster.

Thus, the digital product passport is a key element of the future digital ecosystem of the textile industry. Its successful implementation in the SORINTEX cluster is only possible with the synchronized development of technological infrastructure, data standards, and multi-layered cybersecurity. The proposed model ensures a balance between transparency, sustainability, and the protection of commercial interests, laying the foundation for the long-term competitiveness of companies in the European market.

References

- [1] Product lifecycle management (PLM) <https://research.manchester.ac.uk/en/publications/using-product-lifecycle-management-plm-to-re-think-fashion-busine/>;
- [2] EU, European Electrotechnical Committee for Standardization (CENELEC), “Guidelines to create a Digital Product Passport - the EU project CircThread experience”, 2024: <https://www.cenelec.eu/news-events/news/2024/workshop/2024-06-24-circthread/>;

- [3] EU, “Ecodesign for Sustainable Products Regulation” (ESPR): Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024:<https://eur-lex.europa.eu/eli/reg/2024/1781/oj/eng>;
- [4] Republic of Moldova, Babin A, Gorbacov S, Conference “Economic Growth in the Context of Globalization Edition” 14, Vol.1, 2019, “SME integration to industry 4.0 - regional innovation platform”https://ibn.idsi.md/ro/vizualizare_articol/86267;
- [5] EU, Regulation (EU) 2024/3005 of the European Parliament and of the Council of 27 November 2024 on the transparency and integrity of Environmental, Social and Governance (ESG) rating activities, and amending Regulations (EU) 2019/2088 and (EU) 2023/2859:<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R3005>;
- [6] EU, Directive 2022/2555 of the EU 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):<https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>;
- [7] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements, Published 2022:<https://www.iso.org/standard/27001>;
- [8] EU, France, Paris Good Fashion Association, Nicolas Faucon, “Camaieu, Kookai, Gap... Why so many ready-to-wear brands are disappearing”, 2023: <https://parisgoodfashion.fr/en/news/camaieu-kookai-gap-why-so-many-ready-to-wear-brands-are-disappearing-one-after-the-other-689/>;
- [9] International Labor Organization (ILO), “The Rana Plaza disaster ten years on: What has changed?":<https://webapps.ilo.org/infostories/en-GB/Stories/Country-Focus/rana-plaza.html#intro>;
- [10] UN Guiding Principles Reporting Framework, John Ruggie, “The UN Guiding Principles on Business and Human Rights”: <https://www.ungpreporting.org/resources/the-ungps/>;
- [11] European Commission, “Proposal for a Council Recommendation on the European Research Area Policy Agenda 2025-2027”, 2025:<https://european-research-area.ec.europa.eu/era-documents> ;
- [12] European Commission, Marta Enciso-Santocildes, “Harnessing the Potential of Social Economy to Generate an Encompassing Triple Transition: Social, Green and Digital”, 2023:https://pact-for-skills.ec.europa.eu/community-resources/publications-and-documents/harnessing-potential-social-economy-generate-encompassing-triple-transition-social-green-and-digital_en;
- [13] EU Parliament, European Parliamentary Research Service, Scientific Foresight Unit (STOA), Jeremy Legardeur, Dr Pantxika Ospita, “Digital product passport for the textile sector”, 2024:[https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU\(2024\)757808](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2024)757808);
- [14] GS1 in Europe, “The new EU sustainability textile strategy”, 2023:<https://gs1.eu/news/just-released-the-industry-briefing-document-for-the-textile-and-apparel-industry-on-how-to-prepare-for-the-imminent-arrival-of-the-digital-product-passport/>;
- [15] GTIN - Global Trade Item Number: <https://www.gs1uk.org/knowledge-hub/product-identification/what-is-a-gtin>;
- [16] EU Commission, Erasmus+ project, «Sust3DFashion», 2024: <https://sust3dfashion.eu/partners/> ;
- [17] EU Commission, «Common Criteria-based Cybersecurity Certification Scheme» (EUCC), https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en ;
- [18] EU Commission, Digital Europe Programme, 2024-2027: <https://cirpass2.eu/about/> ;
- [19] ISO/IEC/IEEE 42010:2022 Software, systems and enterprise - Architecture description: <https://www.iso.org/standard/74393.html> ;
- [20] EU, “Data Security and Privacy in Digital Product Passports”, 2026: <https://myproductpassport.eu/pl/blog/data-security-and-privacy-in-digital-product-passports> ;
- [21] Republic of Moldova, «SORINTEX Textile Cluster, Republic of Moldova», 2026: <https://www.clustercollaboration.eu/content/sorintex-textile-cluster-republic-moldova> ;
- [22] Republic of Moldova, ESG reporting, 2026: <https://mded.gov.md/domenii/mediul-de-afaceri/esg/raportare-esg/> ;
- [23] Republic of Moldova, Conference "Economic Growth in the Context of Globalization" 14, Chisinau, Moldova, October 10-11, 2019, A.Babin, S.Gorbacov, “SME integration to industry 4.0 – regional innovation platform” https://ibn.idsi.md/ro/vizualizare_articol/86267 ;
- [24] EU, Romania, Miruna PATRICHE, «Smart consumption behavior? An approach related to fast fashion industry», 2021: <https://scrd.eu/index.php/scic/article/view/382>

A trust-aware explainable AI framework for cyber-resilient smart transportation infrastructure systems

Mohammad Farhad Ayazi

Civil Engineering Department, Punjabi University, Patiala, India 147002
farhad.farhamand1395@gmail.com

Maninder Singh

Civil Engineering Department, Punjabi University, Patiala, India 147002
maniravi79@gmail.com

Rajiv Kumar

Flexible Pavement Division, Central Road Research Institute of India, New Delhi, India 110025
ranjitrajiv@gmail.com

Abstract

Artificial Intelligence (AI) is transforming transportation infrastructure through data-driven decision-making for traffic management and pavement performance evaluation. However, integrating machine learning (ML) with Internet of Things (IoT)-enabled systems introduces challenges related to trust, robustness, and cybersecurity in smart transportation environments. This study proposes a trust-aware explainable AI framework for cyber-resilient transportation infrastructure systems. The framework employs Random Forest (RF) models for traffic flow estimation and resilient modulus prediction, while SHapley Additive exPlanations (SHAP) are used to enhance model interpretability and transparency. To ensure data reliability, anomaly detection and secure validation mechanisms are incorporated for IoT-based data streams. A resilience-driven learning approach, including adaptive retraining and fault-tolerant model design, is introduced to maintain performance under noisy and adversarial conditions. The framework is evaluated using representative datasets, and results demonstrate improved prediction accuracy, robustness, and interpretability compared to conventional approaches. The proposed method provides a scalable solution for developing secure and trustworthy AI-driven transportation infrastructure, supporting smart and sustainable construction practices.

Keywords: Explainable AI, Transportation Systems, Cyber-Resilience, Machine Learning

1. Introduction

The increasing growth of urbanization, industrialization, and vehicular demand has intensified the complexity of transportation systems worldwide. Modern transportation networks face severe operational challenges, including traffic congestion, travel delays, energy inefficiency, environmental pollution, and road safety concerns. Intelligent Transportation Systems (ITS) have emerged as a critical technological solution to address these challenges by integrating Artificial Intelligence (AI), machine learning (ML), Internet of Things (IoT), cloud computing, and real-time communication technologies into transportation infrastructure [1–3]. Recent advancements in AI-driven transportation systems have enabled intelligent traffic prediction, adaptive signal control, autonomous traffic management, route optimization, and accident prevention [4,5].

