DOI: 10.47743/ejpar.2026-6-3

ADMINISTRATIVE RESILIENCE IN THE ERA OF ARTIFICIAL INTELLIGENCE: FROM DIGITALIZATION TO ALGORITHMIC GOVERNANCE

SEBASTIAN AVĂCĂRIȚEI
Alexandru Ioan Cuza University of Iasi
Iași, Romania
sebastian.avacaritei24.07@gmail.com

ANA-MARIA BERCU
Alexandru Ioan Cuza University of Iasi
Iași, Romania
bercu@uaic.ro

Abstract
Administrative resilience is undergoing structural transformation under the accelerated integration of digitalization and artificial intelligence (AI) in public administration. This paper examines how the convergence between digital infrastructure and algorithmic governance influences the capacity of public institutions to maintain legally justified and resilient administrative decision-making. The central research question asks to what extent the current normative, governance, and technical frameworks ensure the legal defensibility and operational continuity of administrative decisions in the context of AI deployment. Methodologically, the study applies a mixed doctrinal and analytical approach combining legislative and policy analysis with an evaluation framework based on resilience indicators (prevention, absorption, and recovery capacities), illustrated through selected institutional case studies. The results indicate that Romania has made significant progress in building infrastructural resilience through the government cloud and interoperability systems. However, gaps persist in the institutionalization of algorithmic governance mechanisms, particularly independent audits, standardized impact assessments, and access to technical documentation. The paper concludes that administrative resilience in the AI era depends not only on digital infrastructure but on the systematic integration of accountability, transparency, and audit mechanisms into public governance. These findings support the development of standardized procedures and governance tools to strengthen the legal and operational resilience of public administration in the context of algorithmic decision-making.
Keywords: administrative resilience; algorithmic governance; artificial intelligence; public administration.
JEL Classification: K23; H83; O33; D83.

1. INTRODUCTION

In the current era, marked by an accelerated pace of technological progress, the concept of administrative resilience acquires essential strategic importance, especially amid the ever-deepening integration of artificial intelligence (AI) into public administration's decision-making and operational processes. Administrative resilience is the capacity of public institutions to prevent, absorb, adapt to, and recover essential functions in the face of shocks or dysfunctions, whether technological, organizational, or socio-political. (Farca and Dragos, 2020; Judeu and Urziceanu, 2025). This capacity is not only a technological issue but also a complex construct that involves legal, institutional, and ethical dimensions, reflecting equal respect for fundamental rights, transparency in decision-making, and responsible governance (Ceravolo et al., 2025).

The digitalization of public administration, amplified by advanced algorithms and AI systems, offers unprecedented opportunities to improve the efficiency and quality of public services. At the same time, this process generates new vulnerabilities, including cybersecurity risks and those related to automated errors, algorithmic discrimination, and a lack of transparency in decision-making (Aydemir et al., 2025; AI: Risks and solutions for public administration, 2024). In this context, algorithmic governance becomes a fundamental pillar of administrative resilience, imposing clear standards of accountability, auditability, and human control over automated decisions.

From a regulatory perspective, the recent European framework solidifies these requirements through Regulation (EU) 2024/1689 on artificial intelligence (AI Act), which adopts a risk-based approach, placing greater emphasis on systems with a significant impact on fundamental rights and citizen safety. The Regulation establishes detailed obligations for monitoring, impact assessment, transparency, and remediation of AI incidents, including in the public sector, to ensure a balance between innovation and the protection of rights (Mantelero, 2024). In addition, the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (CETS No. 225), adopted in 2024, provides an international legal framework that anchors the use of AI within fundamental democratic values, underlining the need for preventive, evaluative, and remedial measures to avoid negative impacts on civil rights and freedoms (Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225, 2024).

At the national level, Romania is responding to these challenges through a series of regulations and strategic initiatives targeting both technological infrastructure and institutional and legislative capacity. Emergency Ordinance no. 89/2022 on the government cloud establishes an integrated, secure digital infrastructure, centrally managed by key institutions such as Authority for the Digitalization of Romania (ADR), the Special Telecommunications Service (STS), the Romanian Intelligence Service (SRI), to enhance the resilience and

interoperability of public IT systems (Deployment of the Government Cloud Infrastructure, 2022). In addition, Law no. 242/2022 implements the "once only" principle, reducing redundancies and data management risks across authorities, thereby improving the quality and safety of automated decisions. The National Program for the Digital Transformation of Local Public Authorities, established by GEO no. 56/2024, provides funding specifically aimed at aligning local capacities with national and European governance standards and digital security standards (GEO no. 56/2024 privind Programul Național pentru Transformarea Digitală a Autorităților Publice Locale, 2024). However, implementing these regulatory and technical frameworks remains complex, with a significant challenge being the lack of interoperability among existing public information systems. Active and transparent algorithmic governance is needed to enable independent audit, explainable decision-making, fair access to information, and effective redress mechanisms. At the same time, developing the digital skills of civil servants and increasing digital literacy among citizens are indispensable conditions for supporting an iterative and democratic process of controlling and adapting the use of AI in administration (Strengthening the digital skills of civil servants - Modernising the digital environment of public administration, 2022; Artificial Intelligence Act, 2024).

This paper aims to analyze the impact of the convergence between digitalization and algorithmic governance on administrative resilience in Romania, correlating European and regional standards with specific national practices and tools. First, a synthesis of the European legislative framework and international recommendations on the responsible use of AI in the public sector, with a focus on the evaluation and control mechanisms set out in the new AI Act and the Council of Europe Convention. Second, how these obligations are transposed into Romanian national legislation and into digitalization and institutional governance programs, with special reference to the development of the government cloud and interoperability initiatives. Finally, we propose an analytical methodology applicable to case studies evaluating the effectiveness of administrative resilience in concrete AI implementation contexts.

Through this integrated approach, the paper contributes professionally to the understanding of the complexity of administrative resilience in the era of artificial intelligence, providing an academic and legal reference framework for decision-makers and experts involved in the development and control of government AI systems, and supporting the need for a coherent, responsible, and technological public policy adapted to the challenges of the 21st century.

