

Generative AI as a Knowledge Governance Mechanism: The Role of Digital Trust and Information Security

Justyna Żywiołek

Faculty of Management, Czestochowa University of Technology, Poland

justyna.zywiolek@wz.pcz.pl

Abstract: The rapid diffusion of generative artificial intelligence (GAI) is transforming organizational knowledge processes, yet existing research offers limited insight into its governance implications. This study addresses this gap by conceptualizing GAI as a mechanism of knowledge governance and examining its relationship with digital trust, information security maturity, and decision quality. Data from 300 firms across Poland, Germany, and Spain were collected using a CAWI survey of top management teams. Structural equation modeling (SEM) and multilevel analysis were applied to test relationships between AI-mediated knowledge practices, digital trust, information security maturity, and perceived decision quality. The results show that AI use significantly increases digital trust, which in turn improves decision quality. Digital trust acts as a mediator, while information security maturity moderates this relationship. The findings indicate that the impact of generative AI on decision-making depends on governance conditions rather than technology alone.

Keywords: Generative artificial intelligence, Knowledge governance, Digital trust, Information security

1. Introduction

In the contemporary digital economy, the rapid advancement and diffusion of generative artificial intelligence (GAI) is fundamentally transforming how knowledge is created, interpreted, and governed within organizations. Unlike earlier forms of artificial intelligence, generative systems operate not only as analytical tools but as autonomous agents capable of producing novel content, shaping interpretations, and influencing decision-making processes (Bresciani et al. 2021). As a result, organizations increasingly rely on algorithmically generated knowledge, which challenges traditional assumptions about epistemic authority, knowledge ownership, and managerial cognition. These developments signal a shift from human-centered knowledge paradigms toward hybrid epistemic systems in which human and non-human actors co-produce organizational knowledge.

This transformation introduces a critical need to reconceptualize knowledge governance. While prior research has extensively explored knowledge management systems, organizational learning, and AI adoption, existing frameworks remain largely grounded in anthropocentric epistemologies and do not sufficiently address the governance implications of algorithmically mediated knowledge processes. In particular, the integration of generative AI raises fundamental questions regarding trust, reliability, accountability, and security in knowledge-intensive environments (Żywiołek et al. 2025a). Consequently, knowledge governance must be redefined to incorporate both technological infrastructures and socio-organizational mechanisms that regulate the production, validation, and use of AI-generated knowledge.

Two interrelated constructs—digital trust and information security—emerge as central to this new governance landscape. Digital trust reflects the extent to which organizational actors are willing to rely on algorithmically generated knowledge in decision-making processes, while information security ensures the integrity, confidentiality, and controllability of data and knowledge flows. Together, these dimensions form the foundation for the legitimacy and stability of AI-mediated knowledge systems (Almustafa and Kalash 2025). Without sufficient levels of digital trust, managers may resist or underutilize AI outputs, whereas inadequate information security can undermine organizational resilience and expose firms to new forms of epistemic and operational risk (Hussain et al. 2024).

The intersection of generative artificial intelligence, knowledge governance, and information security has begun to attract scholarly attention; however, existing studies tend to focus either on technological capabilities or on isolated organizational outcomes (Żywiołek et al. 2025c). At the team level, it transforms coordination mechanisms, collective validation processes, and knowledge-sharing practices. At the organizational level, it introduces new forms of synthetic memory, algorithmic dependency, and governance complexity (Khan et al. 2026).

Building on these considerations, this study conceptualizes generative artificial intelligence as a new regime of knowledge governance that restructures epistemic processes across multiple organizational levels. By integrating perspectives from knowledge management, information systems, and organizational theory, the research develops a comprehensive framework linking AI-mediated knowledge practices with digital trust, information security maturity, and decision quality (Alavi and Leidner 2001). Empirically, the study draws on a

large-scale, multi-country dataset collected from top management teams in knowledge-intensive firms, enabling the examination of cross-level relationships using advanced analytical techniques (Żywiłek et al. 2025b).

Despite the growing body of research on artificial intelligence in organizational contexts, important gaps remain in understanding its implications for knowledge governance. First, existing studies are rarely anchored in knowledge governance theory and tend to focus on technological capabilities rather than on the structures that regulate knowledge creation, validation, and use. Second, limited attention has been given to digital trust as a mediating mechanism that conditions whether AI-generated knowledge is incorporated into managerial decision-making. Third, there is a lack of multilevel empirical evidence capturing how AI-mediated knowledge processes simultaneously affect individual cognition, team dynamics, and organizational governance structures.

To address these gaps, this study conceptualizes generative artificial intelligence as a mechanism of knowledge governance that reshapes epistemic processes across organizational levels and examines its relationship with digital trust, information security maturity, and decision quality (Tsai et al. 2022).

For analytical clarity, several key constructs are defined. Knowledge governance is understood as the set of formal and informal mechanisms that regulate the creation, validation, distribution, and use of knowledge within organizations. Digital trust refers to the extent to which organizational actors are willing to rely on AI-generated knowledge in decision-making processes. Epistemic authority denotes the perceived legitimacy of a source—human or algorithmic—in shaping knowledge claims and guiding judgment. Synthetic organizational memory describes the accumulation and use of AI-generated knowledge artifacts that are stored, recombined, and reused within organizational systems independently of direct human cognition. This study builds on these definitions to examine how generative artificial intelligence reconfigures knowledge governance and influences decision-making outcomes in contemporary organizations (Modgil et al. 2026).

Existing research on artificial intelligence in organizations has primarily focused on technological capabilities, adoption processes, and performance outcomes, with limited integration into knowledge governance theory. While knowledge management literature provides robust frameworks for understanding knowledge creation and sharing, it remains largely grounded in human-centered assumptions and does not fully account for the role of algorithmic agents in shaping epistemic processes. As a result, the governance implications of AI-mediated knowledge remain underdeveloped.