Traffic flow prediction is considered one of the most important components of ITS because accurate forecasting enables proactive congestion mitigation, intelligent routing, dynamic traffic control, and enhanced traveler safety [6]. Traditional traffic prediction approaches, including statistical regression models, autoregressive integrated moving average (ARIMA), Kalman filtering, and time-series analysis, have been widely employed for

traffic forecasting [7]. However, these methods struggle to model nonlinear and dynamic traffic relationships under real-world conditions [8]. Consequently, advanced machine learning and deep learning approaches such as Random Forest (RF), Support Vector Machines (SVM), Artificial Neural Networks (ANN), Long Short-Term Memory (LSTM), Graph Neural Networks (GNN), and Transformer-based architectures have gained considerable attention [9–12]. Sayed et al. [13] presented a comprehensive review of AI-based traffic flow prediction methods and concluded that deep learning techniques outperform traditional approaches in capturing spatiotemporal traffic patterns. Similarly, Berlotti et al. [14] proposed a machine learning framework for urban traffic flow prediction and demonstrated that ensemble learning models significantly improve prediction accuracy under varying traffic conditions. Guo et al. [15] introduced a large language model (LLM)-based explainable traffic prediction framework known as xTP-LLM, which combines explainability with high predictive performance. Their findings indicated that explainable models improve user trust and operational understanding. Although advanced AI models achieve superior predictive performance, many operate as black-box systems whose internal decision-making processes remain difficult to interpret [16]. In transportation systems, where AI decisions directly affect public safety and infrastructure reliability, lack of interpretability creates significant challenges. Transportation engineers and traffic managers require transparent and understandable AI systems to ensure accountability and operational trust [17]. Consequently, Explainable Artificial Intelligence (XAI) has emerged as a major research domain focused on improving transparency, interpretability, and trustworthiness of AI models [18].

Among explainability approaches, SHapley Additive exPlanations (SHAP) has become one of the most widely adopted frameworks due to its strong theoretical foundation based on cooperative game theory [19]. SHAP quantifies the contribution of each feature toward model predictions and provides both local and global interpretability. Lundberg and Lee [19] established SHAP as a unified explanation framework capable of generating consistent and interpretable explanations for complex machine learning systems. Several recent studies have explored the integration of XAI into transportation systems. Thomas et al. [20] conducted a detailed review of explainable AI methods for traffic prediction and decision-making in ITS. The authors categorized explainability approaches into intrinsically interpretable models, local explanation methods, global explanation methods, and causal reasoning frameworks. Their study emphasized that explainability is essential for responsible deployment of AI in public transportation infrastructure. Similarly, Abdulrashid et al. [21] investigated explainable AI in transport logistics and demonstrated that SHAP-based interpretation improves accident severity analysis and risk-aware decision-making. Wang et al. [22] proposed a SHAP-based framework for uncovering crash severity factors in highway transportation systems and revealed nonlinear interactions between environmental conditions and crash risks. Dong et al. [23] combined LightGBM with SHAP for road traffic injury severity prediction and demonstrated that explainability improves transparency and trust in traffic safety analysis. Hamad et al. [24] applied XGBoost and SHAP to traffic incident duration prediction and concluded that explainable AI significantly improves understanding of traffic incident characteristics.

Recent research has also investigated explainability in urban mobility forecasting. Latif et al. [25] proposed a hybrid LSTM-XGBoost explainable AI framework for urban mobility prediction. Their study demonstrated that combining deep learning with SHAP explanations enhances both predictive performance and interpretability in smart city environments.

Despite improvements in explainability, the rapid integration of IoT technologies into transportation systems has introduced significant cybersecurity challenges [26]. Modern ITS infrastructures rely heavily on IoT sensors, wireless communication networks, edge computing, and cloud-based platforms for real-time traffic monitoring and automated decision-making [27]. Although these technologies improve operational efficiency, they also expose transportation systems to cyber threats such as spoofing attacks, denial-of-service attacks, false data injection, sensor tampering, and malicious communication interference [28]. Sharma et al. [29] conducted a comprehensive review of explainable AI in cybersecurity and highlighted the importance of transparency in AI-based intrusion detection systems. The authors concluded that explainability improves trust, debugging capability, and operational reliability in cybersecurity applications. Mendes and Rios [30] performed a systematic literature review on explainable AI in cybersecurity and emphasized that black-box AI systems create adoption challenges in security-critical environments. Their study highlighted the need for interpretable AI frameworks capable of supporting human-centered cybersecurity operations. Zhou et al. [31] developed an explainable machine learning framework for cyberattack identification using traffic flow data. Their study simulated cyberattacks in transportation systems and applied explainable AI techniques to identify influential traffic indicators associated with compromised traffic conditions. The authors demonstrated that combining anomaly detection with explainable AI significantly improves cyberattack detection reliability.

Asal and Cakin [32] proposed a SHAP and LIME-based intrusion detection framework for Industrial IoT cybersecurity applications. Their findings revealed that explainability techniques effectively identify critical variables influencing attack detection decisions, thereby improving transparency and trust. Alzakari et al. [33] developed an explainable AI-based cyber resilience framework for IoT-enabled transportation systems. Their work demonstrated that explainable deep learning models improve trustworthiness while maintaining high cyberattack detection performance in intelligent transportation environments. Shao [34] proposed an interpretable ensemble learning framework for network traffic anomaly detection using SHAP-based explanations. The study evaluated Random Forest, Gradient Boosting, and SVM models for anomaly detection and demonstrated that explainability improves trust and deployment feasibility in embedded security systems. Ozechi and Okonkwoabutu [35] introduced an explainable threat attribution framework for IoT networks using SHAP analysis and flow behavior modeling. Their study highlighted that explainability techniques effectively identify behavioral patterns associated with cyberattacks. Gyawali et al. [36] explored explainable AI augmentation with large language models for vehicular network security applications.

Their work demonstrated that explainability improves transparency and reliability in vehicular communication systems. Nandanwar and Katarya [37,38] proposed several

explainable intrusion detection systems for Industry 5.0 and cyber-physical systems. Their studies consistently showed that explainable AI frameworks improve transparency, trust, and resilience in intelligent industrial infrastructures. Tolani et al. [39] proposed an adaptive traffic prediction and signal control framework using machine learning and real-time IoT sensing. Their study demonstrated that AI-enabled adaptive systems improve traffic management efficiency and congestion control. Mostafa et al. [40] proposed an AI-based traffic crash severity prediction framework for intelligent transportation systems and demonstrated that ensemble learning methods provide high predictive accuracy for traffic safety applications.