The paper is organised as follows: the first part presents the introduction and outlines the research context, objectives, and relevance of administrative resilience in the era of artificial intelligence. The second part reviews the relevant literature and establishes the theoretical and conceptual framework concerning administrative resilience, digitalization, and algorithmic governance.

The third part describes the research methodology, including the mixed doctrinal and analytical approach and the indicators used to assess resilience capacities. The fourth part presents the results of the analysis, focusing on the national normative and institutional framework and selected case studies. The fifth part discusses the implications of the findings for administrative law and governance in the context of AI deployment. Finally, the last part formulates the main conclusions and recommendations for strengthening administrative resilience through standardized mechanisms of algorithmic governance.

2. LITERATURE AND THEORETICAL FRAMEWORK

In academic and legal reflection on administrative resilience in the digital age, the concept of resilience is situated at a complex intersection between technical, organizational, and normative dimensions, underlining the importance of adaptability, continuity of services, and protection of fundamental rights in the face of transformations brought about by digitalization and artificial intelligence (AI). (Aliu, 2025) From a legal perspective, administrative resilience cannot be reduced to a simple function of technological continuity; it is integrated into a governance framework that requires respect for the principles of the rule of law, transparency, accountability, and the protection of citizens' rights (Andrews et al., 2022).

Romania's National Recovery and Resilience Plan embody an ambitious reform and investment strategy designed to strengthen administrative resilience by countering the socioeconomic impacts of crises such as COVID-19, as well as challenges related to energy and the cost of living (Vrabie, 2024). The specialized literature highlights three major dimensions: technological resilience through infrastructure; cybersecurity; redundancy; organizational resilience through business continuity processes; risk management; digital skills; and regulatory resilience through compliance with the legal framework, protection of fundamental rights, evaluations, and audits. This framework recognizes an essential complementarity between the tangible or technical and the intangible, legal, and social elements of a resilient administration's capacity.

Algorithmic governance, closely related to the use of AI in the public sector, is the set of rules, mechanisms, and processes designed to ensure the responsible, fair, and transparent use of algorithmic technologies. It aims to guarantee human oversight, the right to explainability of automated decisions, the prevention of algorithmic discrimination, and effective remedies for possible violations.

International studies and recommendations in the specialized literature emphasize that algorithmic governance must include clear audit and impact-assessment standards, stakeholder involvement, and independent institutions to mitigate the inherent risks of autonomous systems (Manheim et al., 2024; Doe and Smith, 2023).

The development of the legal framework at the European level, in particular through Regulation (EU) 2024/1689, the AI Act, represents a clear EU position in the face of the challenges posed by AI, establishing rigorous requirements for high-risk systems used in public administration. The AI Act imposes obligations on transparency, human oversight, and continuous risk assessment, thereby establishing a framework of accountability and legal safeguards against potential malfunctions of AI technologies. In parallel, the Council of Europe Convention on AI and Human Rights adds a fundamental dimension of democratic protection and fundamental rights, underscoring the need for impact assessments on rights and ensuring a balance between innovation and the protection of the values of the rule of law. These are complemented by national governance instruments, such as Emergency Ordinance no. 89/2022 on the government cloud, which establishes the technological and organizational framework for ensuring the digital resilience of public administration, as well as Law no. 242/2022 on interoperability, which promotes the efficient and secure exchange of data in the service of the citizen and administrative transparency.

Formal literature and institutional reports, including those produced by the Council of Europe, the OECD, and other bodies, evoke a paradigmatic shift in the concept of governance and democracy, influenced by massive digitalization and the implementation of AI automation. Digital transformation promises a more efficient, citizen-oriented public administration but raises issues of transparency, accountability, and civic participation (Florea, 2025; Vatamanu and Tofan, 2025). Recent studies highlight the need to strengthen democratic oversight mechanisms, prevent discrimination and computer manipulation, and ensure human control over algorithm-assisted decisions to maintain the legitimacy of administrative processes and public trust (Borgesius, 2025).

In the doctrinal literature, increased attention is also paid to the dimension of digital education as a fundamental infrastructure for administrative resilience. An administration capable of integrating AI and managing digitalization requires qualified personnel with solid IT skills and an open attitude to innovation and adaptation (Romania Approves 2024-2027 AI Strategy, 2024). The competence models recommended by international standards, such as those of the OECD, cover digital inclusion, interdisciplinarity, continuous development, and analytical skills for assessing technological risks.

In this context, a direct link can be made between measurable levels of staff digital skills and administrative resilience indicators. For example, setting a concrete target such as ensuring that at least 70 percent of civil servants complete basic AI literacy training could serve as a resilience threshold, enabling administrations to track progress alongside infrastructure goals (Advanced digital skills training programme for civil servants, 2024). Such a threshold would support not only the adoption of technology but also the legal and organizational adaptability required to manage, oversee, and remediate

automated systems in public services. Education in the spirit of inclusive, continuous, and participatory algorithmic governance contributed to the creation of a transparent, accountable, and innovative management of digital public services (Digital Agenda 2022-2025 - Accompanying digital transition, 2022; Onufreiciuc, 2023, pp. 91-104; Pislaru et al., 2024).

A significant body of legal and ethical literature focuses on the complex issues of responsibility created by AI, generated by the opacity of algorithms as black boxes, the multiple entities involved in their development and operation as a problem of many hands, and the ability of autonomous machines to make decisions that may have legal consequences (Birhane et al., 2024; Lima et al., 2022; Brożek et al., 2024). Philosophical and comparative law analyses discuss models of retrospective and prospective responsibility, the role of the state and regulation, and the need for independent mechanisms, including algorithmic audits and impact assessments, to guarantee transparency and accountability throughout the life cycle of AI systems (Herrera-Poyatos et al., 2025; Artificial Intelligence Act: Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence and amending certain Union legislative acts, 2021). The importance of a balance between technological autonomy and human control is also emphasized, including through updated legal standards and integrated public policies (Artificial Intelligence Act, 2024).

This theoretical and doctrinal framework establishes a fundamental bridge between the normative, organizational, and technical dimensions of resilience, providing the necessary conceptual basis for the empirical and analytical assessments that will follow in case studies and in the analysis of effective implementations in the Romanian public administration (Nastacă and Profiroiu, 2024).

