

INFORMATION MANAGEMENT ETHICS AS AN ELEMENT OF THE NON-MILITARY SECURITY OF STATES AND ORGANIZATIONS

Łukasz SKIBA

Politechnika Częstochowska, Wydział Zarządzania; lukasz.skiba@pcz.pl, ORCID: 0000-0002-5176-3265

Purpose: This article examines the role of information management ethics in the non-military security of states and organizations. It explores how information governance affects institutional resilience, critical infrastructure protection, and public trust, while identifying risks related to artificial intelligence, dual-use technologies, and state information infrastructure.

Design/methodology/approach: The study employs a qualitative comparative analysis of literature and normative documents in the fields of security, management, technology ethics, and international law. The theoretical considerations are supported by a comparative analysis of artificial intelligence systems, dual-use technologies, and state information infrastructure, representing algorithmic, strategic, and systemic information-related risks. The assessment is based on transparency, accountability, institutional control, proportionality, and resilience.

Findings: The results suggest that threats to non-military security arise primarily from deficiencies in information governance rather than from technology itself. Transparency, accountability, control, and proportionality emerge as key factors shaping security and resilience. The study also proposes a four-dimensional model of ethical information management comprising normative, procedural, control, and cultural dimensions.

Research limitations/implications: The article is theoretical in nature and does not include empirical verification of the proposed model. Further research is needed to examine the implementation of ethical information management principles and their impact on security and institutional resilience.

Practical implications: The proposed model may support the development of information governance systems, security policies, compliance procedures, and ethical standards, particularly in relation to AI, data protection, and cybersecurity.

Social implications: Ethical information management contributes to the protection of citizens' rights, the strengthening of public trust, and greater resilience to hybrid, cyber, and information threats.

Originality/value: The article integrates perspectives from management, security, information ethics, and emerging technologies within a single analytical framework. It highlights the relationship between information management quality and non-military security, while identifying mechanisms through which ethical governance may support institutional resilience.

Keywords: information ethics, information management, non-military security, artificial intelligence, information governance.

Category of the paper: Conceptual Paper / Research Paper.

1. Introduction

The security of the modern state can no longer be analyzed solely in military terms (Burgess, 2007; Kitler, 2011). The development of digital technologies, the globalization of information flows, and the growing dependence of socio-economic systems on information and communication technology (ICT) infrastructure have led to the emergence of non-military security as an important field of study (Kitler, 2011). Hybrid, cyber, and information threats demonstrate that a state may be destabilized without the use of armed force, through information manipulation, disinformation, or disruptions to ICT systems (Franke, 2015).

In this context, information ceases to be merely a resource supporting decision-making processes and becomes an integral element of security infrastructure (Boin, van Eeten, 2013). In management studies, the concept of information governance has gained increasing attention and is understood as a system of principles and mechanisms regulating the information life cycle within an organization (Smallwood, 2019; Singh, 2025). It encompasses both an operational dimension - related to data quality and integrity - and a normative dimension, referring to legal compliance, proportionality, and institutional accountability (Rhodes, 1996; Bovens, 2007).

The development of artificial intelligence and predictive analytics in public administration complicates the relationship between efficiency and accountability (Pasquale, 2015; Clever, 2025). The AI Act (European Parliament and Council, 2024) introduces a classification of AI systems based on their level of risk and imposes requirements regarding transparency and the assessment of their impact on fundamental rights. Consequently, information management becomes an integral component of the regulatory framework that determines the level of security.

At the same time, Regulation (EU) 2021/821 (European Parliament and Council, 2021) extends the responsibilities of states and enterprises with regard to the transfer of dual-use technologies. Analytical and cryptographic technologies may serve both civilian and military purposes (Rath, Ischi, Perkins, 2014), which necessitates the implementation of risk identification and assessment procedures. In this context, ethical information management becomes a tool for the prevention of strategic risks (Floridi, 2013).

Despite the growing body of research on cybersecurity and artificial intelligence, there is still a lack of in-depth analysis of information management ethics as a component of non-military security from a management perspective (Floridi, 2013). The aim of this article is to demonstrate that the integration of the principles of proportionality, transparency, accountability, and compliance into information governance systems enhances institutional resilience and mitigates the risk of informational destabilization (Boin, van Eeten, 2013; Power, 2007).

The foregoing considerations justify the need to examine non-military security from a management perspective, in which the quality of information governance constitutes a key analytical category (Rhodes, 1996).

2. Non-Military Security from a Management Perspective

2.1. Non-Military Security as a Governance Challenge

The concept of non-military security has evolved alongside the expansion of the spectrum of threats extending beyond the traditional military paradigm (Burgess, 2007). The literature emphasizes that the modern state functions as a complex organizational system whose stability depends on the effective functioning of social, economic, and informational processes (Kitler, 2011). Security is understood as the ability to maintain the continuity of critical structures and functions under conditions of disruption (Boin, van Eeten, 2013; OECD, 2024).