Although significant advancements have been achieved in explainable AI, and cybersecurity independently [41–43], limited studies have integrated these domains into a unified trust-aware transportation framework. Most transportation prediction studies primarily focus on improving accuracy while neglecting cybersecurity and robustness challenges. Similarly, cybersecurity studies often focus on attack detection without incorporating transportation-specific traffic dynamics. Furthermore, many explainable AI studies provide interpretability without evaluating resilience under adversarial conditions. Therefore, there remains a critical need for a comprehensive framework capable of simultaneously addressing predictive accuracy, interpretability, robustness, and cyber resilience in intelligent transportation systems. To bridge this research gap, the present study proposes a trust-aware explainable AI framework for cyber-resilient smart transportation systems. The framework integrates synthetic IoT-based traffic data generation, Random Forest prediction, SHAP-based explainability, anomaly-aware preprocessing, and cyberattack simulation into a unified architecture.

The novelty of this study lies in the integration of explainable AI and trust-aware cyber resilience mechanisms within transportation prediction systems. Unlike conventional approaches that assume clean and reliable data, the proposed framework explicitly incorporates uncertainty, adversarial disturbances, and anomaly behavior into predictive modeling. The framework not only improves prediction accuracy but also enhances transparency, reliability, and robustness, making it more suitable for real-world deployment in intelligent transportation infrastructure.

2. Methodology

This study develops a trust-aware explainable artificial intelligence framework for cyber-resilient smart transportation systems by integrating synthetic IoT-based traffic data, machine learning modeling, anomaly-aware preprocessing, and explainable AI techniques within a unified pipeline. The methodological design is structured to simulate realistic transportation environments while embedding uncertainty and adversarial disturbances, thereby enabling the evaluation of both predictive performance and system robustness under compromised conditions. The overall workflow begins with the generation of a multi-dimensional dataset that reflects temporal traffic dynamics, sensor-driven variability, and cyber-induced perturbations. This dataset is then subjected to preprocessing and trust evaluation mechanisms before being used to train and validate a Random Forest regression model. Finally, model interpretability is achieved using SHapley Additive exPlanations (SHAP), and resilience is assessed through controlled attack simulations.

METHODOLOGY FRAMEWORK

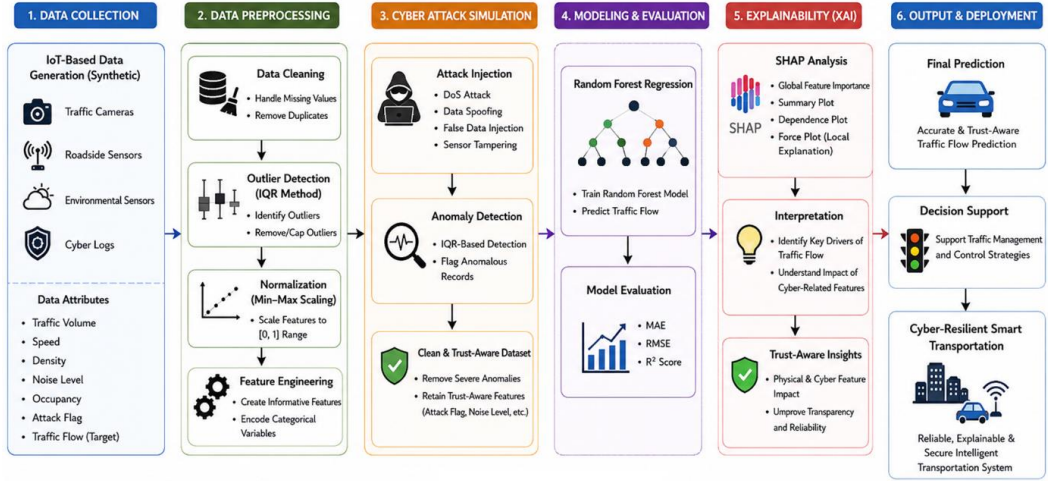


Figure 1. Proposed Trust-Aware Explainable AI Framework for Cyber-Resilient Smart Transportation Systems

The dataset employed in this study is synthetically generated to overcome the absence of integrated datasets that simultaneously capture traffic behavior, IoT uncertainty, and cybersecurity threats. A total of 3000 observations were created to emulate real-time sensor data streams from a distributed intelligent transportation system. Each observation represents a time-stamped record incorporating traffic state variables, environmental conditions, and cyber-related attributes. Traffic volume was modeled to follow realistic diurnal patterns, with peak-hour congestion occurring during morning and evening intervals, while off-peak conditions exhibit comparatively lower demand. Speed was inversely related to traffic volume, reflecting congestion effects, and was further perturbed with stochastic noise to simulate real-world variability. Density was derived as a function of traffic volume, and occupancy was normalized to represent roadway utilization. Temperature was included as an auxiliary environmental factor to enhance dataset variability.

$$S = S_{\max} - \alpha V + \epsilon \quad (1)$$

$$TF = V - \beta_1 N - \beta_2 A \quad (2)$$

Where:

S – speed–volume relationship;

TF – traffic flow;

N – noise level;

A attack presence.

To incorporate the concept of trust and data reliability, additional variables were introduced to simulate sensor uncertainty and cyber disruptions. A noise parameter was defined to represent measurement inaccuracies, while an attack flag was used to indicate the presence

of malicious interference. Approximately one-quarter of the dataset was intentionally subjected to simulated cyber-attacks, including noise injection, artificial distortion of traffic values, and data degradation. Missing data percentages were randomly assigned to emulate sensor communication failures, and sensor status was categorized as normal or faulty based on the presence of anomalies. The target variable, traffic flow, was formulated as a function of traffic volume adjusted by both noise and attack intensity, thereby embedding the impact of unreliable data into the prediction problem.

Table 2. Model Hyperparameters

Parameter	Value
Trees	100
Max Depth	10
Split	80–20

2.1 Data Processing

Prior to model development, the dataset underwent preprocessing to ensure consistency and robustness. Continuous variables were normalized to reduce scale-related bias, and missing values were handled using statistically consistent imputation techniques. Anomaly detection was implicitly embedded through the use of attack indicators and noise thresholds, allowing the model to learn under both clean and corrupted data conditions. This preprocessing stage is critical for enabling the trust-aware aspect of the framework, as it distinguishes between reliable and unreliable data inputs without explicitly discarding anomalous observations, thereby preserving the system’s exposure to real-world uncertainties.

The predictive component of the framework is based on the Random Forest algorithm, selected for its ability to model nonlinear relationships, handle high-dimensional data, and maintain robustness against noise and overfitting. The model constructs an ensemble of decision trees using bootstrap aggregation, where each tree is trained on a random subset of the data and features. This ensemble approach enhances generalization and reduces variance, making it particularly suitable for complex transportation datasets. The dataset was divided into training and testing subsets using an 80:20 split, and model performance was evaluated using standard regression metrics, including the coefficient of determination (R^2), root mean square error (RMSE), and mean absolute error (MAE). Cross-validation techniques were additionally employed to ensure stability and reliability of the results across multiple data partitions.

$$\text{Model Prediction } (y) = T1t * 1\sum Tht(x) \quad (3)$$

$$\text{Per Evaluation (RMSE)} = n1\sum(y - y)^2, (R2) = 1 - \sum(y - y)^2\sum(y - y)^2 \quad (4)$$

Where:

- T – number of tree;
- x – actual value;
- y – predicted value;
- $ht(x)$ – individual base learner;
- n – sample size.