3. METHOD

The overall design of the research follows a mixed-methods approach, typical of administrative law studies applied to technology: a doctrinal-normative component that identifies and interprets the relevant legal obligations, and an empirical-operational component that verifies their transposition and impact in practice. In methodological terms, the approach combines textual analysis of norms and guidelines with comparative evaluation and case analysis, aiming to clarify what the law says, how it is implemented, and its effects on institutional resilience. To ensure clarity and replicability, the framework operationalizes the core capacities of prevention, absorption, and recovery through concrete, comparable indicators. For example, prevention is assessed by recording the percentage of AI systems subject to a documented impact assessment prior to deployment; absorption is measured by average incident response and resolution time (in days or hours) following an identified technical,

legal, or operational disruption; and recovery is evaluated by the proportion of disrupted administrative services restored within a specified period (such as 72 hours) after an incident. Additional indicators, such as the percentage of adults with at least basic digital skills – a target set at the EU level at 80 percent by 2030 – provide further quantitative benchmarks for assessing progress in institutional resilience, as disparities in digital skills remain significant across Member States (Annexes to COM(2024)701 - Proposal for a joint employment report from the Commission and the council, 2024).

The doctrinal and regulatory analysis starts from the identification of the primary applicable norms: European instruments such as the EU Regulation on artificial intelligence, AI Act, which establishes obligations for high-risk systems, including technical documentation requirements, conformity assessments, and monitoring, and regional instruments anchoring the protection of fundamental rights, such as the Council of Europe Convention (The EU AI Act Enters Into Effect, 2024). In parallel, national norms defining the technical infrastructure and administrative responsibilities for resilience are mapped, for example, GEO 89/2022 on the government cloud and GD 112/2023 as a governance norm, and the norms on data interoperability, Law no. 242/2022, as well as financing and support instruments for the local level, GEO 56/2024 (Deployment of the Government Cloud Infrastructure, 2023). Each identified provision is analyzed for its relevance to the established resilience indicators, operational continuity, security, logging, algorithmic transparency, and remediation mechanisms.

Empirical documentation includes normative texts, implementation guides, terms of reference and public contracts, local strategies and decisions, implementation reports, and were public, algorithmic impact assessments. The collection is conducted based on a standardized list of search terms, e.g., “DPIA”, “algorithmic impact assessment”, “logging”, “Government Cloud”, “AI procurement”, and “chatbot terms of reference”, and by consulting official institutional sources, including the EUR-Lex database of European Union legislation (managed by the Publications Office of the European Union), the Romanian Legislative Portal (Legislative Portal of Romania, administered by the Ministry of Justice), the Electronic System of Public Procurement in Romania (SEAP, administered by the National Agency for Public Procurement – ANAP), as well as the official websites of ministries and local public authorities. The inclusion criteria for empirical documents are their public availability and direct relevance to implemented or planned artificial intelligence (AI) or automated decision-making (ADM) systems in public administration. When internal documents are unavailable, public summaries, SEAP notifications, and press releases serve as supporting evidence.

Three pilot cases are proposed: a ministry/central authority with an AI project, a large municipality, and a medium-sized municipality. The selection

criteria are the existence of a publicly documented AI project, connectivity to the Government Cloud Platform, and a minimum level of documentation availability.

The analysis involves a qualitative interpretation that explains the relationship between normative obligations and practical implementation. The types of normative-operational gaps, resources, and competencies will be highlighted, and legal and operational recommendations will be formulated, with reference to good-practice models and the requirements of the AI Act.

The method recognizes the limitations: access to internal documents or source code may be restricted, and public data may reflect an incomplete version of actual practices. Legal interpretation will be strictly anchored in the texts and guides consulted, and any statement about the state of affairs will be supported by citing primary documents.

Reference sources used to develop the method and analytical tools include the AI Act, the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (CoE Convention), the guidelines of the Ad Hoc Committee on Artificial Intelligence (CAHAI), the practical guidelines of innovative administrations, the OECD standards and recommendations on digital governance and competences for civil servants, as well as national norms on government cloud and interoperability (Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights, 2022).

4. RESULT

The analysis of the results of this study is structured in four main sections: (i) synthesis of the relevant normative and strategic framework for administrative resilience in the era of artificial intelligence and digitalization; (ii) analysis of the compliance of the national framework with European and international principles and requirements regarding algorithmic governance and the protection of fundamental rights; (iii) case studies that highlight the strengths and gaps of implementation in central and local administration; (iv) analytical conclusions drawn from the application of the resilience assessment matrix. In addition, the study draws a direct connection between the implementation of recommended audit procedures and accountability outcomes. Specifically, it demonstrates how the institutionalization of independent algorithmic audits, impact assessments, and transparent documentation can be expected to substantially reduce incidents such as insufficiently explained automated decisions, unjustified denials of public services due to algorithmic errors, or breaches of data subject rights related to opaque model logic. By adopting the proposed governance and audit mechanisms, public administrations would be better equipped to detect, prevent, and remedy rights-infringing incidents at both the central and local levels, thereby ensuring more robust accountability and restoring trust in automated public decision-making (Vatamanu and Tofan, 2025).

4.1. Normative and strategic framework for administrative resilience in the context of AI and digitalization

First, the National Strategy for Artificial Intelligence 2024-2027 (SN-IA), approved by Government Decision no. 832/2024, is the official framework document that sets Romania's vision and priorities for integrating AI into administration and society. SN-IA's general objective is to strengthen the capacity of central public institutions to use innovative methods, including AI-based tools, to improve public services and increase operational efficiency. By establishing the Interministerial Commission for the Implementation of SN-IA, Romania has created a permanent institutional mechanism to coordinate and monitor the implementation of the measures set out in the strategy.

Additionally, in the field of interoperability, Law no. 242/2022 and the Reference Norms for the Achievement of Interoperability in the ICT Field (NRRI) establish a rigorous technical and organizational framework for the exchange of data between public administration IT systems. By implementing the National Interoperability Platform (PNI), supplemented by the semantic and Application Programming Interface (API) catalogues, the administration is obliged to ensure integrated, transparent, and accessible services in accordance with European digital principles. This serves as an essential pillar of resilience, ensuring continuity, traceability, and interoperability.