From a management perspective, non-military security may be interpreted as an outcome of the quality of governance, understood as a system of oversight, accountability, and control of decision-making processes (Rhodes, 1996; Bovens, 2007). Institutional resilience stems not only from the redundancy of technical infrastructure but also from the quality of the information upon which decisions are based (Boin, van Eeten, 2013). In the digital environment, information becomes both a strategic resource (Barney, 1991) and a potential source of risk (Floridi, 2013).

Disruptions in the flow of information - resulting from disinformation, manipulation, or failures of information and communication technology (ICT) systems - may lead to a loss of decision-making capacity and the erosion of public trust (Franke, 2015). In this sense, non-military security is closely linked to the quality of information management. Ethical standards for data processing, procedural transparency, and control mechanisms constitute an integral part of security infrastructure (Bovens, 2007; Power, 2007).

2.2. Information as Security Infrastructure

In the context of digitalization, information infrastructure underpins the functioning of other critical systems, including energy, transportation, and financial systems (Boin, van Eeten, 2013). Administrative systems based on digital data processing, combined with analytical tools employed in crisis management, constitute a complex decision-making architecture, the disruption of which may result in destabilization without the use of armed force (Franke, 2015).

From this perspective, information management ethics performs an infrastructural function (Floridi, 2013). A lack of transparency, uncontrolled data processing, or the instrumental use of information may result in the loss of legitimacy of public institutions (Hausner, 2008). Public trust thus becomes an essential component of systemic security (Kitler, 2011).

2.3. Governance as a Security Mechanism

Governance in the public sector encompasses regulatory mechanisms, oversight procedures, and systems of accountability (Rhodes, 1996; Bovens, 2007). In the digital environment, information governance must integrate both technical and normative dimensions (Smallwood, 2019). European regulations, such as the AI Act (European Parliament and Council, 2024) and Regulation (EU) 2021/821 (European Parliament and Council, 2021), emphasize the need for risk assessment, documentation of decision-making processes, and control over technology transfers. Consequently, information management becomes an integral component of compliance and risk management (Power, 2007), and its quality directly affects the level of non-military security (Boin, van Eeten, 2013).

Since non-military security depends on the quality of information processes, a deeper understanding of information as a strategic resource of states and organizations is required (Barney, 1991).

3. Information as a Strategic Resource for States and Organizations

The ongoing digitalization of public administration is transforming information into a strategic resource (Barney, 1991). In a data-driven economy, organizational advantage depends not only on access to tangible resources but also on the quality of information and the ability to process it effectively (Barney, 1991; Smallwood, 2019). In the public sector, this translates into the quality of administrative decision-making, the effectiveness of crisis management, and the protection of critical infrastructure (Boin, van Eeten, 2013; Kitler, 2011).

Decisions based on incomplete, outdated, or distorted data lead to deficiencies in the decision-making process, which, in the context of non-military security, may generate systemic consequences (Kitler, 2011). Digital transformation also shifts responsibility from the level of individual administrative decisions to that of information systems and algorithmic processes (Pasquale, 2015). Artificial intelligence systems used in public administration directly affect the legal status of citizens, thereby increasing the importance of transparency and oversight (European Parliament and Council, 2024; Bovens, 2007).

3.1. Information Capital and Systemic Resilience

Institutional resilience refers to the ability to maintain critical functions under conditions of disruption (Boin, van Eeten, 2013). In the digital environment, it depends on the quality of the information architecture, including data integrity, system security, and the clear allocation of responsibility (Smallwood, 2019; Bovens, 2007). Technical redundancy alone is not sufficient unless it is supported by a coherent system of governance (Rhodes, 1996).

The key elements include:

- the clear assignment of responsibility for data (Bovens, 2007),
- access control and auditing of data processing activities (Power, 2007),
- compliance with national and European Union regulations (European Parliament and Council, 2016; European Parliament and Council, 2022),
- the systematic assessment of technological risks (European Parliament and Council, 2024; Power, 2007).

The lack of these mechanisms increases susceptibility to abuse, data breaches, and the instrumentalization of information for purposes that conflict with the public interest (Floridi, 2013; Pasquale, 2015).

3.2. The Regulatory Dimension and Dual-Use Technologies

The strengthening of the regulatory framework within the European Union underscores the strategic nature of information. The AI Act imposes obligations regarding risk assessment and the documentation of decision-making processes in high-risk systems (European Parliament and Council, 2024). Regulation (EU) 2021/821 extends export controls to dual-use technologies, including information technology solutions (European Parliament and Council, 2021). The GDPR and the NIS2 Directive further reinforce accountability in the areas of data protection and ICT risk management (European Parliament and Council, 2016; European Parliament and Council, 2022).

Dual-use technologies - including analytical and cryptographic systems - may be employed for both civilian and military purposes (Rath, Ischi, Perkins, 2014). This requires the implementation of procedures for identifying sensitive technologies, assessing transfer risks, and monitoring international cooperation (European Parliament and Council, 2021). On this basis, information management becomes an element of strategic security (Franke, 2015; Kitler, 2011).