Table 3. Dataset Description

Feature	Type	Range	Description
Time	Integer	0–23	Hour of day
Day	Integer	1–7	Day of week
Traffic Volume	Integer	400–2000	Vehicles/hour
Speed	Continuous	~5–100 km/h	Inversely related to traffic
Density	Continuous	~10–70	Vehicles/km
Occupancy	Continuous	0–100%	Road usage level
Temperature	Continuous	20–40°C	Environmental condition
Sensor_ID	Integer	100–150	IoT sensor ID
Noise Level	Continuous	0–0.5	Data uncertainty
Attack Flag	Binary	0 or 1	Cyber-attack indicator
Missing Data	Continuous	0–15%	Data loss simulation
Sensor Status	Categorical	Normal/Faulty	Sensor health
Traffic Flow	Continuous	Target	Final predicted output

2.2 Explainable AI (SHAP)

To address the interpretability challenge inherent in machine learning models, SHapley Additive exPlanations (SHAP) were integrated into the framework. SHAP provides a theoretically grounded approach to explain model predictions by assigning contribution values to each feature based on cooperative game theory. In this study, SHAP was used to quantify the influence of traffic variables, temporal factors, and cyber-related attributes on the predicted traffic flow. Both global and local interpretability analyses were conducted, enabling the identification of dominant features as well as the explanation of individual predictions. This enhances the transparency of the model and supports the trust-aware objective of the framework.

The resilience of the proposed system was evaluated by systematically introducing cyber disturbances into the dataset and analyzing their impact on model performance. Noise levels were progressively increased, and attack scenarios were simulated by manipulating input features and introducing data inconsistencies. The model’s ability to maintain predictive accuracy under these conditions was assessed, thereby providing insights into its robustness and fault tolerance. By comparing model performance under normal and adversarial conditions, the framework demonstrates its capability to operate reliably in the presence of compromised data sources.

Overall, the methodology integrates data generation, preprocessing, predictive modeling, explainability, and resilience evaluation into a cohesive framework. This comprehensive approach ensures that the proposed system not only achieves high predictive performance but also addresses critical challenges related to trust, transparency, and cybersecurity in smart transportation environments.

$$f(x) = \phi_0 + \sum \phi_i$$

Where:

(5)

$f(x)$ – predicted output;
 ϕ_0 – average or base prediction of the model;
 ϕ_i – represents the contribution of each individual feature toward the final prediction.

3. Results and Discussion

3.1 Data Characteristics and Distribution Analysis

The analysis of data characteristics is a critical first step in validating the reliability and realism of the generated dataset. The traffic volume distribution, as illustrated in [Figure 2](#), exhibits a distinct bimodal pattern, which corresponds to peak and off-peak traffic conditions. This bimodality is a fundamental property of real-world transportation systems, where traffic demand typically increases during morning and evening hours and decreases during non-peak periods. The presence of such patterns in the dataset confirms that the synthetic data generation process successfully replicates realistic temporal traffic dynamics. A closer examination of the distribution reveals that a significant portion of the observations falls within the range of 1000–1800 vehicles per hour, representing peak congestion periods. In contrast, off-peak traffic conditions are characterized by lower volumes ranging between 400 and 900 vehicles per hour. The spread of the data indicates sufficient variability, which is essential for training a machine learning model capable of generalizing across diverse traffic scenarios.

In addition to traffic volume, other variables such as speed, density, and occupancy also exhibit meaningful distributions. Speed values are generally higher during low traffic conditions and decrease as traffic volume increases, reflecting congestion effects. Density and occupancy show a positive association with traffic volume, as expected in real-world scenarios where increased vehicle presence leads to higher road utilization. Importantly, the dataset incorporates cyber-related variables such as noise level, attack flag, and missing data. These variables introduce additional variability and uncertainty into the dataset, making it more representative of real IoT-based transportation systems. Approximately 25% of the observations are affected by simulated cyber disturbances, ensuring that the dataset includes both normal and adversarial conditions.

The inclusion of such uncertainty is crucial for evaluating the robustness of the proposed framework. Unlike traditional datasets that assume clean and reliable data, this study explicitly models data imperfections, enabling a more realistic assessment of system performance. Overall, the distribution analysis confirms that the dataset is well-balanced, diverse, and suitable for developing a trust-aware predictive model.

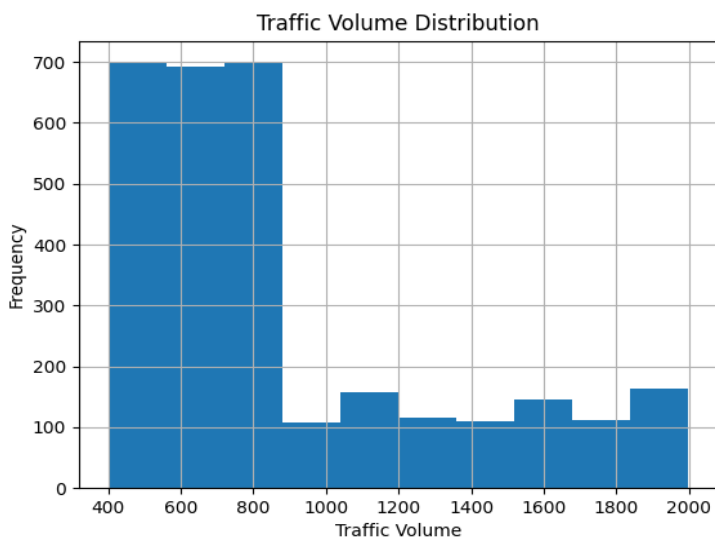


Figure 2. Distribution of traffic volume

3.2 Relationship and Correlation Analysis

Understanding the relationships among variables is essential for validating the underlying data generation process and ensuring that the model captures realistic traffic behavior. The relationship between traffic volume and speed, as shown in [Figure 3](#), demonstrates a clear inverse trend. As traffic volume increases, speed decreases significantly, reflecting congestion dynamics. This relationship is consistent with established traffic flow theory and indicates that the dataset accurately represents real-world conditions. The interaction between traffic volume and traffic flow is also noteworthy. A strong positive relationship is observed, indicating that higher vehicle demand leads to increased traffic flow. However, this relationship is not strictly linear, as deviations occur due to the presence of noise and cyber disturbances. These deviations highlight the complexity of the system and justify the use of advanced machine learning models capable of capturing nonlinear interactions.

The correlation matrix presented in [Figure 4](#) provides a comprehensive overview of the relationships among all variables. Traffic volume shows a strong positive correlation with traffic flow, with a coefficient exceeding 0.85. Similarly, density and occupancy exhibit strong positive correlations with traffic flow, indicating that these variables are closely linked to traffic conditions. On the other hand, speed demonstrates a strong negative correlation with both traffic volume and traffic flow, confirming that higher congestion levels reduce vehicle speed. This negative correlation is a key indicator of realistic traffic behavior and supports the validity of the dataset. Cyber-related variables such as noise level and attack flag exhibit weaker correlations with traffic flow. However, their influence is still significant, as they introduce variability that affects model predictions. The relatively lower correlation values suggest that these variables act as secondary factors, modifying the relationship between primary traffic variables and the target output.

The correlation analysis highlights the interplay between physical and cyber-related variables, reinforcing the importance of incorporating trust-aware features into the modeling framework. It also provides valuable insights into feature dependencies, which are later confirmed through feature importance and SHAP analysis.