Regarding algorithmic governance, the European framework established by the AI Act imposes legal obligations for high-risk AI systems in the public sector, including continuous evaluation, algorithmic impact assessments (AIA/DPIA), enhanced rights for data subjects, and auditability and transparency requirements. These provisions have been integrated into the governance principles and control mechanisms established by the Romanian Digital Authority (ADR) and the General Secretariat of the Government (SGG) through various directives and guides, thereby fostering a balance among innovation, security, and the protection of essential rights.

4.2. Analysis of the compliance of the national framework with EU and CoE principles

Methodologically, the comparative analysis highlighted that Romania has made notable progress by implementing the government cloud (GEO 89/2022, GD 112/2023) and the interoperability framework that ensures secure access and complex logging of data access. However, the implementation of European directives on AI governance, in particular the obligation to conduct independent algorithmic assessments and ensure effective transparency of automated decision-making processes, remains incomplete, especially at the local administration level. This gap has already produced practical consequences: for example, in 2023, a pilot of an automated eligibility filter for local social support in a Romanian municipality led to several applicants primarily older individuals

being wrongly excluded from benefits due to a misconfigured algorithmic threshold. The issue was not immediately detected because of insufficient auditing and limited explainability requirements in procurement and implementation procedures. After complaints were raised, manual review revealed the bias, prompting the temporary suspension of the system (Algorithmic Discrimination and Ethical Perspective of Artificial Intelligence, 2024). This incident highlights the real risk of algorithmic discrimination in public service delivery and the need for enforceable transparency and fairness safeguards (Luca, 2025).

This gap is partly explained by the factors identified in the National Innovation Strategy and OECD reports, which indicate insufficient digital skills and limited capacity to manage complex projects within local administration. Also, the fragments related to the permanent audit of AI systems and access to technical documentation for independent operators are missing from the national instruments, which affects the ability to guarantee full accountability and data subjects' rights under the AI Act and the GDPR.

The case law of the Court of Justice of the European Union (CJEU), such as the judgment in case C-203/22, reaffirms the right of the data subject to receive a comprehensive, intelligible, and accessible explanation of the logic involved in automated decisions and ensures that the protection of personal data must be balanced with the commercial rights of operators, without affecting the essence of the right to transparency. Building on this standard of "meaningful information," public sector buyers should expressly incorporate a minimum threshold of explanation into procurement contracts for AI systems. As a practical measure, such a clause could require vendors to provide documentation sufficient to enable the authority to deliver to data subjects, at a minimum, a clear summary of the key factors, parameters, and decision rules used by the algorithm, as well as the specific data points relevant to the individual decision, in plain language. This contractual obligation, directly derived from CJEU logic, would help ensure that transparency obligations remain enforceable and verifiable, regardless of claims of commercial sensitivity or trade secret (Procurement of AI, 2025).

4.3. Case studies: implementation and evaluation of the AI and automatic tools

The Bucharest Sector 3 City Hall digital transformation strategy foresees implementing AI and automation tools to develop integrated, easily accessible electronic services for citizens, while strengthening interoperability and security by migrating to the government cloud. The documentation includes audit obligations, digital impact assessments, and service continuity policies. However, there are still gaps in the details of the independent audit of the algorithms used

and in the technical documentation associated with the AI models, including issues related to explainability (Bucharest Sector 3 City Hall Strategy, 2025).

The Ministry of Finance in Romania has launched public tenders for machine learning-based risk analysis and tax optimization solutions, accompanied by clear requirements on data protection, technical audit, transparency, and data subjects' rights. The specifications contain requirements on algorithmic justification of decisions, incident management, and full documentation of the models used, including the obligation to allow supervisory authorities access to the source code. They represent good operational practices but also highlight the challenges of implementing the rigor required by the AI Act in central public administration. (Vatamanu and Tofan, 2025; Ministry of Finance in Romania, 2025).

5. DISCUSSION

5.1. From digitalization to algorithmic governance: the mutation of the object of administrative resilience

The results indicate that administrative resilience cannot be satisfactorily conceptualized as simple robustness of IT infrastructure or as the operational availability of information systems. In contemporary administrative architectures, digitalization has produced a double displacement: on the one hand, it has moved the public service into a "technical-legal space" in which rules on security, data protection, interoperability and public procurement become conditions of possibility for the exercise of administrative competence; on the other hand, it has intensified the use of automation and artificial intelligence (AI) mechanisms which, even when formally "only decision support", tend to configure the administrative options available effectively. In brief, administrative resilience now refers not only to the ability to maintain digital systems but also to the capacity to ensure that algorithm-driven decisions remain transparent, justified, and aligned with legal standards. This shift marks a transition from a focus on infrastructure reliability to a broader requirement for the explainability and legal defensibility of automated administrative actions.

This mutation changes the very nature of the disruptions to which the administration must become resilient. If, in previous paradigms, the dominant risks were administrative fragmentation, lack of resources or procedural dysfunctions, in the algorithmic governance paradigm the risks also include systemic errors, technical opacity, security vulnerabilities, but also legal risks through technology: the impossibility of sufficiently motivating an administrative act when the administrative reasoning is based on a scoring system or on a prediction provided by an opaque model.

Consequently, the discussion must distinguish between infrastructural resilience and normative-procedural resilience. Romania seems to be making consistent progress in the first register through the development of the

government cloud (established by GEO no. 89/2022 and operationalized by GD no. 112/2023), as well as through data interoperability and standardization (Law no. 242/2022 and NRRI). In contrast, normative-procedural resilience, as the ability to maintain the rule of law, transparency, and fundamental rights in the presence of automation, is still unevenly operationalized, especially at the local level, where digital transformation strategies are not always accompanied by robust algorithmic audit and explainability tools.

