

Automated Decision-Making and Data Protection: A Systematic Review on Organizational Risk, and Managerial Control

Cristina-Mihaela STANCIU*

National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania

*Corresponding author, cristina.stanciu00@upb.ro

Augustin SEMENESCU

¹National University of Science and Technology POLITEHNICA Bucharest, Bucharest, Romania

Academy of Romanian Scientists, Bucharest, Romania

augustin.semenescu@upb.ro

Abstract. *The purpose of this paper is to present a systematic review of recent literature regarding the way in which automated processing redefines organizational risk management and internal control practices. It also examines how managers integrate oversight mechanisms, performance monitoring of algorithmic models, and the early detection of operational risks into day-to-day decision workflows. Furthermore, the review explores also the legal context, outlining Article 22 of the GDPR and its interpretation, the rights of data subject and also the boundaries applicable to profiling. Based on more than a decade of European and international research, this paper aims to highlight the way by which managerial and legal perspectives converge through principles such as accountability, privacy by design and algorithmic auditing. It also takes into consideration the incorporation of ethical safeguards concerning the automated decision processes. The examination suggests that organizations benefit from integrated methodologies skilled of aligning compliance requirements with operational objectives while maintaining measures for fundamental rights.*

Keywords: managerial control, organizational risk, automated decision-making, GDPR, profiling, algorithmic audit, privacy by design, AI governance, data protection.

Introduction

In recent days, a common practice in organizations is represented by the adoption of automated decision-making systems based on artificial intelligence. These systems are used in multiple areas, including risk assessment, performance management, customer segmentation, and compliance monitoring. This way of developing has become relevant because of the ability of algorithmic systems to process large volumes of data and deliver standardized outputs within short timeframes. In the recent literature, it is indicated that automated decisions can no longer be considered just auxiliary tools. Instead, they are considered structural components of organizational decision architectures, shaping how managerial control is exercised and how internal responsibility is allocated (Shrestha et al., 2023; Benbya & McKelvey, 2023).

Considering that automated decisions are used in contexts with direct effects on individuals and organizations, it makes this topic so relevant. Given that in almost all organizations we can find two categories of individuals, executives and managers, the implications of automated decision making are important for both of them. On the executive side, the assessment process might be taken into account, because, if it is made in an automatic way, it can generate legal effects or outcomes with comparable consequences for the persons concerned. Also, it might generate issues linked to transparency, explainability, and the ability to challenge decisions. On the other hand,

from a managerial perspective, these developments reshape control mechanisms, since managers increasingly supervise the operation of decision systems rather than individual decisions themselves (Benbya & McKelvey, 2023).

Within the European Union, the use of automated decision-making is governed by a consolidated regulatory framework, most notably the General Data Protection Regulation. Article 22 of the GDPR addresses decisions based solely on automated processing and establishes specific rights for data subjects, including the right to human intervention and access to meaningful information about the logic involved. Recent guidance issued by the European Data Protection Board clarifies that these provisions have direct implications for how organizations must design and deploy automated decision systems. Legal compliance thus becomes an operational element of organizational governance rather than an external constraint (EDPB, 2023).

The main issue examined in this paper is the tension between the extensive usage of the automated decisions-making systems and the capacity of organizations to maintain managerial control and risk management mechanisms. Although automation is often associated with increased efficiency and consistency, recent studies indicate that this might intensify some organizational risks such as the lack of decision-making transparency, difficulties in the process of tasks allocation and the weakening of traditional forms of managerial oversight. (Kara & Ozalp, 2023; Sokol, 2024).

In terms of specific challenges, the organizations are faced with identifying and managing the risks generated by the behavior of algorithmic systems. These risks exceed the dimension of simple technical errors and also include cumulative effects regarding the decision-making process which might be difficult to fix, especially given the lack of adequate monitoring mechanisms. The recent researches highlight that dependence on external technical providers and the complexity of the implemented models limit the ability of organizations to fully understand and control the decision logic of the implemented systems. (Chiriță & Chiriță, 2025; Ispas, 2025).

Another challenge might be the integration of GDPR requirements into the existing managerial processes. Even though the law establishes clear requirements regarding the transparency, human intervention and protection of the rights of the involved persons, the literature highlights a difference between these and effective organizational practices. The formal adoption of compliance policies does not guarantee the efficient management of risks associated with automated decision-making processes when functional managerial mechanisms are missing. (Wachter & Mittelstadt, 2023).

The article adopts a systematic review and conceptual analysis approach, focusing on open-access academic and institutional literature published from 2023 onward. The analysis draws on articles indexed in recognized databases such as Web of Science and Scopus, alongside documents issued by European institutions relevant to data protection and artificial intelligence governance.