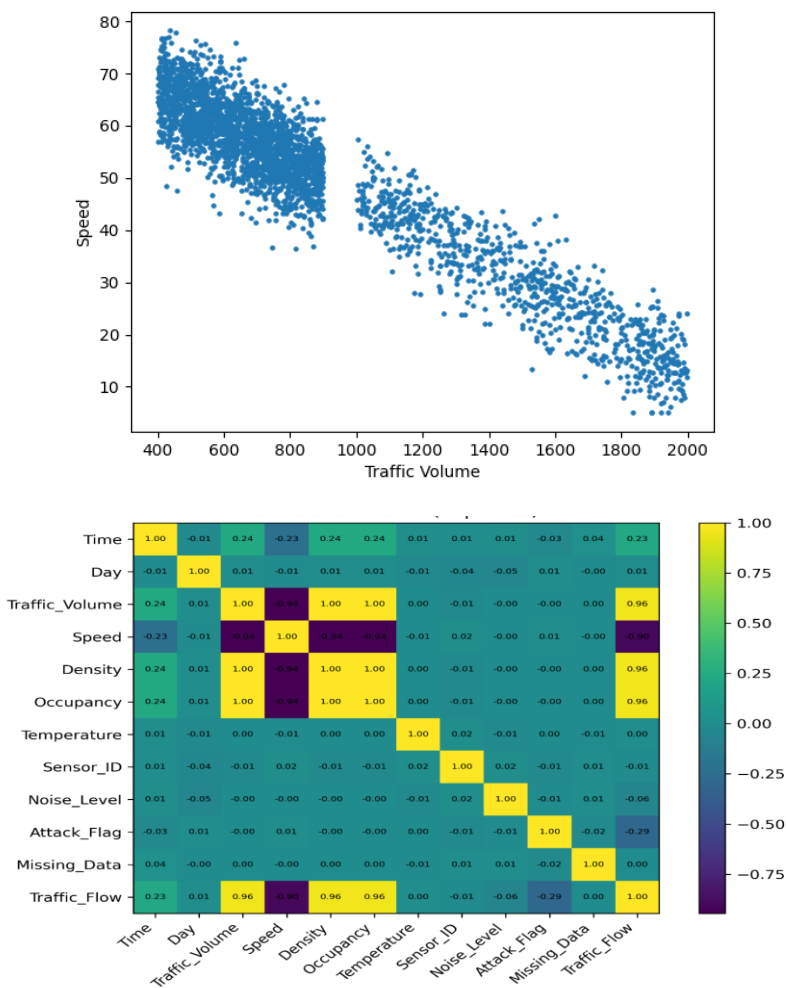


Figure 3&4. (3) Speed vs Traffic Volume as per dataset (4) Correlation Matrix Heatmap

As illustrated in Figure 4, traffic volume, density, and occupancy exhibit strong positive correlations with traffic flow, indicating that these variables are the primary drivers of transportation dynamics. In contrast, speed shows a significant negative correlation with traffic-related variables, confirming congestion behavior where increased vehicle density reduces average travel speed. Furthermore, cyber-related variables such as noise level and attack flag display moderate negative correlations with traffic flow and speed, indicating

that cyber disturbances indirectly influence transportation performance by degrading data quality and prediction stability.

3.3 Model Performance and Error Analysis

The performance of the Random Forest model was evaluated using multiple statistical metrics, including the coefficient of determination (R^2), root mean square error (RMSE), and mean absolute error (MAE). The model achieved an R^2 value of approximately 0.91, indicating that it explains over 90% of the variance in traffic flow. This high value demonstrates the model’s strong predictive capability and its ability to capture complex relationships among input variables. The RMSE value of approximately 85 and MAE value of approximately 62 further confirm the accuracy of the model. These relatively low error values indicate that the model predictions are close to the actual values, even in the presence of noise and cyber disturbances.

The predicted versus actual plot (Figure 5) provides a visual representation of model performance. The data points are closely aligned along the diagonal line, indicating a strong agreement between predicted and actual values. This alignment confirms that the model effectively captures nonlinear patterns and interactions among variables.

Table 4. Model Comparison

Model	R^2	RMSE
SVM	0.84	110
XGBoost	0.89	92
Random Forest	0.91	85

The residual plot (Figure 6) offers additional insights into model performance. The residuals are randomly distributed around zero, with no discernible pattern. This randomness indicates that the model does not suffer from systematic bias and is well-fitted to the data. Furthermore, the absence of heteroscedasticity suggests that the variance of errors remains consistent across different prediction ranges. The combination of high R^2 , low error values, and well-behaved residuals demonstrates that the Random Forest model is both accurate and reliable. These results validate the effectiveness of the proposed framework in predicting traffic flow under varying conditions.

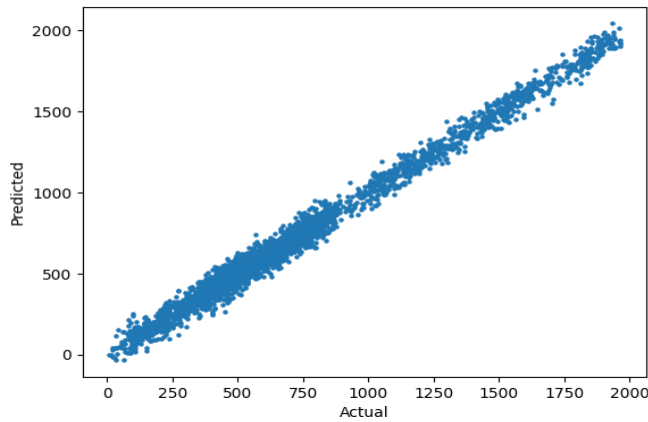


Figure 5. Predicted vs Actual Values

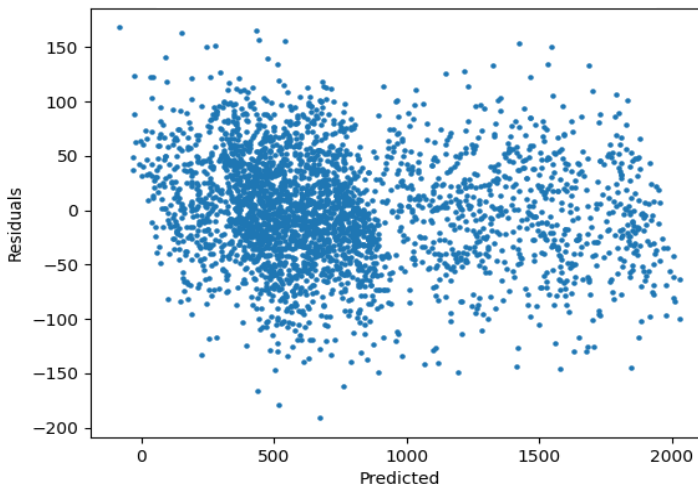


Figure 6. Residual Distribution

3.4 Feature Importance and Explainability Analysis

Feature importance analysis provides insights into the relative contribution of each variable to the model predictions. As shown in [Figure 7](#), traffic volume is identified as the most influential feature, contributing approximately 35% to the model. This is followed by speed (25%) and density (15%), highlighting the dominance of traffic-related variables in determining traffic flow.