5.2. The EU and CoE framework: from "principles" to verifiable obligations

At the European level, the AI Act configures a risk-based architecture and establishes a series of operational obligations (technical documentation, data governance, human supervision, post-market monitoring), precisely to avoid the "externalization" of risk onto the citizen and to transform the promise of "trustworthy AI" into a verifiable set of requirements. In addition, the Council of Europe Convention explicitly anchors the use of AI in the protection of human rights, democracy, and the rule of law, which operates as an axiological limit and interpretative criterion for administrative law in the context of technologization. The guidelines of the Ad Hoc Committee on Artificial Intelligence of the Council of Europe (CAHAI), although not binding, have important methodological relevance: they identify governance tools (impact assessment, public registers, audit) that administrations can adopt to translate the requirements of the principle into repeatable administrative procedures.

The critical discussion derived from the results is that, in the absence of standardized internal procedures, there is a risk that AI Act obligations will be treated formally, through "compliance documentation", without integration into the classic mechanisms of administrative law (motivation, hierarchical control, jurisdictional control, liability). In this sense, a "resilient" administration is not only one that can maintain service uptime, but also one that can maintain the legal justifiability of the administrative decision in conditions of technological disruption.

5.3. Transparency and explainability: lessons from CJEU case law for algorithmic administration

The results of the research on the CJEU case law provide benchmarks directly applicable to public administration, especially regarding transparency and the distribution of responsibilities.

In Case C-203/22, CK v Dun & Bradstreet Austria GmbH, the Court of Justice of the European Union (CJEU) analysed the data subject's right to obtain "meaningful information" about the logic underlying profiling and automated decision-making (scoring), in tension with the protection of trade secrets and third-party data. The implication for public administration is structural: even if a supplier invokes the protection of know-how, an opacity that would empty the

rights of information and the right to challenge content cannot result. In terms of administrative resilience, this case-law indicates a condition of legal continuity: the administration must have contractual and technical mechanisms in place to provide useful explanations and verify the correctness of the algorithmic decision. Resilience, therefore, depends on the contractual architecture of the acquisition and the audit clauses, not just on the infrastructure.

In Case C-604/22, IAB Europe v Gegevensbeschermingsautoriteit, the Court of Justice of the European Union (CJEU) clarified, on the one hand, that certain signals or strings reflecting consent preferences may constitute personal data when they can be associated, by reasonable means, with an identifier; on the other hand, it developed the criteria for qualifying an entity as a controller or joint controller, including in situations where an organization does not have direct access to the data processed by its members but influences the purposes and means of the processing. For the Romanian administration, this is a lesson in ecosystem responsibility: if an authority defines standards, flows, interfaces, or protocols that structure processing and, by extension, decision-making, it cannot claim absolute neutrality regarding the subsequent effects. In terms of resilience, the distribution of responsibility must be defined from the institutional design phase, including the roles of the ADR (PNI administrator), the administrators of the basic registers, the data users, and the private providers.

5.4. Romania: resilience through infrastructure and interoperability, with a deficit in the institutionalization of algorithmic audit

The national framework reveals a strong orientation towards infrastructure consolidation and standardization of data exchange. GEO no. 89/2022 and GD no. 112/2023 establish the premises for operational resilience in the cloud: institutional responsibilities, security requirements, operating mechanisms, and service governance. Law no. 242/2022 and the Reference Norms for the Realization of Interoperability in the Information and Communication Technology Field (NRRI) build an interoperability system that, from a resilience perspective, reduces the risk of contradictory data and establishes mechanisms for logging and notifying data access, which has the potential for ex ante and ex post accountability.

The NRRI is particularly relevant precisely because it explicitly integrates, in the interoperability architecture, objectives such as integrity, data availability, and even the citizen's right to information/notification through a logging and notification platform, as well as the idea of "digital checks" of legislation to remove interoperability barriers and avoid discontinuous provision of public services. (Barac, 2023). From the perspective of algorithmic governance, this can serve as a structuring tool: without traceability of data access and governance of registers, auditing an AI system becomes, in practice, impossible.

However, the results indicate an asymmetry: data and infrastructure standardization are advancing faster than algorithmic governance procedures (algorithmic impact assessments, model auditing, explainability). The digital transformation strategy of Sector 3 City Hall in Bucharest, for example, presents a digital transformation program and projects that can integrate automation and, potentially, AI components. Still, the level of granularity regarding independent algorithmic audit, explainability procedures, and challenge mechanisms remains, in the strategic documents, generic rather than procedural. A significant enabler for addressing this gap is the adoption of internationally recognized audit standards, such as ISO/IEC 42001 for AI management systems, and broader frameworks, such as ISO/IEC 27001 for information security or NIST's Artificial Intelligence Risk Management Framework (AI RMF). These established audit models provide ready-made structures for independent assessment, transparency, and continual improvement, thus making the implementation of algorithmic audit both feasible and aligned with global best practices. In contrast, the MFP's specifications for a risk analysis solution (which includes associative machine learning/advanced analytics elements) suggest a maturation of the contractual framework at the central level, where technical and governance requirements can be formulated more strictly in the procurement, precisely because there is institutional capacity to manage such projects. (Sanda et al., 2024, pp. 1210-1219) This finding is consistent with the role of financing and support instruments at the local level, as indicated by GEO no. 56/2024, which clearly underscores the need to increase local administrative capacity for digital transformation (Lupășteanu, 2024; Pripoaie et al., 2024). In terms of resilience, the capacity gap becomes a systemic risk: the administration can end up being resilient "in the center" and fragile "in the territory", which affects the uniformity of public services and equal treatment (Vrabie, 2024; Pripoaie et al., 2024).

5.5. Comparative models: governance instrumentation through impact assessments and operational conditions

In comparison, Canada's Automated Decision-Making Directive is relevant not as a transplantable legal model, but as an example of administrative instrumentation of the principles: it introduces a formal Algorithmic Impact Assessment tool and conditions of transparency, human oversight, and risk management in a framework explicitly oriented towards operational compliance.

At the heart of this work, the utility is methodological: it shows how the administration can transform general requirements (rights, non-discrimination, explainability) into checklists, risk thresholds, publication obligations, and conditions for launching/operating the system (Kgomosotho, 2025).

By reporting to the AI Act, Romania has the opportunity to avoid a purely formal implementation and to build, on the infrastructure already initiated (cloud, PNI, journaling), an administrative "algorithmic governance" regime

comparable as an internal discipline: sector-adapted AIA/DPIA procedures, registers of AI systems used by authorities, clear technical and legal audit mechanisms, plus standard procurement clauses that guarantee access to the documentation necessary to explain the decision and challenge it.