The analytical framework is grounded in a managerial perspective, examining how automated decisions affect organizational control and risk management. The legal dimension is addressed subsequently, not as an external framework, but as a set of constraints that shape managerial practices and the structure of decision processes. The article seeks to identify points of convergence between managerial control, legal compliance, and ethical governance as reflected in recent literature (Floridi & Taddeo, 2024).

The main research question guiding the analysis is how the use of artificial intelligence-based automated decisions influences the structure of managerial control and organizational risk management under the constraints imposed by the GDPR and the emerging framework of artificial intelligence governance. This question aims to clarify the relationship between decision efficiency, organizational governance, and the protection of fundamental rights.

The analysis proceeds from the assumption that the use of automated decisions leads to a shift from managerial control centered on the evaluation of individual decisions toward control focused on the supervision of decision systems and processes. A second assumption holds that automated decisions intensify organizational risks in the absence of adequate mechanisms for algorithmic auditing and continuous monitoring. A third assumption suggests that GDPR requirements on automated decision-making and profiling cannot be addressed effectively through isolated legal measures, but require integration into managerial control structures. A fourth assumption posits that governance models combining managerial control, legal compliance, and ethical oversight reduce the tension between operational efficiency and the protection of fundamental rights, enabling more responsible use of automation (Rahwan et al., 2023; Goodman, 2023).

Literature review

Recent literature treats the automated decision-making process as an essential component of the organizational development, having direct effects on the way in which the decision-making processes are structured and on how the managerial control is exercised. Research on the management and information systems merges on the idea that AI integration into decision-making processes reconfigures the traditional logic of the decision-making process. From the supervising process of individual decisions, the focus shifts to the supervision of the tool generating them. (Shrestha et al., 2023). This change reflects the adaptability to large data volumes, faster decision-making cycles and a growing complexity of the organizational environments in which the automated decisions operate.

Within this framework, managerial control is no longer primarily oriented toward validating final outcomes, but toward the continuous evaluation of automated decision processes. The literature notes that managers are less involved in approving each decision and more engaged in defining the rules, parameters, and boundaries within which algorithmic systems operate. This change requires a redefinition of managerial responsibilities and a different set of competencies, with greater emphasis on interpreting performance indicators and detecting systemic deviations (Benbya & McKelvey, 2023).

Figure 1 illustrates the structural difference between traditional decision-making, based on repeated managerial intervention, and automated decision-making, where control is exercised at the level of the decision system.

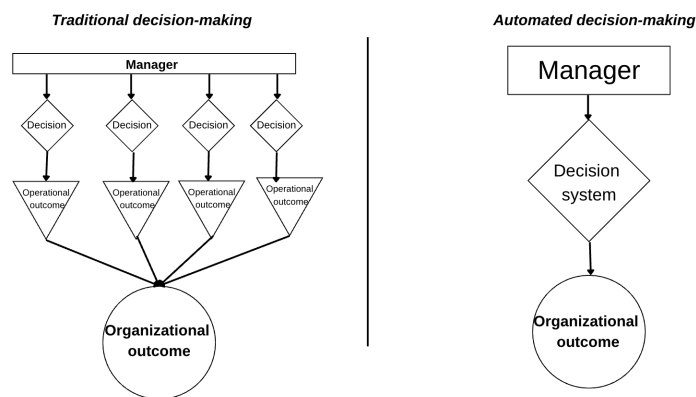


Figure 1. Comparison between traditional decision-making and automated decision-making from a managerial control perspective.

Author's own elaboration.

The transformation of the control logic is described as a transition from the direct control of decisions to a mediate control, exercised through quantitative indicators, trigger thresholds, and feedback mechanisms which are integrated into information systems. Control becomes less visible at the individual decision level, but is more present on the processes and automatized infrastructure levels. This kind of control is considered adequate for the contexts characterized by a high degree of complexity, in which human intervention, by a case to another, would be inefficient or difficult to apply on a large scale (Benbya & McKelvey, 2023).

At the same time, the literature underlines the fact that this reconfiguration does not exclude managerial positions. In fact, this role is transformed into one focused on the projection, evaluation and correction of systems. The purpose of the managers will be to supervise the behavior of algorithmic systems in a medium and long term.

Together with these risks, research highlights the fact that the reconfiguration of managerial control is associated with specific risks. Automated decisions might amplify the operational, reputational and, compliance risks when they are implemented without supervision, monitoring and audit mechanisms. Low levels of decision-making transparency and difficulties in explaining algorithmic results may lower trust in internal processes and may complicate the management of critical situations (Kara & Ozalp, 2023).

These risks are not presented just as side effects of the technology, but as results of the interaction between algorithmic systems and existing organizational structures. The way in which responsibilities are defined, in which internal control processes are organized and in which reporting channels work directly affect the organizational capacity of manage the risks associated with automatization. If there is a lack of governance structures adapted to these systems, problems generated by automated decisions will be difficult to identify and fix at a later stage, reinforcing the need for an integrated approach to managerial control and risk management.