The strategic nature of information implies the need for its normative conceptualization, which has led to the emergence of information management ethics as a distinct analytical category within management studies (Floridi, 2013; Crane, Matten, 2016).

4. Information Management Ethics as a Normative Category

In management studies, ethics has traditionally been examined in the context of organizational responsibility toward stakeholders and corporate governance (Freeman, 1984; Crane, Matten, 2016). However, the digitalization of decision-making processes has necessitated the recognition of information management ethics as a distinct area of inquiry (Floridi, 2013; Ribeiro et al., 2025). It encompasses norms governing the collection, processing, and use of data, as well as responsibility for the consequences of decisions based on digital systems (Pasquale, 2015).

In the information society, information shapes both institutional and social relationships (Floridi, 2013; Ribeiro et al., 2025). Managing information therefore entails managing its impact on citizens and stakeholders (Freeman, 1984). Information management ethics is not merely a moral category but also a regulatory mechanism that influences the level of systemic security (Burgess, 2007; Kitler, 2011).

In the public sector, particular importance is attached to the principle of proportionality, according to which data processing must be appropriate and proportionate to the public purpose it serves (European Parliament and Council, 2016). European regulations - particularly the GDPR and the AI Act - strengthen the obligation to conduct risk assessments, document decision-making processes, and ensure algorithmic transparency (European Parliament and Council, 2016; European Parliament and Council, 2024). Information governance thus becomes a system that integrates ethical standards with operational practice (Smallwood, 2019; Bovens, 2007).

4.1. Accountability and Transparency

Accountability refers to the ability to assign responsibility for decisions and to ensure the existence of control mechanisms (Bovens, 2007). In the context of information management, it includes the identification of the entity responsible for data, the ability to reconstruct the decision-making process, and the availability of information to supervisory authorities (Rhodes, 1996).

A lack of transparency leads to the emergence of “black-box decision-making”, in which decisions of public significance are made without the possibility of verification (Pasquale, 2015). In the context of information threats, deficits in transparency increase the vulnerability of institutions to a loss of legitimacy and destabilization (Franke, 2015; Floridi, 2013).

4.2. Information Ethics and Risk Management

Information management is associated with multidimensional risks, including data protection breaches, algorithmic errors, information manipulation, and the uncontrolled transfer of dual-use technologies (Rath, Ischi, Perkins, 2014; Pasquale, 2015). Regulations such as

Regulation (EU) 2021/821 require the implementation of due diligence procedures and compliance systems (European Parliament and Council, 2021).

The integration of ethics into risk management reduces the likelihood of destabilizing events (Power, 2007; Mokander, Floridi, 2024). Responsible information governance mitigates the risks of critical infrastructure data breaches, systemic algorithmic discrimination, and the strategic consequences of technology transfers (Floridi, 2013; Boin, van Eeten, 2013).

4.3. The Cultural Dimension

Formal regulations do not guarantee effectiveness unless they are accompanied by an organizational culture grounded in responsibility (Schein, 2010). The internalization of ethical norms by members of an organization strengthens institutional resilience (Boin, van Eeten, 2013). Information management ethics thus becomes an element of a security culture that encompasses awareness of information-related threats, a willingness to report violations, and responsible leadership (Hausner, 2008; Kitler, 2011).

The conceptualization of information management ethics as a normative category makes it possible to identify the fundamental mechanisms governing information processes within organizations and state structures. However, this perspective remains primarily theoretical and requires further development through reference to specific technological domains in which the tensions between efficiency, control, and accountability become most apparent.

For this reason, a comparative analysis of selected areas of digital transformation is undertaken to operationalize the adopted analytical categories and identify recurring patterns of risk. The analysis focuses on artificial intelligence systems, dual-use technologies, and state information infrastructure.

5. Qualitative Study: Operationalization and Comparative Analysis of Information Management Risks

To further develop the adopted theoretical assumptions, a qualitative comparative study was conducted based on a content analysis of academic literature, legal regulations, and publications concerning information security. The study adopts an exploratory and interpretive approach and seeks to identify recurring risk patterns associated with information management in the context of digital transformation, with particular emphasis on the development of artificial intelligence systems and their implications for information security (OECD, 2024; Zhang, Zhao, Meng, Lai, Chen, 2025).

The starting point of the analysis was the operationalization of analytical categories derived from the preceding theoretical considerations. It was assumed that the key dimensions for assessing the quality of information governance include the transparency of data-processing

processes, the ability to assign responsibility for decisions, the effectiveness of institutional control mechanisms, the appropriateness of data processing in relation to public objectives, and the impact of information systems on institutional resilience (Bovens, 2007; Boin, van Eeten, 2013; European Parliament and Council, 2016). The application of these categories enables a shift from a normative analysis to a comparative approach, allowing for the identification of recurring risk mechanisms.

The selection of research cases was theoretical in nature and focused on areas of particular significance for non-military security (Kitler, 2011).