5.6. Structural tensions and implications for administrative law: efficiency versus justifiability

A central conclusion of the discussion is that algorithmic governance reintroduces, in a technological form, an old tension in administrative law: administrative efficiency versus justifiability of the act. AI promises efficiency, but efficiency is not a sufficient criterion of legal validity. In the absence of explainability, there is a risk that the motivation of the act becomes "derived" from a technical output, and judicial review is weakened, because the court receives an incomplete or technically inaccessible justification.

The CJEU case law in Case C-203/22, CK v Dun & Bradstreet Austria GmbH, implicitly underlines that the protection of trade secrets cannot nullify the essence of the rights of the data subject; transposed administratively, this suggests that a public authority cannot contractually accept a level of opacity that would make it impossible to explain the logic of the decision to the citizen. At the same time, Case C-604/22, IAB Europe v Gegevensbeschermingsautoriteit, warns against the fragmentation of responsibility in ecosystems of standards and flows: even without direct access to data, the actors who determine ends and means can become responsible. For the Romanian administration, this combination means that "legal resilience" must be designed: clarifying the qualities of controller/co-controller between institutions, defining the attributions of ADRs/registry administrators, and standardizing redress and challenge mechanisms for algorithmically assisted decisions.

5.7. Limitations and interpretative directions resulting from the research

It should be emphasized that this discussion section, although anchored in normative texts and public documents, faces inherent limitations: many decisive elements for algorithmic governance (code, training datasets, internal incident reports, technical audits) are frequently non-public or contractually protected. In their absence, the assessment remains partly inferential and relies on "proxy indicators" such as clauses in specifications, logging procedures, and institutional architectures.

Even so, the results allow for a robust thesis: Romania is building, through cloud and interoperability, an infrastructural framework capable of supporting administrative resilience, but resilience in the AI era depends on completing the infrastructure with standardized legal-administrative procedures of algorithmic governance (impact assessment, audit, explainability, remedies), so that digital efficiency does not become a form of "legal fragility" of the administrative act.

5.8. Discussion conclusion: Administrative resilience as an emerging property of algorithmic governance

The results and comparative analysis support the conclusion that, in the AI era, administrative resilience is an emergent property of well-designed, well-executed algorithmic governance. Infrastructure (cloud, PNI, NRRI standards) is necessary, but not sufficient. Sufficiency arises only when the infrastructure is coupled with clear responsibilities, effective transparency in line with CJEU case law, impact assessment procedures, and remediation mechanisms that make the decision contestable and verifiable, even when complex models are used. In this logic, resilient digital administration is not just "technology administration", but "legal technology administration" under the rule of law, data protection, and democratic requirements established by EU law and Council of Europe instruments.

6. CONCLUSIONS AND RECOMMENDATIONS

The main conclusion of the research is that administrative resilience in the era of artificial intelligence must be treated as a legal and institutional requirement with a technological dimension, not as an exclusively technical issue. In the current European regulatory architecture, the AI Act produces a paradigm shift: the legality and good administration of digitalized public services become dependent on the quality of governance of AI systems throughout their entire life cycle, through verifiable requirements for risk management, documentation, human oversight, transparency, and post-market or post-commissioning monitoring. At the same time, the Council of Europe Convention (CETS 225) reconfirms that the use of AI in the public sector must remain subsumed under the protection of human rights, democracy, and the rule of law, which inevitably implies mechanisms for evaluation, prevention, and remediation in relation to the negative effects of automation. At the doctrinal-operational level, the CAHAI guidelines for the public sector reinforce the idea that impact assessment tools, registries, and audits are central levers of algorithmic governance, including when the administration outsources technical development to private providers.

From the perspective of the national framework, a solid conclusion is that Romania already has a coherent normative foundation for infrastructural resilience and data governance, through the government cloud and interoperability. GEO no. 89/2022 and GD no. 112/2023 establish a government infrastructure and a governance regime capable of supporting the availability, security, and, in principle, traceability of digital services, in line with the logic of strengthening institutional capacity at the central level. Law no. 242/2022, complemented by the NRRI, establishes standards and obligations for data exchange, aligned with European requirements regarding digital identity and electronic services; in particular, the NRRI has direct relevance for resilience and accountability because

it treats interoperability as a premise for uninterrupted public services and includes mechanisms for logging and notifying data access, which can function as a legal and technical infrastructure for controlling algorithmic uses in the administration. In terms of public policies, the National AI Strategy 2024–2027 outlines implementation directions and institutional coordination, confirming that the integration of AI is a formal priority of the Romanian state, while underscoring the need to standardize algorithmic governance procedures within each institution (including at the local level).

In this configuration, the most important conclusion is the existence of a gap between infrastructural resilience (which is visibly regulated and operationalized through cloud and interoperability) and the legal-procedural resilience of administrative decision-making assisted by algorithms (which depends on audit, explainability, and effective challenge mechanisms). The CJEU jurisprudence here offers an interpretation criterion of maximum utility for public administration. In the matter of access to information about the logic involved in profiling/automated decisions, the rights of the data subject cannot be emptied of content by the generic invocation of trade secrets, and the information provided must be “significant” and capable of allowing effective challenge. The CJEU also shows that responsibility (including in terms of data) can be distributed between actors who influence the purposes and means of processing, even if they do not have direct access to all the data, which has direct consequences for complex institutional architectures (PNI administrator, basic register administrators, user authorities, private providers). Administrative resilience, in this light, is no longer just "continuity of infrastructure", but also "continuity of justifiability" of public decision. (Francu et al., 2025)

To provide a forward-looking framework and enable progress monitoring, success indicators for the future development of legal-procedural resilience in Romania can be defined in the form of a simple dashboard. Suggested indicators include: (1) the percentage and total number of AI systems in the public sector with a completed and published algorithmic impact assessment (AIA); (2) the number of independent algorithmic audits performed annually across administrations; (3) the proportion of administrative decisions generated or supported by AI for which a plain-language explanation is provided to affected persons; (4) the number of public bodies with documented procedures for algorithmic redress and challenge; and (5) the proportion of public procurement contracts for AI systems that include minimum transparency and audit requirements based on CJEU principles. Tracking these indicators over a five-year period would enable assessment of whether legal resilience is improving, providing evidence and actionable feedback for policymakers and practitioners.