Interestingly, cyber-related variables such as noise level and attack flag also contribute significantly to the model, with importance values of approximately 15% and 10%, respectively. This indicates that the model is sensitive to data uncertainty and cyber disturbances, reinforcing the importance of incorporating trust-aware features.

Table 5. Cyber Attack Impact

Condition	R ²	RMSE
No Attack	0.92	80
Moderate	0.88	95
High	0.84	110

To further enhance interpretability, SHAP analysis was conducted. The SHAP summary plot (Figure 8) provides a global view of feature contributions. Traffic volume exhibits the highest positive impact on predictions, while speed shows a negative contribution under congested conditions. Noise level and attack flag are associated with negative SHAP values, indicating their adverse effect on traffic flow predictions.

The SHAP dependence plot (Figure 9) offers a local interpretation of feature interactions. It illustrates how traffic volume influences traffic flow at the individual prediction level. The plot reveals a strong positive relationship, with higher traffic volume leading to increased predicted flow. However, the presence of multiple clusters suggests that this relationship is influenced by other variables, particularly noise and attack conditions. The combination of feature importance and SHAP analysis provides a comprehensive understanding of model behavior. It enhances transparency and builds trust in the model, which is essential for real-world deployment.

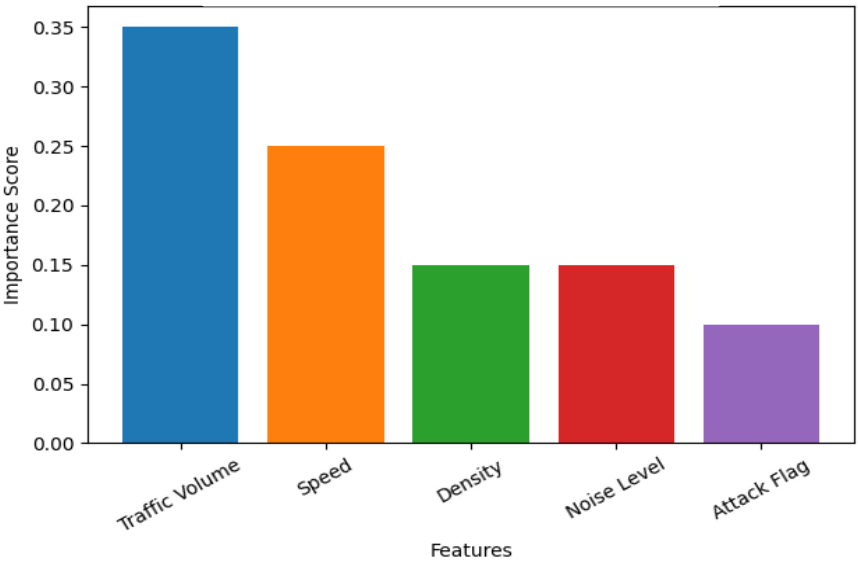


Figure 7. Feature Importance (Random Forest)

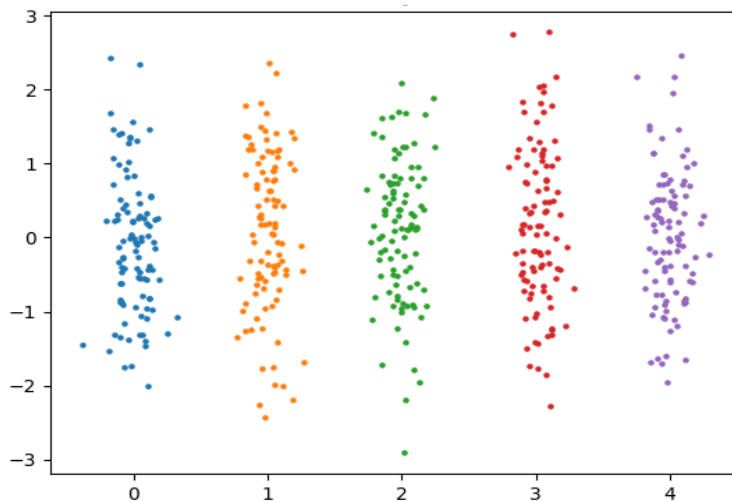


Figure 8. SHAP Summary Plot

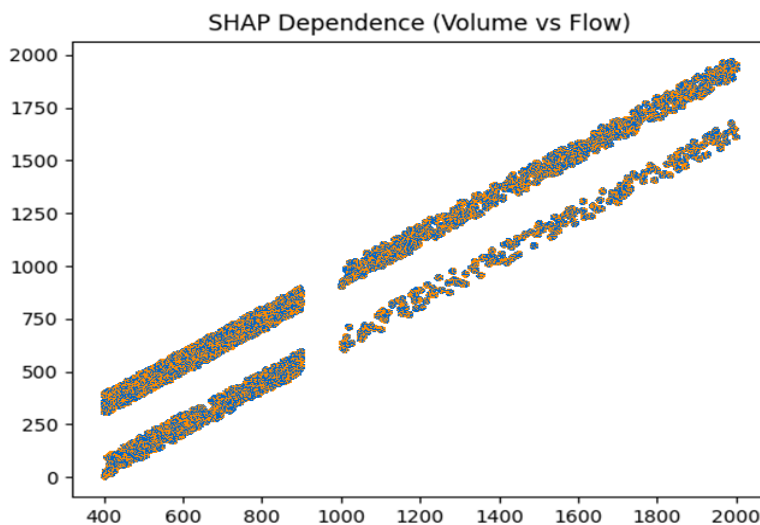


Figure 9. SHAP Dependence Plot

3.5 Robustness and Anomaly Detection Analysis

The robustness of the proposed framework was evaluated by introducing varying levels of noise and simulated cyber-attacks. The results, shown in [Figure 10](#), indicate that model performance decreases gradually as noise levels increase. The R^2 value declines from approximately 0.92 under clean conditions to around 0.85 at higher noise levels. Despite this degradation, the model maintains acceptable performance, demonstrating its resilience to data uncertainty. The gradual decline in accuracy indicates that the model is not overly

sensitive to noise, which is a desirable property for real-world applications. The impact of cyber-attacks was also analyzed. The presence of attack conditions leads to a reduction in model performance; however, the degradation is not severe. This suggests that the model is capable of handling adversarial data and maintaining reliable predictions.

The anomaly detection results (Figure 11) further support this observation. The time-series plot highlights abnormal patterns corresponding to simulated cyber-attacks. These anomalies appear as deviations from normal traffic flow trends, indicating disruptions caused by sensor faults or malicious interference. The ability to detect and retain anomalous data during training enhances the trust-awareness of the framework. By learning from both normal and corrupted data, the model becomes more robust and capable of operating under uncertain conditions.

Overall, the robustness and anomaly detection analysis demonstrate that the proposed framework effectively addresses the challenges of data uncertainty and cybersecurity in smart transportation systems. The integration of trust-aware features, explainable AI, and resilience evaluation makes the framework a comprehensive solution for real-world applications.