To ensure analytical coherence, the study focuses on three areas that represent distinct but complementary dimensions of information-related security risks. Artificial intelligence systems illustrate algorithmic risks associated with automated decision-making, opacity, and accountability deficits. Dual-use technologies represent strategic risks arising from the transfer and potential misuse of technologies that may serve both civilian and military purposes. State information infrastructure reflects systemic risks connected with the continuity and resilience of critical public functions dependent on digital information systems.

Together, these areas capture three fundamental levels at which information management influences non-military security: decision-making processes, technology governance, and the operational functioning of state structures. The objective was not to provide an exhaustive overview of all information-related threats, but rather to identify recurring governance mechanisms across different categories of risk.

Other important domains, including cybersecurity management, disinformation governance, and critical data platforms, were not treated as separate analytical categories because they operate as cross-cutting phenomena within the examined areas. Cybersecurity is embedded in the governance of information infrastructure, disinformation directly affects the quality and integrity of information processes, while critical data platforms constitute components of broader information ecosystems. Their exclusion as standalone cases was therefore intended to avoid conceptual overlap and to maintain a clear comparative framework.

The analysis covered artificial intelligence systems used in decision-making processes, dual-use technologies, and state information infrastructure, which constitutes the foundation of contemporary socio-economic systems. Accordingly, each of the selected areas represents a distinct type of risk - algorithmic, strategic, and systemic - thereby enabling a multidimensional analysis of information management challenges within the broader framework of non-military security.

The analysis of artificial intelligence systems indicates that their growing importance in public administration enhances the efficiency of data processing while simultaneously creating tensions between operational effectiveness and institutional accountability (Pasquale, 2015; European Parliament and Council, 2024; Tallam, 2025).

It should be noted, however, that artificial intelligence systems are not a homogeneous category. The level of risk associated with their use depends on both the functional characteristics of the system and the context in which it is deployed. In accordance with the AI Act, different regulatory requirements apply to systems presenting limited, high, or unacceptable levels of risk (European Parliament and Council, 2024).

Particular ethical and governance challenges arise in high-risk applications used within public administration, especially where AI supports decisions concerning access to public services, social benefits, migration procedures, law enforcement, or critical infrastructure management. In such contexts, limitations in explainability and transparency may significantly affect the ability of individuals to understand, challenge, or verify administrative decisions. By contrast, AI systems used for routine administrative support or information management generally pose lower risks to fundamental rights and institutional legitimacy.

Consequently, the concepts of “black-box decision-making” and “automated accountability” should be understood primarily in relation to high-impact decision environments, where algorithmic outputs may substantially influence the legal status, rights, or obligations of individuals.

The limited transparency of algorithms makes it difficult to reconstruct the decision-making process, thereby weakening the ability to assign responsibility. As a consequence, a phenomenon of “automated accountability” emerges, whereby decisions of public significance are increasingly made through processes that are difficult to verify, thereby heightening the risk of systemic errors and undermining public trust (Pasquale, 2015; Floridi, 2013; McCormack, Huyskes, Lewis, Bendeckache, 2025).

In the case of dual-use technologies, the key issue is not the technology itself but rather the insufficient effectiveness of regulatory mechanisms designed to control its use (Rath, Ischi, Perkins, 2014). The dual nature of these technologies means that the boundary between civilian applications and potentially military or repressive uses remains fluid. European Union regulations, particularly Regulation (EU) 2021/821, introduce obligations related to risk assessment and the implementation of due diligence procedures; however, their effectiveness depends on integration with organizational management practices (European Parliament and Council, 2021; Power, 2007). In this area, the problems of dispersed accountability and the limited effectiveness of control mechanisms in a transnational environment are particularly evident.

The analysis of state information infrastructure highlights its fundamental importance for systemic stability. Data-processing systems constitute the foundation for the functioning of other critical infrastructure sectors, meaning that their disruption may lead to cascading effects (Boin, van Eeten, 2013). At the same time, a tension exists between the need for data transparency and openness and the necessity of protecting sensitive information. Excessive data accessibility increases vulnerability to cyber threats, whereas excessive restrictions on data access may reduce the efficiency and transparency of public administration (Franke, 2015).

The results of the comparative analysis are presented in Table 1., which synthesizes the relationships between the informational function of each area, the type of risk involved, and the degree to which key governance categories are implemented.

Table 1.

Comparative Analysis of Information Management Across the Examined Areas

Area	Informational Function	Type of Risk	Transparency	Accountability	Control	Proportionality	Impact on Resilience
AI	Decision automation	Algorithmic	Low	Limited	Moderate	Problematic	High
Dual-use	Technology transfer	Strategic	Moderate	Dispersed	Low-moderate	Critical	High
Information Infrastructure	Systems integration	Systemic	Variable	Formally high	High	Conflicting	Very high

Source: Author's own.

The interpretation of the results indicates that the key factor determining the level of risk is not the degree of technological advancement itself, but rather the quality of information management (Boin, van Eeten, 2013; Power, 2007; Challenges in AI Governance, 2025). As system complexity increases, there is a tendency toward reduced transparency and weakened accountability mechanisms. This trend is particularly evident in artificial intelligence systems, where deficits in transparency lead to the emergence of decision-making structures with limited controllability (Bovens, 2007; Pasquale, 2015).