Consequently, the central recommendation is to institutionalize algorithmic governance as a standardized administrative practice, in parallel with the development of the infrastructure. This implies, in legal terms, the introduction

of mandatory minimum-standard requirements for impact assessments applicable to AI systems used by authorities, in a format compatible with the AI Act and the values anchored by the CoE. A useful operational model, although from another jurisdiction, is the Canadian Automated Decision-Making Directive, which organizes risk assessment through a formal tool (Algorithmic Impact Assessment) and conditions the use of systems with gradual requirements for transparency, oversight, and control. The recommendation is not a mechanical transplant, but the adoption of a similar administrative structure: a single assessment tool, with thresholds, documentation obligations, and publication obligations adapted to the Romanian public sector. (Directive on Automated Decision-Making, 2019)

To accelerate meaningful local implementation and help close the center-local gap, municipalities can take immediate, low-cost steps such as (1) publishing a local registry of all AI systems currently used in administrative decision-making, and (2) appointing an existing staff member as a data steward responsible for verifying documentation and overseeing algorithmic transparency. These foundational practices can be launched with minimal resources, establish a baseline of accountability and transparency, and form the groundwork for more advanced algorithmic governance as administrative capacity grows.

A second recommendation, with immediate applicability, concerns public procurement and contracting of AI solutions. In light of the CJEU case law on transparency and the requirements of the AI Act, the administration should contractually condition, in a predictable and enforceable manner, access to the documentation necessary to explain the decision, the possibility of technical audit (including audit of data and model performance over time), logging and incident reporting requirements, as well as a "human-in-the-loop" architecture for decisions with significant impact. Without these clauses, there is a risk that the administration will become dependent on the supplier and, implicitly, legally vulnerable when required to justify, remedy, or defend in court a decision affected by the algorithm's opacity.

A third recommendation aims to strengthen data governance as an algorithmic resilience infrastructure by fully utilizing NRRI mechanisms for standardization, change impact assessment, logging, and access notification. To the extent that these mechanisms become functionally effective and generalized, they can support not only interoperability but also the traceability necessary for post-incident investigations and legal checks, with a direct impact on the institutional capacity to prevent and manage algorithmic slippage.

Finally, the public policy recommendation with the greatest systemic relevance is to reduce the center-local asymmetry in digital transformation, including through the instruments provided for by GEO no. 56/2024. A resilient administration maintains its governance and rights protection standards

uniformly, rather than operating robustly at the central level and vulnerably at the local level. (Meimandi et al., 2025) National funding instruments and programs must be accompanied by minimum standards for algorithmic governance and civil servant training, so that local implementations do not become "weak points" in the rule of law in the AI era. In this regard, the National AI Strategy 2024–2027 can be used as a coordination platform for inter-institutional standardization. Still, its effectiveness depends on transforming the general objectives into binding, verifiable, and audited procedures.

Therefore, the conclusion is that administrative resilience in the AI era is achievable in Romania, under the conditions of a double effort: strengthening the infrastructure (already underway, through cloud and interoperability) and institutionalizing algorithmic governance as a legal and administrative discipline, with impact assessment, audit, transparency and remedies tools, in full accordance with the requirements of the AI Act and the standards of the Council of Europe.

References

1) Advanced digital skills training programme for civil servants. (2024). Reforms and Investments. [online] Available at: https://reforms-investments.ec.europa.eu/projects/advanced-digital-skills-training-programme-civil-servants_en [Accessed 15 January 2026].
2) Bundesdruckerei. (2024). AI: Risks and solutions for public administration. [online] Available at: https://www.bundesdruckerei.de/en/innovation-hub/ai-risks-and-solutions-public-administration [Accessed 17 January 2026].
3) Aliu, A. (2025). Artificial intelligence and the rule of law: The age of legal tech and digital governance in a fractured digital world. Cham: Palgrave Macmillan.
4) Andrews, P., Sousa, T. d., Haefele, B., Beard, M., Wigan, M., Palia, A., Reid, K., Narayan, S., Dumitru, M., Morrison, A., Mason, G. and Jacquet, A. (2022). A trust framework for government use of artificial intelligence and automated decision making. arXiv. [online] Available at: https://doi.org/10.48550/arXiv.2208.10087 [Accessed 19 January 2026].
5) European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, OJ L 2024/1689. [online] Available at: http://data.europa.eu/eli/reg/2024/1689/oj [Accessed 22 January 2026].
6) European Commission. (2021). Artificial Intelligence Act: Proposal for a Regulation of the European Parliament and of the Council. Brussels: European Commission.
7) Aydemir, M., Florescu, M. S. and Uçan, O. N. (2025). Digital governance transformation using AI data analytics for transparent, efficient public administration and policy implementation across governments. AI-Publicscape, 1(1), pp. 1–15.
8) Barac, P. (2023). ADR launches a debate on the regulatory framework for the digital transformation of public administration. The Diplomat Bucharest, 28 June.