Managerial perspectives on organizational risk in automated contexts

From a managerial perspective, the risks associated with automated decision are conceptualized as multidimensional phenomena go beyond the technical aspects and include governance, responsibilities and governmental control. Decision automation also introduces risks which might simultaneously affect operating processes, organizational structure and organization's capacity to respond quickly to unpredictable situations. These risks are amplified by the speed and scale at which they are applied which could lead to cumulative effects on the organizational performance. (Chiriță & Chiriță, 2025).

Literature highlights the fact that algorithmic systems could introduce systematic errors and discrepancies that are hard to identify, especially when monitoring mechanisms are lacking. Contrary to isolated human errors, the system errors could be replicated on a large scale, affecting a several number of decisions in a short period. From this perspective, the associated risk of automation is characterized by a high degree of propagation and persistence, and it requires different managerial approaches from those used in decisions-making contexts driven by humans.

The studies regarding risk management indicates that these risks are not fully controlled using traditional mechanisms of internal control designed for decision-making processes centred on the human resource. Verification procedures ex post and formal controls prove to be insufficient in automated decision-making environments, where the decisions are continuously generated in large

volumes. As a result, using AI in risks management systems needs de adaptability of existing procedures and developing new capacities for monitoring, evaluation and intervention. (Ispas, 2025).

The multidimensional and cumulative nature of organizational risks associated with automated decision-making is summarized in Figure 2.

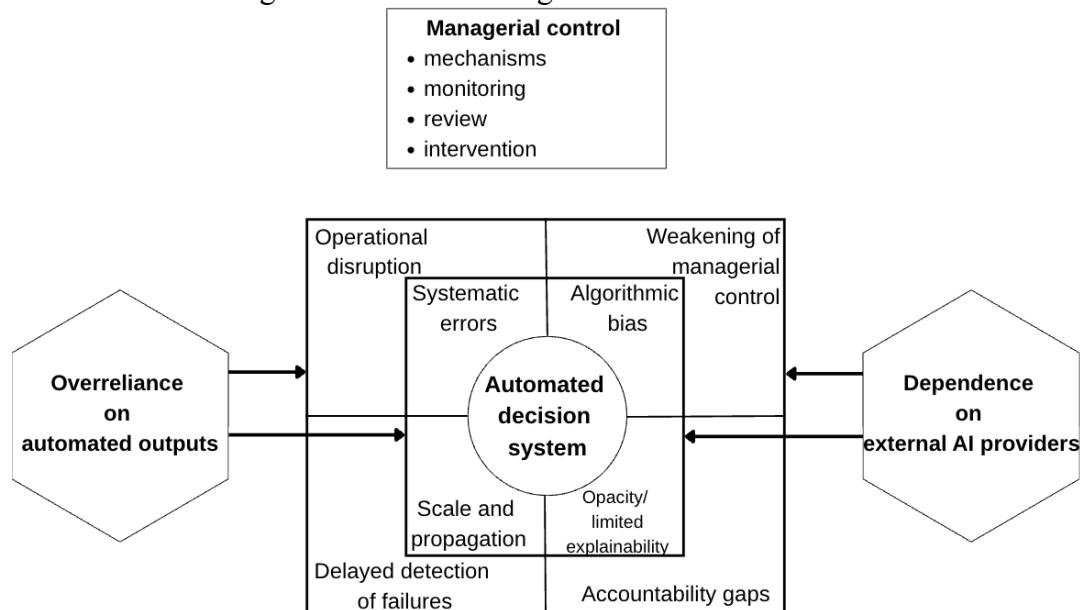


Figure 2. Multidimensional organizational risks associated with automated decision-making and their amplification mechanisms.

Author's own elaboration.

The absence of such adaptations is associated with a tendency toward overreliance on automated outputs. Managers may treat algorithmic decisions as objective or neutral, reducing critical assessment and weakening managerial vigilance. This dynamic can erode organizational control and delay the identification of problems, particularly when system performance deteriorates gradually.

A recurring theme in recent research is the role of algorithmic opacity in amplifying organizational risks. Limited explainability constrains managers' ability to understand the causes of errors and to intervene in a timely manner. This lack of transparency affects not only decision quality, but also the organization's capacity to assign responsibility and justify decisions to relevant stakeholders.

Opacity becomes more pronounced when organizations rely on artificial intelligence solutions developed by external providers. In such cases, control over models, data, and decision logic is restricted, reducing the ability to conduct independent assessments or implement rapid corrections. The literature identifies this dependence as an additional risk factor that must be incorporated into governance and risk management strategies for automated decision-making (Benbya & McKelvey, 2023).