The analysis further indicates that accountability constitutes one of the weakest elements of the system, particularly in transnational and technological contexts where responsibility becomes dispersed (Bovens, 2007). In the case of dual-use technologies and AI systems, this problem is structural in nature and cannot be resolved solely through formal regulation. At the same time, the findings suggest that the effectiveness of control mechanisms depends on their integration with organizational processes, implying that formal compliance alone is insufficient to ensure security (Power, 2007).

On this basis, it can be argued that information management ethics functions as a mechanism for reducing systemic risk by integrating normative and operational dimensions (Floridi, 2013). Its importance increases particularly under conditions of high technological complexity, limited transparency, and dispersed accountability. In such circumstances, deficiencies in information governance may lead to systemic destabilization, thereby confirming its crucial role within the structure of non-military security (Franke, 2015; Kitler, 2011).

The analysis conducted indicates that the identified risk mechanisms are systemic and recurring in nature, regardless of the technological characteristics of the areas under examination. This suggests that their source lies not solely in the level of technological advancement but, above all, in the quality of information management and the degree of

integration among normative, procedural, and control mechanisms (Boin, van Eeten, 2013; Power, 2007).

The findings justify the need for a synthetic conceptualization of the relationship between information management ethics and non-military security. In response to this need, the following section proposes a theoretical model that integrates the identified dimensions into a coherent system of information governance (Rhodes, 1996; Smallwood, 2019).

6. A Model of Ethical Information Management as an Element of Non-Military Security

The analysis conducted allows for the conclusion that information management ethics constitutes a structural component of non-military security (Burgess, 2007; Kitler, 2011). On this basis, a model has been proposed that integrates normative, organizational, and systemic dimensions, illustrating how ethical standards are translated into institutional resilience (Boin, van Eeten, 2013; Choung, David, Seberger, 2023).

The model is four-dimensional and comprises:

- The normative dimension - relating to the principles of proportionality, the protection of individual rights, transparency, and accountability (European Parliament and Council, 2016; Bovens, 2007).
- The procedural dimension - encompassing the standardization of data-processing activities, the documentation of decisions, and information quality control (Smallwood, 2019).
- The control dimension – associated with auditing, compliance systems, risk assessment, and oversight mechanisms (Power, 2007).
- The cultural dimension – concerning the internalization of ethical norms and responsible leadership (Schein, 2010).

This approach is consistent with recent proposals concerning responsible AI systems, which emphasize the interdependence of trustworthy AI design, auditability, accountability, and governance as conditions for embedding responsibility throughout the AI lifecycle (Herrera-Poyatos et al., 2025).

The model is systemic in nature because it assumes the interdependence of all dimensions, and the weakening of any one of them leads to the erosion of the entire information security mechanism (Boin, van Eeten, 2013). The integration of these four dimensions within an information governance system enhances institutional resilience and, consequently, strengthens non-military security (Kitler, 2011).

6.1. The Normative Dimension

The normative dimension is grounded in both European Union and national regulations. The AI Act introduces the obligation to assess risks associated with high-risk AI systems (European Parliament and Council, 2024), the GDPR reinforces the principles of data minimization and accountability (European Parliament and Council, 2016), and regulations concerning dual-use technologies impose requirements for controlling technology transfers (European Parliament and Council, 2021). In practice, this entails the need to assess the impact of information systems on fundamental rights and to ensure that data processing remains proportionate to the public purpose it serves (Floridi, 2013).

From a security perspective, normative frameworks reduce the risk of the instrumentalization of technology and strengthen the legitimacy of public decisions (Burgess, 2007).

6.2. The Procedural Dimension

The procedural dimension refers to the technical and organizational principles governing information processing. It encompasses the standardization of procedures, the documentation of algorithmic decisions, and access control mechanisms for data (Smallwood, 2019). The quality and integrity of information determine the reliability of the decision-making process, while their absence may lead to systemic errors of strategic significance (Barney, 1991; Kitler, 2011).

6.3. The Control Dimension

The control dimension encompasses systems of auditing, reporting, and risk assessment (Power, 2007). Due diligence procedures related to technology transfers, data protection impact assessments, and the monitoring of ICT threats constitute essential elements of information risk management (European Parliament and Council, 2021; European Parliament and Council, 2022). These mechanisms reduce the likelihood of destabilizing events (Boin, van Eeten, 2013).

6.4. The Cultural Dimension

Organizational culture determines the effectiveness of formal regulations (Schein, 2010). The internalization of ethical norms, awareness of information-related threats, and responsible leadership strengthen the coherence of the governance system (Hausner, 2008). Without this dimension, compliance procedures may become merely formalized practices lacking real effectiveness (Power, 2007).