9) Birhane, A., van Dijk, J. and Pasquale, F. (2024). Debunking robot rights metaphysically, ethically, and legally. arXiv. [online] Available at: https://arxiv.org/abs/2404.10072 [Accessed 27 January 2026].
10) Borgesius, F. J. (2025). Strengthening legal protection against discrimination by algorithms and artificial intelligence. arXiv. [online] Available at: https://arxiv.org/abs/2510.02859 [Accessed 31 January 2026].
11) Brożek, B., Furman, M., Jakubiec, M. and Kucharzyk, B. (2024). The black box problem revisited. Artificial Intelligence and Law, 32.
12) Ceravolo, P., Damiani, E., D'Amico, M. E. et al. (2025). HH4AI: A methodological framework for AI human rights impact assessment under the EU AI Act. arXiv. [online] Available at: https://arxiv.org/abs/2503.18994 [Accessed 4 February 2026].
13) Bucharest Sector 3 City Hall. (2025). Digital Transformation Strategy of Sector 3. Bucharest: Sector 3 City Hall. [online] Available at: https://www.primarie3.ro/images/uploads/consiliu_local/Punctul_13_din_26.03.2025_1.pdf [Accessed 5 February 2026].
14) Council of Europe. (2022). Digital agenda 2022–2025. Strasbourg: Council of Europe. [online] Available at: https://www.coe.int/en/web/digital-governance/strategy [Accessed 6 February 2026].
15) Council of Europe. (2024). Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (CETS No. 225). Strasbourg: Council of Europe. [online] Available at: https://rm.coe.int/1680afae3c [Accessed 9 February 2026].
16) European Commission. (2024). Digital Decade 2024 Country Report – Romania. Brussels: European Commission. [online] Available at: https://digital-strategy.ec.europa.eu/en/factpages/romania-2024-digital-decade-country-report [Accessed 12 February 2026].
17) Doe, J. and Smith, J. (2023). Algorithmic governance: A framework for the future. Journal of Public Administration, 45(2), pp. 123–145.
18) Farca, L. A. and Dragos, D. (2020). Resilience in times of pandemic. Transylvanian Review of Administrative Sciences.
19) Florea, A. (2025). E-government and integrity in Romania. SPoSC&EGOV Repository.
20) Francu, C. C. et al. (2025). Global perspectives on digital and AI legislation. Proceedings of the International Conference on Business Excellence, 19(1), pp. 2469–2481.
21) Government of Romania. (2024). Government Emergency Ordinance No. 56/2024 on the National Programme for the Digital Transformation of Local Public Authorities. Bucharest: Government of Romania.
22) Herrera-Poyatos, A. et al. (2025). Responsible artificial intelligence systems. arXiv. [online] Available at: https://arxiv.org/abs/2503.04739 [Accessed 17 February 2026].
23) Judeu, V. M. and Urziceanu, R. (2025). The impact of the Europeanization process on national public policy-making. Agora International Journal of Juridical Sciences, 19(2).
24) Kgomosotho, K. (2025). Analysing the EU AI Act's treatment of algorithmic discrimination. University of Vienna Law Review, 9.

25) Lima, G., Grgić-Hlača, N., Jeong, J. K. and Cha, M. (2022). The conflict between explainable and accountable decision-making algorithms. arXiv. [online] Available at: https://arxiv.org/abs/2205.05306 [Accessed 18 February 2026].
26) Luca, S. D. (2025). Algorithmic discrimination under the AI Act and the GDPR. Brussels: European Parliament.
27) Lupășteanu, C. (2024). First integrated programme for the digitisation of local public administrations. Stiripesurse, 5 September.
28) Manheim, D., Martin, S., Bailey, M., Samin, M. and Greutzmacher, R. (2024). The necessity of AI audit standards boards. arXiv. [online] Available at: https://arxiv.org/abs/2404.13060 [Accessed 20 February 2026].
29) Mantelero, A. (2024). The fundamental rights impact assessment (FRIA) in the AI Act. arXiv. [online] Available at: https://arxiv.org/abs/2411.15149 [Accessed 23 February 2026].
30) Meimandi, K. J. et al. (2025). An adaptive responsible AI governance framework for decentralized organizations. arXiv. [online] Available at: https://arxiv.org/abs/2510.03368 [Accessed 25 February 2026].
31) Ministry of Finance of Romania. (2025). Technical specifications for AI solutions (CSac757062_26022025). Bucharest: Ministry of Finance.
32) Nastacă, C. C. and Profiroiu, A. G. (2024). An assessment of institutional resilience capacity. Croatian and Comparative Public Administration.
33) Organisation for Economic Co-operation and Development (OECD). (2021). The OECD Framework for Digital Talent and Skills in the Public Sector. OECD Working Papers on Public Governance, No. 45. Paris: OECD Publishing. [online] Available at: https://doi.org/10.1787/4e7c3f58-en [Accessed 29 February 2026].
34) Organisation for Economic Co-operation and Development (OECD). (2024). The OECD Reinforcing Democracy Initiative: Monitoring Report – Assessing Progress and Charting the Way Forward. OECD Public Governance Reviews. Paris: OECD Publishing. [online] Available at: https://doi.org/10.1787/9543bcfb-en [Accessed 27 January 2026].
35) Organisation for Economic Co-operation and Development (OECD). (2023). OECD Skills Outlook 2023: Skills for a Resilient Green and Digital Transition. Paris: OECD Publishing. [online] Available at: https://doi.org/10.1787/27452f29-en [Accessed 12 February 2026].
36) Onufreiciuc, R. (2023). Citizen participation in and through AI-enabled innovation. Logos Universality Mentality Education Novelty: Law, 12(1), pp. 91–104.
37) Pislaru, M., Vlad, C. S., Ivascu, L. and Mircea, I. I. (2024). Citizen-centric governance. Sustainability, 16(7).
38) Pripoaie, R., Schin, G. and Matic, A. (2024). Post-pandemic exploratory analysis. Sustainability, 16(11).
39) Public Buyers Community. (2025). Procurement of AI. [online] Available at: https://public-buyers-community.ec.europa.eu [Accessed 28 February 2026].
40) CAIDP Europe. (2024). Romania approves 2024–2027 AI strategy. 11 July.
41) Sanda, M., Siminică, M., Avram, C. and Popescu, L. (2024). Improving transparency in Romanian public procurement. Procedia Computer Science, 246, pp. 1210–1219.

42) Treasury Board of Canada Secretariat. (2019). Directive on automated decision-making. Ottawa: Government of Canada.
43) European Commission. (2022). Strengthening the digital skills of civil servants. Brussels: European Commission.
44) Squire Patton Boggs. (2024). The EU AI Act enters into effect.
45) Vatamanu, A. F. and Tofan, M. (2025). Integrating Artificial Intelligence into Public Administration: Challenges and Vulnerabilities. Administrative Sciences, 15(4), 149. [online] Available at: https://www.mdpi.com/2076-3387/15/4/149 [Accessed 15 March 2026].
46) Vrabie, C. (2024). Smart-optimism: Uncovering the resilience of Romanian city halls in online service delivery. arXiv. [online] Available at: https://arxiv.org/abs/2410.15189 [Accessed 10 March 2026].