Algorithmic auditing and organizational accountability

A distinct body of recent literature focuses on algorithmic auditing as a central instrument for ensuring organizational accountability and reducing risks linked to automated decisions. Algorithmic auditing is defined as a systematic process for evaluating the performance, correctness,

and impact of automated systems, integrated into governance structures and internal control mechanisms. This approach reflects the need to adapt control tools to the specific characteristics of automated decision processes, which operate at scale and with high complexity (Kara & Ozalp, 2023).

From a managerial and legal perspective, algorithmically auditing is analyzed as a mechanism which allows organizations to demonstrate efficient control over the implemented systems. Periodic assessments of algorithmic behavior contribute to an early identification of emergent risks and deviations from organizational objectives or regulatory requirements. This preventive function is relevant in situations where automated decision-making process could lead to similar effects on individual or important legal consequences. (Goodman, 2023).

Research underlines also that algorithmic auditing contributes to reducing accountability gaps generated by the use of AI. In absence of evaluation and documentation mechanisms, the responsibility for automated decisions might become diffuse and might lead to a difficult allocation of accountability between developers, users and managers. As a result, auditing is associated to a better decision traceability and to a better determination of roles and responsibilities in the organizational flow. (Goodman, 2023).

Another essential aspect that is highlighted in literature is the fact that algorithmic auditing does not have to be treated as an isolated activity or a reactive one, initiated only after the issues arise. In contrast, this is described as a continuous process, integrated throughout the whole life cycle of the automated decision-making systems, from design and implementation to use and later upgrades of the models. This type of approach allows a dynamic monitoring of performance and systems impact, supporting risk management in the long term. (Kara & Ozalp, 2023).

Recent analysis regarding algorithmic auditing ecosystem highlights the need of coordination between managerial functions, legal and technical functions. Auditing could not be effective if there is a lack of organizational structures that facilitate the communication between these departments and to integrate the audit results into decision-making processes. In the absence of this approach, the responsibility becomes fragmented and the auditing risks being reduced to a formal exercise, with a limited practical impact. (Costanza-Chock et al., 2023).

Consequently, literature highlights that algorithmic auditing must be correlated with existing governance mechanisms and adapted to the organizational context.

Legal perspectives on automated decision-making and profiling

Legal perspectives focus on the interpretation and application of Article 22 of General Data Protection Regulation, which governs decisions based exclusively on an automated processing and establishes the conditions under which these may produce legal effects or comparable effects on individuals. Recent studies underline the fact that these dispositions do not have only a declarative character, but they generate concrete operational obligations for organizations, shaping the way in which automated decision-making systems are designed and used. Guidelines established at the European level clarify the need to ensure decision transparency, human intervention and the effective protection of individuals' rights, positioning legal compliance as a structural element of organizational governance. (EDPB, 2023).

This legal approach is correlated with a functional interpretation of rights provided of GDPR. Individuals' rights are analyzed not only as formal guarantees, but also as instruments which allow them to understand the decision logic and to effectively challenge automated results. This interpretation highlights the limits of compliance strategies that are purely formal and

underlines the importance of integrating legal requirements into managerial processes and into internal control mechanisms. (Wachter & Mittelstadt, 2023).

The literature warns that, in the absence of this integration, the rights stipulated by GDPR risk to remaining difficult to integrate. The lack of clear internal procedures regarding the explanation and review of automated decisions may leave affected individuals without possibilities to challenge or understand the decisions. From this perspective, legal requirements are considered factors which might shape the structure of decision-making processes and the distribution of responsibility within organizations.

Profiling is addressed as a specific form of automated processing associated with high risks for fundamental rights. Its use in managerial contexts, as risk evaluation or customer segmentation is widely acknowledged. However, the research highlights that potential discriminatory, disproportioned side effects when adequate safeguard are lacking, especially in sensible decision-making context, with impact on individuals. (EDPB, 2023).

In response, legal literature underlines the need for rigorous data protection impact assessments and for additional control mechanisms. These include limitation of profiling activity, possibility of human intervention and the guarantee of decisions traceability. The risk-based approach adopted by European guidelines requires the adaptation of legal obligations to the significance of potential consequences, consolidating the link between legal compliance and organizational governance.

Overall, legal research treats Article 22 of the GDPR and profiling not just as data protection norms, but as instruments that directly influence the architecture of decision-making procedures. Integrating these requirements is presented as an essential condition for the responsible use of automated decisions and for maintaining the balance between operational efficiency and the protection of fundamental rights.

Artificial intelligence governance and human oversight

Recent literature regarding AI governance conceptualizes it as an integrative framework for managing organizational, legal and ethical effects of automated systems. AI governance is analyzed as a set of structures, processes and mechanisms of control which allow organizations to supervise the entire life cycle of intelligent systems, from design and implementation to impact assessment. This approach reflects a move away from the perspective of treating AI as a simple technical instrument and toward recognition of its structural role within the decision-making process. (Floridi & Taddeo, 2024).