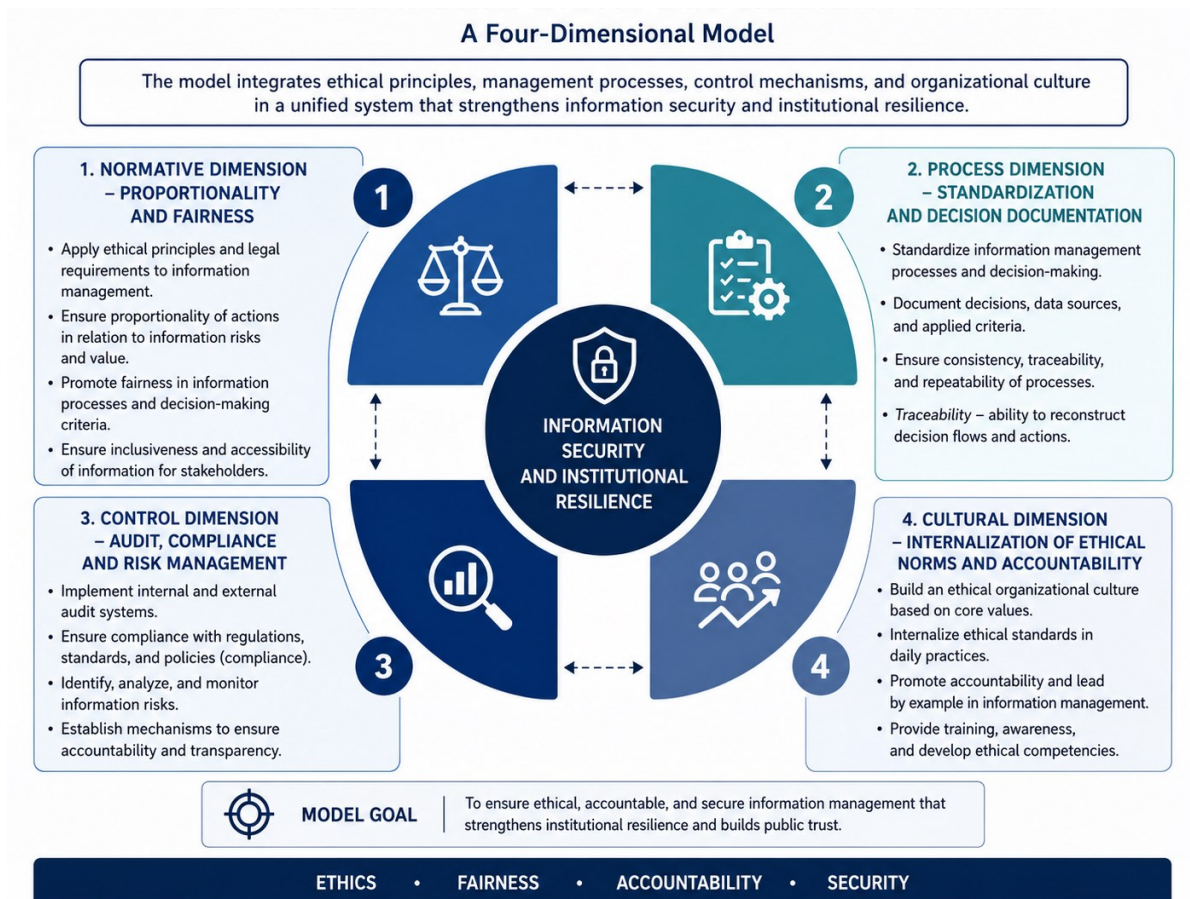


Figure 1. Ethical information management model.

Source: Author's own.

The model presents four complementary dimensions - normative, procedural, control, and cultural - integrated within an information governance system. The combined effect of these dimensions is institutional resilience, which in turn contributes to the non-military security of states and organizations (Boin, van Eeten, 2013; Kitler, 2011).

However, the proposed model requires validation through its application in public management practice and through engagement with contemporary regulatory challenges (European Parliament and Council, 2024).

7. Discussion: Implications for Public Management and Systemic Security

The findings presented indicate that non-military security should not be understood solely as a strategic category analyzed within security studies, but rather as an outcome of the quality of management processes, particularly those related to the processing and use of information (Burgess, 2007; Kitler, 2011). From this perspective, information governance serves as

a mechanism for stabilizing public systems by integrating regulatory, technological, and axiological dimensions (Rhodes, 1996; Floridi, 2013; UNDP, 2025).

The results of the comparative analysis confirm that institutional resilience is largely determined by the quality of information management. Regardless of the specific area under examination—artificial intelligence systems, dual-use technologies, or state information infrastructure—the transparency of decision-making processes, the ability to assign responsibility, and the effectiveness of control mechanisms remain of critical importance (Boin, van Eeten, 2013; Bovens, 2007). Deficiencies in these areas give rise to systemic risks, the source of which lies not in the technology itself but in the manner in which it is governed and managed.