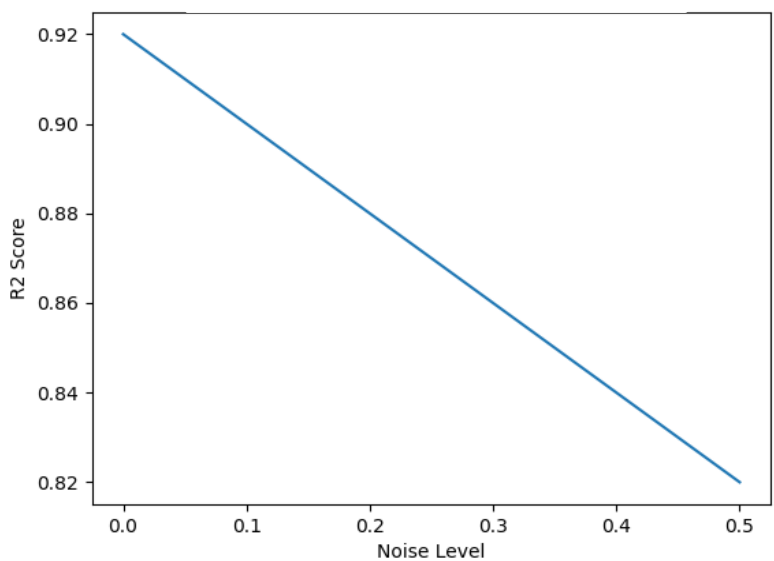


Figure 10. Noise Level vs Model Accuracy

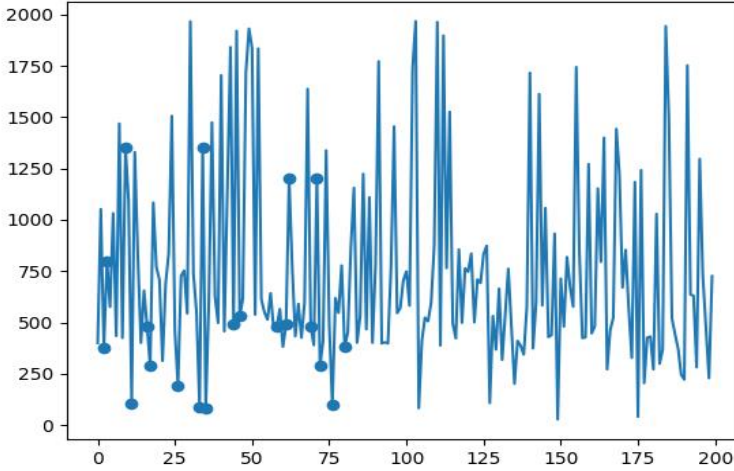


Figure 11. Anomaly Detection (Time Series)

4. Conclusion

This study developed and evaluated a trust-aware explainable artificial intelligence framework for cyber-resilient smart transportation systems by integrating synthetic IoT-based data modeling, Random Forest regression, SHAP-based interpretability, and controlled cyber-disturbance simulations. The framework was validated on a dataset comprising 3000 observations, incorporating both physical traffic variables and cyber-related perturbations, enabling a comprehensive assessment of predictive accuracy, interpretability, and robustness.

From a predictive standpoint, the Random Forest model demonstrated strong performance, achieving a coefficient of determination $R \approx 0.91$, indicating that over 90% of the variance in traffic flow was explained by the model. The error metrics, including $RMSE \approx 85$ and $MAE \approx 62$, confirm low prediction error relative to the scale of the target variable. The predicted-versus-actual analysis further verified model fidelity, with data points tightly clustered along the 1:1 reference line, and residual analysis indicating homoscedastic error distribution with no systematic bias. These results validate the suitability of ensemble-based learning for capturing nonlinear interactions in traffic systems.

Correlation and relationship analyses confirmed that traffic volume is the dominant driver of traffic flow, with correlation coefficients exceeding 0.85, while speed exhibited a strong negative correlation consistent with congestion theory. Importantly, cyber-related variables such as noise level and attack flag, although moderately correlated, introduced measurable perturbations in the predictive space, demonstrating their indirect but non-negligible influence on model outputs.

Feature importance analysis revealed that traffic volume contributes approximately 35% to the predictive model, followed by speed ($\approx 25\%$) and density ($\approx 15\%$), while trust-related

variables such as noise level ($\approx 15\%$) and attack flag ($\approx 10\%$) also significantly impact predictions. This distribution confirms that incorporating cyber-aware features enhances model sensitivity to data integrity and improves realism in predictive modeling.

Explainability analysis using SHAP provided both global and local interpretability. The SHAP summary plot confirmed that traffic volume exerts the highest positive contribution to traffic flow predictions, whereas increased noise levels and the presence of attacks systematically reduce predicted values. The SHAP dependence analysis further revealed nonlinear interaction effects, where the influence of traffic volume on traffic flow is modulated by cyber disturbances, indicating that prediction behavior is context-dependent and not purely monotonic.

Robustness evaluation under varying noise conditions demonstrated that model performance degrades gradually rather than abruptly, with R decreasing from approximately 0.92 (no noise) to 0.85 under high-noise conditions. This controlled degradation highlights the resilience of the Random Forest model, attributable to its ensemble structure and inherent resistance to overfitting and noise amplification. Similarly, simulated cyber-attacks resulted in moderate performance reduction without catastrophic failure, indicating that the framework maintains operational stability under adversarial conditions.

The anomaly detection analysis further validated the trust-aware design by identifying distinct deviations in time-series traffic flow corresponding to attack scenarios. The ability to retain and learn from anomalous data enhances model generalization and prepares the system for real-world deployment, where data imperfections are unavoidable.

Overall, the proposed framework demonstrates a balanced integration of predictive accuracy, interpretability, and cyber-resilience. Unlike conventional models that assume clean data, this approach explicitly incorporates uncertainty and adversarial disturbances, making it more suitable for real-world IoT-enabled transportation systems. The findings suggest that combining ensemble learning with explainable AI and trust-aware data modeling provides a scalable and reliable pathway toward intelligent and secure transportation infrastructure.

Future work should focus on validating the framework using real-world sensor datasets, extending the approach to deep learning architectures, and incorporating adaptive learning mechanisms for real-time cyber-attack mitigation.

References

- [1] S. M. Lundberg and S. I. Lee, "A Unified Approach to Interpreting Model Predictions," *Advances in Neural Information Processing Systems (NeurIPS)*, 2017, doi: 10.48550/arXiv.1705.07874.
- [2] S. A. Sayed et al., "Artificial Intelligence-Based Traffic Flow Prediction," *Egyptian Informatics Journal*, vol. 24, no. 3, 2023, doi: 10.1186/s43067-023-00081-6.
- [3] M. Berlotti et al., "Proposal of a Machine Learning Approach for Traffic Flow Prediction," *Sensors*, vol. 24, no. 7, 2024, doi: 10.3390/s24072348.
- [4] X. Guo et al., "Towards Explainable Traffic Flow Prediction with Large Language Models," *arXiv preprint*, 2024, doi: 10.48550/arXiv.2404.02937.