Within this framework, AI governance is usually associated with the capacity to define clear responsibilities, to document the decision-making processes in proportion with systems' risk levels. The focus is on the development of flexible frameworks, able to adapt to different organizational contexts and to different types of automated decisions. This flexibility is considerate necessary in order to avoid excessive internal regulation and to maintain operational efficiency, especially in organizations at different stages of digital maturity. (Floridi & Taddeo, 2024).

Human oversight appears as a central element of AI governance, being presented as a balancing mechanism within the decision-making process. Oversight is not defined as a constant intervention in every decision, but as a set of institutional mechanisms which allow supervising, review and, when necessary, correction of automated results. Its role is to prevent negative effects and to maintain organizational control over decision-making processes. (Rahwan et al., 2023).

Research also underlines that human oversight must be adapted to the context and level of risks. In low-impact situations, the control might rely on moderate oversight and periodic

assessments. In contrast, in high-impact situations, more intensive forms of oversights are recommended, including the possibility of direct intervention and system suspension when significant deviations are identified. (Rahwan et al., 2023).

The human oversight integration in AI governance has direct implications on managerial structures. A clear definition of roles and responsibilities linked to systems' oversight also supports accountability and reduces the risks of responsibility diffusion. Without such mechanisms, automated decisions might generate situations in which none of the organizational actors is accountable for results, reducing the capacity for risks management. (Sokol, 2024).

The need to integrate managerial control, legal requirements, and ethical oversight into a coherent governance framework is illustrated in Figure 3.

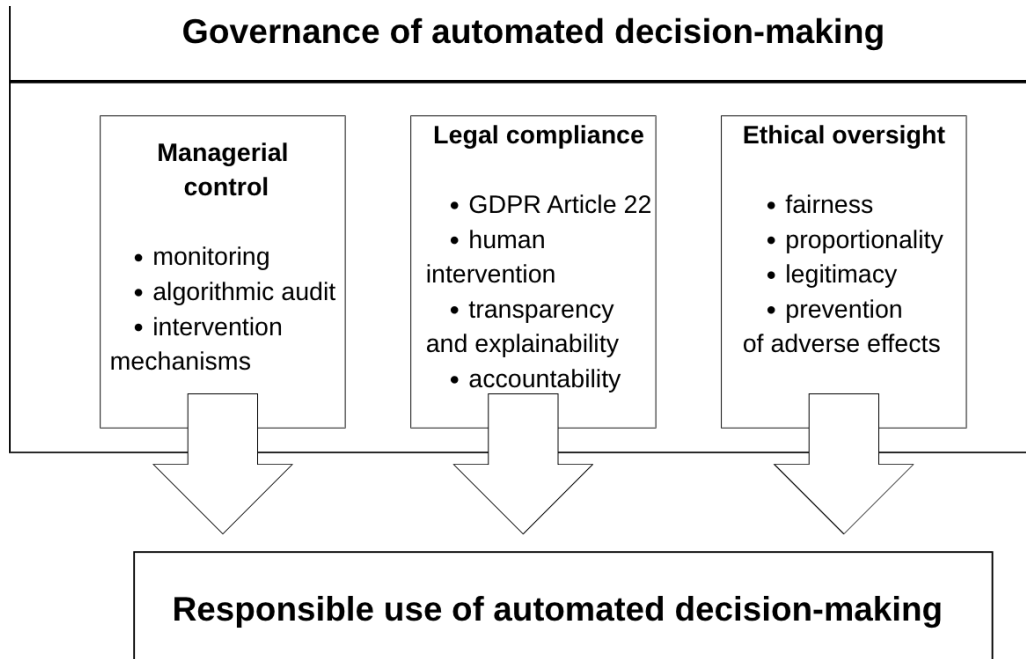


Figure 3. Integrated governance framework for automated decision-making

Author's own elaboration.

Another highlighted issue is the link between AI governance and legal requirements regarding data protection and automated decisions. Human oversight is considered a way of implementing legal obligations, like the right to human intervention and the possibility to challenge automated decisions. The integration of these mechanisms into governance frameworks aligns managerial control with legal requirements and strengthens legal compliance. (EDPB, 2023).

When viewed collectively, recent research presents AI governance and human oversight as interdependent elements of a broader managerial system. AI governance provides structural integration of legal, managerial and ethical requirements, while human oversight functions as an operational mechanism for reducing risks and maintaining legitimacy of automated decisions.

Working definitions of key concepts

In concordance with the analyzed literature, the automated decision-making process is defined as a decision-making process performed by algorithmic systems which generate results with limited

or absent human involvement and may produce significant effects on individuals or organizations. Managerial control refers to the set of mechanisms which allows organizations to monitor, evaluate and correct decision-making processes' behavior, including for the automated ones.(Benbya & McKelvey, 2023).