The findings extend existing approaches in the literature, which have focused primarily on the technical aspects of cybersecurity or the regulatory frameworks governing AI systems. The analysis conducted indicates that the key challenge lies in the insufficient integration of the normative dimension with operational practice. In particular, a tension is evident between the efficiency of decision-making processes and the requirements of transparency and accountability, a tension that becomes increasingly pronounced in the context of digitalization (Pasquale, 2015; Crane, Matten, 2016).

This phenomenon is reflected in the observed tendency toward the “automation of accountability”, whereby responsibility for decisions is increasingly shifted to algorithmic systems without a corresponding strengthening of institutional control mechanisms. As a consequence, situations may arise in which formal compliance with regulatory requirements does not translate into genuine transparency or the effective verifiability of decision-making processes (Bovens, 2007; Pasquale, 2015; Habibu, Obudra, 2025).

European Union regulations, including the AI Act and Regulation (EU) 2021/821, strengthen the normative and control dimensions of information management by introducing documentation requirements, risk assessment obligations, and oversight mechanisms governing the transfer of technologies (European Parliament and Council, 2024; European Parliament and Council, 2021). At the same time, they reveal a structural tension between the need to ensure security and the need to preserve innovation and operational efficiency. Excessive regulation may constrain the adaptive capacity of organizations, whereas insufficient regulation increases vulnerability to systemic risks.

From a public management perspective, the integration of information governance with risk management and quality management systems is of critical importance. The findings indicate that the effectiveness of control mechanisms depends not only on their formal implementation but also on the extent to which they are embedded in organizational processes and institutional culture (Power, 2007; Schein, 2010). This implies that information management ethics cannot be reduced to a matter of compliance alone; rather, it should be regarded as an integral component of organizational culture and management practice.

In this context, the proposed four-dimensional model may be interpreted as a tool that integrates three levels of analysis: normative, organizational, and systemic. Its significance lies in demonstrating the mechanism through which ethical standards influence the quality of decision-making processes and, consequently, the level of institutional resilience (Boin, van Eeten, 2013).

Accordingly, non-military security may be reinterpreted as the outcome of an organization's ability to manage information in a responsible, transparent, and governance-oriented manner. This perspective shifts the focus from reactive crisis management toward the proactive development of information systems that are resilient to disruptions and abuses (Rhodes, 1996; Floridi, 2013).

8. Conclusion

The theoretical considerations and qualitative analysis conducted in this study support the view that information management ethics may be regarded as a structural component of the non-military security of states and organizations. In the context of digital transformation, information has ceased to serve merely as a resource supporting decision-making processes and has become a strategic asset that determines institutional resilience and systemic stability.

The results of the comparative analysis indicate that the primary source of risk is not the level of technological advancement itself but rather the quality of information management. Regardless of the specific characteristics of the areas examined - including high-risk artificial intelligence systems used in public decision-making, dual-use technologies, and state information infrastructure - the transparency of decision-making processes, the ability to assign responsibility, and the effectiveness of control mechanisms are of fundamental importance. Deficiencies in these areas give rise to systemic risks, including decision-making errors, informational destabilization, and the erosion of trust in public institutions.

The analysis supports the argument that non-military security may be interpreted as being closely related to the quality of information governance. This perspective suggests a shift in focus from viewing threats primarily in technological terms toward the analysis of management processes that determine how information is used within public and organizational systems. From this standpoint, information management ethics may be understood as a mechanism that has the potential to mitigate systemic risk through the integration of normative, operational, and control dimensions.

The proposed four-dimensional model should be regarded as a theoretical framework that explains possible relationships between information governance and institutional resilience. The analysis suggests that the interaction of normative, procedural, control, and cultural dimensions may contribute to the development of more coherent information management

systems and may support resilience-building efforts. However, the effectiveness of these mechanisms has not been empirically verified within the scope of this study and therefore requires further investigation in real organizational and public-sector settings.

The findings also underscore the importance of linking formal regulations with organizational practice. The effectiveness of oversight and control mechanisms derives not solely from their normative foundations but also from their actual implementation within management processes and organizational culture. In this context, information management ethics should be regarded not merely as a component of compliance but as an integral element of management systems and resilience-building efforts.

The article contributes to management studies by conceptualizing non-military security as an outcome of the quality of information management and by identifying the mechanism through which ethical standards contribute to the stability of public and organizational systems. The proposed approach is application-oriented and may serve as a foundation for the design of information security policies and the development of governance systems in both public administration and the private sector.

Future research should focus on the empirical validation of the proposed model and on examining its application in public management practice, particularly in the context of implementing regulations related to artificial intelligence and cybersecurity.