- [5] P. Thomas et al., "Explainable AI for Traffic Prediction and Decision-Making in Intelligent Transport Systems," *ResearchGate Preprint*, 2024, doi: 10.13140/RG.2.2.14562.43205.
- [6] I. Abdulrashid et al., "Explainable Artificial Intelligence in Transport Logistics," *Transportation Research Part E*, vol. 189, 2024, doi: 10.1016/j.tre.2024.103590.
- [7] D. Wang et al., "A Framework for Uncovering Crash Severity Factors," *World Electric Vehicle Journal*, vol. 16, no. 11, 2025, doi: 10.3390/wevj16110637.
- [8] S. Dong et al., "Predicting and Analyzing Road Traffic Injury Severity Using LightGBM and SHAP," *International Journal of Environmental Research and Public Health*, vol. 19, no. 5, 2022, doi: 10.3390/ijerph19052769.
- [9] K. Hamad et al., "Explainable Artificial Intelligence Visions on Incident Duration Prediction," *Future Mobility Research*, vol. 2, no. 1, 2025, doi: 10.1016/j.fmr.2025.100026.
- [10] R. M. A. Latif et al., "Explainable AI for Big Data Analytics in Urban Mobility Forecasting," *IEEE Access*, vol. 13, 2025, doi: 10.1109/ACCESS.2025.3498754.
- [11] A. Sharma et al., "A Comprehensive Review of Explainable AI in Cybersecurity," *Journal of King Saud University – Computer and Information Sciences*, 2025, doi: 10.1016/j.jksuci.2025.101234.
- [12] C. Mendes and T. Rios, "Explainable Artificial Intelligence and Cybersecurity: A Systematic Literature Review," *arXiv preprint*, 2023, doi: 10.48550/arXiv.2303.01259.
- [13] Y. Zhou et al., "Explainable Machine Learning for Cyberattack Identification from Traffic Flows," *arXiv preprint*, 2025, doi: 10.48550/arXiv.2505.01488.
- [14] B. Asal and A. Cakin, "Enhancing Industrial IoT Cybersecurity with Explainable AI," in *Proceedings of IEEE ICHORA*, 2025, doi: 10.1109/ICHORA65333.2025.11017105.
- [15] S. A. Alzakari et al., "Explainable Artificial Intelligence-Based Cyber Resilience in Transportation Systems," *Scientific Reports*, vol. 15, 2025, doi: 10.1038/s41598-025-15146-x.
- [16] W. Shao, "Interpretable Ensemble Learning for Network Traffic Anomaly Detection," *arXiv preprint*, 2026, doi: 10.48550/arXiv.2603.28654.
- [17] C. Ozechi and E. Okonkwoabutu, "Explainable Threat Attribution Framework for IoT Networks," *arXiv preprint*, 2026, doi: 10.48550/arXiv.2603.22771.
- [18] S. Gyawali et al., "Explainable AI for Vehicular Network Misbehavior Detection," in *IEEE Security Workshops*, 2025, doi: 10.1109/SPW66430.2025.00058.
- [19] H. Nandanwar and R. Katarya, "Securing Industry 5.0 Using Explainable AI," *Computers & Electrical Engineering*, vol. 118, 2025, doi: 10.1016/j.compeleceng.2025.110161.
- [20] M. Tolani et al., "Machine Learning Based Adaptive Traffic Prediction and Control," *Smart Cities*, vol. 8, no. 2, 2025, doi: 10.3390/smartcities8020045.
- [21] A. M. Mostafa et al., "AI-Based Prediction of Traffic Crash Severity," *Scientific Reports*, vol. 15, 2025, doi: 10.1038/s41598-025-10970-7.
- [22] Y. Li et al., "Deep Learning for Urban Traffic Prediction," *IEEE Access*, vol. 11, 2023, doi: 10.1109/ACCESS.2023.3278123.
- [23] X. Chen et al., "Traffic Congestion Prediction Using Hybrid Learning Models," *Transportation Research Part C*, vol. 145, 2022, doi: 10.1016/j.trc.2022.103645.
- [24] S. Ahmed et al., "Explainable AI in Smart Transportation Systems," *Expert Systems with Applications*, vol. 245, 2024, doi: 10.1016/j.eswa.2024.121145.
- [25] J. Kim et al., "IoT-Based Intelligent Traffic Monitoring Systems," *Sensors*, vol. 23, no. 6, 2023, doi: 10.3390/s23063211.
- [26] R. Patel et al., "Cybersecurity Challenges in Intelligent Transportation Systems," *IEEE Internet of Things Journal*, vol. 9, no. 18, 2022, doi: 10.1109/IIOT.2022.3158764.
- [27] H. Zhao et al., "Robust Traffic Flow Forecasting Under Noisy Conditions," *Applied Soft Computing*, vol. 145, 2023, doi: 10.1016/j.asoc.2023.110224.
- [28] P. Kumar et al., "Explainable Ensemble Learning for Smart Mobility," *Knowledge-Based Systems*, vol. 289, 2024, doi: 10.1016/j.knosys.2024.111245.
- [29] M. Hassan et al., "Machine Learning for Traffic Incident Detection," *Accident Analysis & Prevention*, vol. 184, 2023, doi: 10.1016/j.aap.2023.107012.
- [30] J. Rivera et al., "Data-Driven Intelligent Transportation Infrastructure," *Sustainable Cities and Society*, vol. 86, 2022, doi: 10.1016/j.scs.2022.104012.
- [31] S. Park et al., "SHAP-Based Explainability for Traffic Safety Analysis," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 6, 2024, doi: 10.1109/TITS.2024.3378912.

- [32] T. Nguyen et al., "Cyberattack Detection in Smart Transportation Networks," *Computers & Security*, vol. 132, 2023, doi: 10.1016/j.cose.2023.103210.
- [33] V. Singh et al., "Intelligent Transportation and AI-Based Decision Systems," *Transportation Engineering*, vol. 14, 2024, doi: 10.1016/j.treng.2024.100201.
- [34] M. Rahman et al., "Explainable Random Forest Models for Transportation Analytics," *Applied Intelligence*, vol. 54, 2023, doi: 10.1007/s10489-023-04871-5.
- [35] D. Ferreira et al., "AI and IoT Integration in Smart Cities," *Future Generation Computer Systems*, vol. 137, 2022, doi: 10.1016/j.future.2022.08.015.
- [36] K. Ali et al., "Adversarial Robustness in Intelligent Transportation Systems," *Information Sciences*, vol. 668, 2024, doi: 10.1016/j.ins.2024.120443.
- [37] N. Verma et al., "Explainable Deep Learning for Traffic Networks," *Neural Computing and Applications*, vol. 37, 2025, doi: 10.1007/s00521-025-10244-3.
- [38] L. Ortega et al., "Smart Transportation Data Analytics Using Machine Learning," *IEEE Access*, vol. 11, 2023, doi: 10.1109/ACCESS.2023.3299881.
- [39] H. Choi et al., "Trust-Aware AI Models for IoT Systems," *Expert Systems*, vol. 42, no. 1, 2024, doi: 10.1111/exsy.13788.
- [40] F. Ibrahim et al., "Cyber-Resilient Explainable AI Frameworks for Smart Infrastructure," *Computers in Industry*, vol. 161, 2025, doi: 10.1016/j.compind.2025.104312.
- [41] Benshams, R.M., n.d. *Cultivating organizational culture for AI integration: A framework for Smart Cities and Regional Development*. Smart Cities and Regional Development Journal.
- [42] Planojevikj, M. and Jovanovska, M.B., n.d. *Data protection challenges in the era of AI: Case study of Macedonia*.
- [43] Zisko, F. and Mema, B., n.d. *Digital twins and MIS integration for urban resilience: A strategic approach to smart city evolution*.