Organizational risks are conceptualized as the probability of negative effects occurring on organizational performance, compliance or reputation, generated by the use of automated systems. Accountability is defined as the organization's capacity to explain, justify and correct automated decisions and to assume the responsibility for its effects. (Goodman, 2023).

Identification of the literature gap

The analysis relies on the existence of a persistent gap between managerial, legal and ethical approaches regarding the automated decision-making process. Even though each perspective is widely discussed, these are rarely integrated into a coherent analytical framework. Research from the management domain mainly focuses on the efficiency and control, while the literature on compliance and ethical analysis focuses on normative principles, with less attention given to the interaction between these dimensions.

Fewer studies, especially examine the way in which managerial control mechanisms may put GDPR requirements into practice regarding the automated decision-making process. Existing literature offers limited models which integrate algorithmic auditing, legal accountability, and ethical oversight into a single system of organizational governance. This gap supports the relevance of present paper and forms the basis of its theoretical contributions.

Methodology

The study adopts a qualitative approach based on a systematic review and conceptual analysis. Its objective is to examine how recent literature describes the impact of automated decision-making on managerial control and organizational risk management. This methodological choice reflects the interdisciplinary nature of the topic and the current stage of research, which points to the need for a structured theoretical synthesis before the development of more consolidated empirical models.

Source selection was carried out through searches in recognized open-access databases, using combinations of terms such as "automated decision-making", "managerial control", "organizational risk", "algorithmic auditing", "AI governance", and "GDPR". Only works published between 2023 and 2025 were included, in order to capture the current state of research. In addition, institutional documents issued by European bodies relevant to data protection and artificial intelligence governance were examined.

Inclusion criteria targeted studies that explicitly address automated decision-making in organizational contexts and analyze implications for managerial control, risk, or governance. Purely technical studies without relevance for management or law were excluded, as were works that discuss artificial intelligence only at an abstract level. The literature was analyzed using a thematic approach, focusing on the identification of recurring concepts and points of convergence between managerial and legal perspectives.

The research design is qualitative and exploratory. The hypotheses formulated in the introduction serve as analytical reference points and are assessed through the consistency and convergence of arguments found in the reviewed literature. Given the conceptual nature of the study, no statistical software was used, and the research does not rely on quantitative empirical data.

Results and discussions

Recent literature review highlights a clear transformation of the way in which the managerial control is exercised in organization that use automated decision-making processes. The integration of AI-based systems moves the control from the evaluation of individual decisions to the system and decision-making oversight. In this context, managerial accountability focuses on parameter configuration, performance monitoring and algorithmic behavior over time, rather than punctual intervention in each individual decision. (Shrestha et al., 2023; Benbya & McKelvey, 2023).

This reconfiguration of managerial control is associated with a higher complexity of organizational governance. Control becomes more preventive and systemically, being exercised through continuous mechanisms for monitoring, performance indicators and feedback processes. If adequate governance structures are lacking, the automation may reduce the organization's capacity of intervention and correction, lowering the efficiency of managerial control. (Benbya & McKelvey, 2023).

A constant conclusion of the analyzed literature is the intensification of organizational risks associated with automated decisions. These risks include systemic errors, decision-making biases, lack of traceability and difficulty in assigning responsibilities. In situations where oversight mechanisms and algorithmic auditing lack, these kinds of risks persist and increase over time, having consequences on the organizational performance, but also on the reputation. (Kara & Ozalp, 2023; Sokol, 2024).

Risks generated by decision-making automatization are not limited to technical aspects. These have a pronounced managerial and strategic dimensions. Excessive dependency on algorithmic results and reducing the level of critical assessment may lead to systemic vulnerabilities, especially within organizations which adopt AI without compliant adjustments of internal procedures and disponible competences. (Chiriță & Chiriță, 2025; Ispas, 2025).

Algorithmic opacity has a central role in amplify the organizational risk. Limited capacity to explain the way automated system operates limits the organizations' ability to identify the deviations and to intervene in time. The issue becomes more significant when organizations use solutions developed by external suppliers on which they have limited technical and contractual control. (Benbya & McKelvey, 2023).

In this context, algorithmic auditing is identified as an essential instrument for maintaining the managerial control and lowering the risks associated with automated decisions. Auditing is defined as a continuous process of performance evaluation, compliance and impact of algorithmic systems, integrated in governance structures of organizations. The integration of auditing mechanisms into internal processes supports decision traceability and clarify organizational responsibility. Kara & Ozalp, 2023; Goodman, 2023).

Recent analyses regarding the algorithmic auditing ecosystem underline that the efficiency of this instrument depends on coordination between managerial, legal and technical functions. Algorithmic auditing produces relevant results only when it is supported by documented processes and clear organizational structures, which allows systematical risks evaluation and corrective intervention when necessary. (Costanza-Chock et al., 2023).