References

1. Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99-120. <https://doi.org/10.1177/014920639101700108>
2. Boin, A., van Eeten, M.J.G. (2013). The resilient organization. *Public Management Review*, 15(3), 429-445. <https://doi.org/10.1080/14719037.2013.769856>
3. Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal*, 13(4), 447-468. <https://doi.org/10.1111/j.1468-0386.2007.00378.x>
4. Burgess, J.P. (2007). The ethical subject of security research. *Security Dialogue*, 38(3), 285-304. <https://doi.org/10.1177/0967010607081519>
5. Choung, H., David, P., Seberger, J.S. (2023). A Multilevel Framework for AI Governance. In: *The Global and Digital Governance Handbook*. Retrieved from: <https://arxiv.org/abs/2307.03198>
6. Clever, D. (2025). *Ethical Governance and Accountability in Artificial Intelligence*. Retrieved from: <https://www.researchgate.net/publication/397655186>
7. Crane, A., Matten, D. (2016). *Business ethics: Managing corporate citizenship and sustainability in the age of globalization* (4th ed.). Oxford University Press.

8. European Parliament and Council (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*, L119, 1-88.
9. European Parliament and Council (2021). Regulation (EU) 2021/821 of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. *Official Journal of the European Union*, L206, 1-461.
10. European Parliament and Council (2022). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*, L333, 80-152.
11. European Parliament and Council (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.
12. Floridi, L. (2013). *The ethics of information*. Oxford University Press.
13. Franke, U. (2015). *War by non-military means: Understanding Russian information warfare*. Swedish Defence Research Agency (FOI), Rapportnr/Report no: FOI-R--4065--SE.
14. Freeman, R.E. (1984). *Strategic management: A stakeholder approach*. Pitman.
15. Habibu, T., Obudra, C. (2025). Ethical AI and Privacy: Strategies for Effective Governance. *DS Reviews of Research in Life Sciences*, Vol. 3, pp. 44-64, doi: 10.59232/AIR-V3I4P101_. Retrieved from: <https://www.researchgate.net/publication/401241385>
16. Hausner, J. (2008). *Zarządzanie publiczne*. Scholar.
17. Herrera-Poyatos, A., Del Ser, J., López de Prado, M., Wang, F.-Y., Herrera-Viedma, E., Herrera, F. (2025). *Responsible Artificial Intelligence Systems: A Roadmap to Society's Trust through Trustworthy AI, Auditability, Accountability, and Governance*. Retrieved from: https://arxiv.org/abs/2503.04739?utm_source=chatgpt.com
18. Kitler, W. (2011). *Bezpieczeństwo narodowe RP. Podstawowe kategorie. Uwarunkowania. System*. Akademia Obrony Narodowej.
19. McCormack, L., Huyskes, D., Lewis, D., Bendeckache, M. (2025). *Trust and Transparency in AI: Industry Voices on Data, Ethics, and Compliance*. Retrieved from: <https://arxiv.org/abs/2509.22709>
20. Mokander, J., Floridi, L. (2024). *Operationalising AI Governance Through Ethics-Based Auditing: An Industry Case Study*. Retrieved from: <https://arxiv.org/abs/2407.06232>
21. Organisation for Economic Co-operation and Development (OECD). (2024). *AI, Data Governance and Privacy: Synergies and Areas of International Co-operation* (OECD Artificial Intelligence Papers, No. 22). Paris: OECD Publishing. Retrieved from: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/ai-data-governance-and-privacy_2ac13a42/2476b1a4-en.pdf

22. Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
23. Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford University Press.
24. Rath, J., Ischi, M., Perkins, R. (2014). Evolution of different dual-use concepts in international and national law. *Science and Engineering Ethics*, 20(3), 769-790. <https://doi.org/10.1007/s11948-014-9519-6>
25. Rhodes, R.A.W. (1996). The new governance: Governing without government. *Political Studies*, 44(4), 652-667. <https://doi.org/10.1111/j.1467-9248.1996.tb01747.x>
26. Ribeiro, D., Rocha, T., Pinto, G., Cartaxo, B., Amaral, M., Davila, N., Camargo, A. (2025). *Toward Effective AI Governance: A Review of Principles*. Retrieved from: <https://arxiv.org/abs/2505.23417>
27. Schein, E.H. (2010). *Organizational culture and leadership* (4th ed.). Jossey-Bass.
28. Singh, A. (2025). Data governance and ethics in AI-Powered Platforms. *World Journal of Advanced Research and Reviews*, Vol. 26, Iss. 1, pp. 398-406, doi: 10.30574/wjarr.2025.26.1.1068
29. Smallwood, R.F. (2019). *Information governance: Concepts, strategies, and best practices*. Hoboken: John Wiley & Sons, p. 544.
30. Tallam, K. (2025). *Decoding the Black Box: Integrating Moral Imagination with Technical AI Governance*. Retrieved from: <https://arxiv.org/abs/2503.06411>
31. United Nations Development Programme (UNDP). (2025). *Global Approaches to AI Governance*. Retrieved from: <https://www.undp.org/sites/g/files/zskgke326/files/2025-11/undp-kazakhstan-global-approaches-ai-governance.pdf>
32. Zhang, Y., Zhao, C., Meng, Z., Lai, C.S., Chen, X. (2025). An Ethical Assessment Framework for AI Security and Ethics in Smart Grid. *Global Energy Interconnection*. Retrieved from: <https://www.sciencedirect.com/science/article/pii/S2096511725001252>