Literature also underlines that legal dimension of the automated decision-making process directly influences the managerial organizational structure and the organizational governance. GDPR requirements regarding decisions exclusively based on automated processing do not perform as simple external constraints but also influence the internal architecture of decision-

making processes by imposing some operational obligations linked to transparency, human intervention and the protection of individuals' rights. (EDPB, 2023).

Another recurrent conclusion is that these legal obligations cannot be efficiently implemented using isolated formal measures such as general policies or standardized notifications. Approaches focused only on formal compliance do not adequately address issues linked to decision-making opacity and responsibility distribution within organizations and, eventually, they are insufficient for the management of risks associated with automation. (Wachter & Mittelstadt, 2023).

Requirements regarding the right to human intervention and access to relevant information on decision-making logic require the existence of some internal mechanisms which allow the explanation and review of automated decisions. Recent literature indicates that these mechanisms need a functional integration between managerial, legal and technical structures, consolidating the role of internal governance as a way of processing of legal norms. (EDPB, 2023).

Profiling is discussed as a specific form of the automated decision-making process which generates higher risks for fundamental rights. Even though its use in legit managerial targets as risk evaluations or customer segmentation is frequently met, research underlines that profiling may produce discriminatory or disproportionate effects when adequate guarantees are lacking. These risks require a rigorous evaluation of the impact and some control mechanisms adapted to the gravity of potential consequences. (EDPB, 2023).

The risks-based approach promoted by European Union, including the context of a future regulation regarding AI (Artificial Intelligence Act), consolidate this perspective. Differentiation based on the level of risk associated to AI systems highlights the need of flexible mechanisms of governance, capable of adapting to different organizational contexts and types of automated decisions. (European Commission, 2023).

Legal and managerial literature converges on the idea the efficient management of automated decisions need the overcoming of fragmented approaches. Treating legal compliance and managerial control as separated domains limits the organizations' capacity to react to complex risks generated by automation. Integrating the legal requirements in managerial control structures supports a clearer allocation to responsibilities and a better traceability of decisions. (Sokol, 2024).

In this context, the governance frameworks of AI are analyzed as ways of aligning of managerial, legal and ethical dimensions of the decision-making process. AI governance is defined as a set of structures and processes which allow the control, accountability and evaluations of automated systems throughout their life cycle. (Floridi & Taddeo, 2024).

Human oversight represents a central element of these frameworks, and it is analyzed as a mechanism of reducing risks associated with complete automation. Maintaining an adequate level of human oversight in automated decisions contribute to preventing negative effects and supports the legitimacy decision-making processes, especially when they have a significant impact on individuals (Rahwan et al., 2023).

The integration of auditing in governance frameworks is, also, highlighted as being essential for guaranteeing compliance and for an efficient managerial control. Algorithmic auditing allows a systematic evaluation of performance and system impacts, supporting the early identification of risks and correcting them before producing important effects. Recent analyses underline that the efficiency of algorithmic auditing depends on its integration in organizational processes and coordination between involved functions. (Costanza-Chock et al., 2023).

Overall, conclusions suggest that integrated models of governance offer organization a better capacity to manage the tension between decision-making efficiency and the protection of

human rights. In comparison with fragmented approaches, integrated frameworks allows a better alignment between managerial control and legal and ethical requirements, supporting a more accountable and suspensible use of the automated decision-making process.

Conclusion

This paper aims to offer an integrated analysis of recent literature regarding the automated decision-making process, examining the way in which the use of AI-based systems reconfigures the managerial control, organizational risk management and governance mechanisms. Its main contribution is the approach to the automated decision-making process as a structural element of organizational processes and not as a simple independent technological instrument. The paper underlines that automation determines a transition from direct control to the systems oversight and to decision-making processes, with clear implications on responsibility and decision traceability.

A second contribution concerns the integration of the legal dimension in managerial control analysis. GDPR requirements regarding automated decision-making process and profiling are analyzed as factors which shape the architecture of internal procedures and not as external isolated obligations. Within this framework, the study underlines the actual role of algorithmic auditing and AI governance as mechanisms which are focused on legal compliance, managerial control and organizational risk management.

This research stems from the necessity to clarify the relationship between automated decision-making processes and the organizations' capacity to maintain control and responsibility within a technological and normative environment which is continuously evolving. Recent literature frequently approaches in a separately managerial, legal and ethical dimensions of automated decisions. By putting together these perspectives in a single analytical framework, this article contributes to reducing conceptual fragmentation already existing in this domain.

The findings are relevant for both academic research and broader debates on the responsible use of artificial intelligence. The analysis offers a theoretical basis for understanding how managerial control needs to adapt to challenges posed by automated decisions, particularly in organizations operating under strict legal constraints, such as those imposed by the European data protection framework.

From an applied perspective, the conclusions may inform organizations in the design or revision of governance mechanisms for automated decision-making. Integrating algorithmic auditing into internal control structures, clearly defining managerial responsibilities, and establishing appropriate forms of human oversight can reduce operational and legal risks associated with automation.

The proposed conceptual framework may also serve as a starting point for developing internal policies on artificial intelligence use, especially in small and medium-sized organizations with limited resources for implementing complex governance models. The integrated approach outlined in this study allows control mechanisms to be adapted to risk levels and organizational maturity.

Future research could focus on empirical testing of the relationships identified in this conceptual analysis. Quantitative or qualitative studies conducted within organizations that rely on automated decisions could assess the effectiveness of managerial control and algorithmic auditing

mechanisms in mitigating identified risks. Comparative research across sectors or jurisdictions could also reveal meaningful differences in how artificial intelligence governance is implemented.

Another relevant avenue for further study concerns the interaction between GDPR requirements and the obligations introduced by the Artificial Intelligence Act, particularly with respect to high-risk systems. Integrating these regulatory frameworks into operational governance models remains underexplored and presents clear research potential.

The main limitation of this study lies in its conceptual nature and reliance on existing literature. Although the analysis draws on recent and relevant sources, the absence of an empirical component limits the generalizability of the conclusions. In addition, the focus on open-access literature published after 2023 may exclude relevant contributions available only through restricted access.

A further limitation relates to the rapid pace of change in this domain. Technological and regulatory developments may quickly alter the conditions under which automated decisions are used, requiring periodic updates to the proposed analytical framework. These limitations do not undermine the relevance of the findings, but they point to the need for complementary research and for adaptive approaches to the study of automated decision governance.

Acknowledgments: During the preparation of this work, the authors used ChatGPT-4 for language revision, translation support, and readability improvement. The use of AI-assisted translation and editing tools may influence the results of automated AI-content detection systems and could generate false-positive indications of AI-generated text. Following the use of these tools, the authors carefully reviewed, revised, and validated the final manuscript and assume full responsibility for the content of the publication.

References

- Chiriță, M., & Chiriță, G. (2025). *Assessing the risk of artificial intelligence impact on decision-making automation in digital businesses*. Annals of “Dunărea de Jos” University of Galați, Fascicle I. <https://doi.org/10.35219/eai15840409503>
- European Commission. (2023). *Artificial Intelligence Act – harmonised rules on artificial intelligence*. European Union. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- European Data Protection Board (EDPB). (2023). *Guidelines on automated decision-making and profiling under GDPR*. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en
- European Data Protection Supervisor (EDPS). (2025, September 23). *TechDispatch #2/2025 – Human oversight of automated decision-making*. https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2025-09-23-techdispatch-2025-human-oversight-automated-making_European_Data_Protection_Supervisor
- Saeri, A. K., Lloyd George, S., Graham, J., Lacarriere, C. D., Slattery, P., Noetel, M., ... Thompson, N. (2025). *Mapping AI risk mitigations: Evidence scan and preliminary AI risk mitigation taxonomy*. arXiv. <https://doi.org/10.48550/arXiv.2512.11931>
- Costanza-Chock, S., Harvey, E., Raji, I. D., Czernuszenko, M., & Buolamwini, J. (2023). *Who audits the auditors? Recommendations from a field scan of the algorithmic auditing ecosystem*. arXiv. <https://doi.org/10.1145/3531146.3533213>
- Górka, E., Baran, D., Wojak, G., Cwiakała, M., Zupok, S., Starkowski, D., ... Okrasa, O. (2025). *The impact of artificial intelligence on enterprise decision-making process*. arXiv. <https://doi.org/10.35808/ersj/4143>
- Ispas, L. (2025). *Artificial intelligence applications in risk management systems*. Systems, 13(11), 967. <https://doi.org/10.3390/systems13110967>

- Goodman, E. P. (2023). *Algorithmic auditing: Chasing AI accountability*. Santa Clara High Technology Law Journal, 37(3), 1–30. Available at <https://digitalcommons.law.scu.edu/chtlj/vol39/iss3/1/>
- Technical University of Vienna & European Institute. (2024). *Towards accountable algorithms: Tools and methods for evaluating AI systems*. https://digitalfuturesociety.com/app/uploads/2024/02/Towards-accountable-algorithms_eng.pdf
- Kloumann, I. M., & Eubank, S. (2025). *AI risk governance frameworks and societal standards*. arXiv. <https://doi.org/10.48550/arXiv.2503.05937>
- Ukanwa, K. (2023). *Why firms should want algorithmic accountability*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4148214
- European Union Agency for Fundamental Rights (FRA). (2023). *Handbook on European data protection law – AI implications*. <https://fra.europa.eu/en/publication/2023/fundamental-rights-report-2023>
- Edinburgh Data Ethics Group. (2024). *Human oversight and responsible AI*. <https://edpms.europa.eu/data-protection/our-work/publications/techdispatch/2025-09-23-techdispatch-22025-human-oversight-automated-making>