Moreover, prior studies have addressed trust in AI mainly as a factor of user acceptance or technology adoption, rather than as a mediating mechanism linking AI-generated knowledge with decision-making outcomes. Similarly, existing research tends to examine AI effects at a single level of analysis, overlooking the interconnected dynamics between individual cognition, team processes, and organizational structures.

This study addresses these limitations by integrating perspectives from knowledge management, AI research, and governance theory into a unified framework. It conceptualizes generative AI as a mechanism of knowledge governance, examines digital trust as a mediating construct, and provides multilevel empirical evidence based on cross-country data.

2. Materials and Methods

This study adopted a quantitative research design to investigate the role of generative artificial intelligence (GAI) as a mechanism of knowledge governance and its impact on digital trust, information security, and decision-making processes within organizations. Data were collected using the Computer-Assisted Web Interviewing (CAWI) method, which enabled the efficient acquisition of standardized responses from senior executives operating in knowledge-intensive industries. The primary objective of the empirical analysis was to examine cross-level relationships between AI-mediated knowledge practices, digital trust, information security maturity, and perceived decision quality.

The research was conducted across three European countries—Poland, Germany, and Spain—to ensure a comparative and cross-national perspective. These countries were selected due to their similar levels of digital transformation, regulatory alignment within the European Union, and increasing adoption of artificial intelligence in organizational contexts. The study focused on top management teams (TMTs), as they play a critical role in shaping strategic decisions, knowledge governance structures, and the adoption of emerging technologies such as generative AI.

In the second phase, a large-scale CAWI survey was conducted in 2024. A total of 300 firms participated in the study, with respondents drawn from senior executive positions, including CEOs, CIOs, CTOs, and other members of top management teams. The sampling strategy ensured representation across knowledge-intensive sectors

such as finance, information technology, consulting, and advanced manufacturing. The multi-country design allowed for the analysis of contextual similarities and differences in AI-driven knowledge governance practices.

The study employed a purposive sampling strategy targeting senior executives from knowledge-intensive firms that actively use or experiment with artificial intelligence solutions. A database of firms operating in Poland, Germany, and Spain was used to identify potential respondents, and invitations to participate in the survey were distributed electronically.

A total of 319 questionnaires were distributed, of which 300 valid responses were obtained, resulting in a response rate of approximately 88%. Only fully completed questionnaires from top management representatives were included in the final dataset. This ensured that respondents possessed sufficient knowledge of organizational decision-making processes and AI adoption practices.

The survey instrument consisted of a structured questionnaire divided into four sections. The first section captured demographic and organizational characteristics, including firm size, industry, respondents' managerial roles, and experience with artificial intelligence technologies. The second section focused on AI-mediated knowledge practices, measuring the extent to which generative AI is used in knowledge creation, interpretation, and decision support. The third section assessed digital trust and information security maturity, capturing managerial perceptions of trust in AI-generated outputs, data reliability, and the robustness of security frameworks. The fourth section evaluated perceived decision quality and governance outcomes, including changes in epistemic authority, knowledge ownership, and organizational risk exposure.

The questionnaire was pre-tested with a group of academic experts and industry practitioners to ensure clarity, reliability, and content validity. All constructs were measured using multi-item scales adapted from prior literature in knowledge management and information systems research and adjusted to the context of generative artificial intelligence. Responses were recorded on a five-point Likert scale (1 = strongly disagree, 5 = strongly agree).

AI-mediated knowledge practices were measured using [5] items capturing the extent to which generative AI supports knowledge creation, interpretation, and decision-making processes. A sample item is: "Generative AI tools are regularly used to support managerial decision-making." Digital trust was measured using [5] items reflecting the perceived reliability, credibility, and usability of AI-generated knowledge. A sample item is: "I trust the outputs generated by AI systems when making decisions."

Information security maturity was assessed using [5] items capturing the robustness of organizational security practices. A sample item is: "Our organization has well-established procedures to ensure the security of AI-related data." Decision quality was measured using [5] items reflecting perceived effectiveness and accuracy of decisions supported by AI. A sample item is: "Decisions supported by AI are of higher quality than those based solely on human judgment."

To analyse the data, structural equation modeling (SEM) and multilevel analytical techniques were employed. SEM was used to test the relationships between key constructs and to assess the mediating role of digital trust in the relationship between AI-mediated knowledge practices and decision quality. Multilevel modeling enabled the examination of cross-level effects, capturing how individual-level perceptions aggregate into team-level dynamics and organizational-level governance outcomes. The reliability and validity of the measurement model were assessed using standard procedures. Internal consistency was confirmed through Cronbach's alpha and composite reliability (CR), with all values exceeding the recommended threshold of 0.70. Convergent validity was evaluated using average variance extracted (AVE), with all constructs exceeding the threshold of 0.50.

Discriminant validity was assessed using the Fornell–Larcker criterion and the heterotrait–monotrait ratio (HTMT). In all cases, the square root of AVE exceeded inter-construct correlations, and HTMT values remained below the recommended threshold of 0.85. The structural model demonstrated a satisfactory fit to the data. The fit indices were within acceptable ranges (CFI = 0.94, TLI = 0.93, RMSEA = 0.05, SRMR = 0.04), indicating that the proposed model adequately represents the observed data.

Figure 1 presents the research design and process, illustrating the sequential stages of the study—from conceptual model development, through survey design and data collection, to advanced statistical analysis and interpretation of results. This structured approach ensures a comprehensive examination of how generative artificial intelligence functions as a new regime of knowledge governance and how it reshapes organizational processes through the interplay of digital trust and information security.

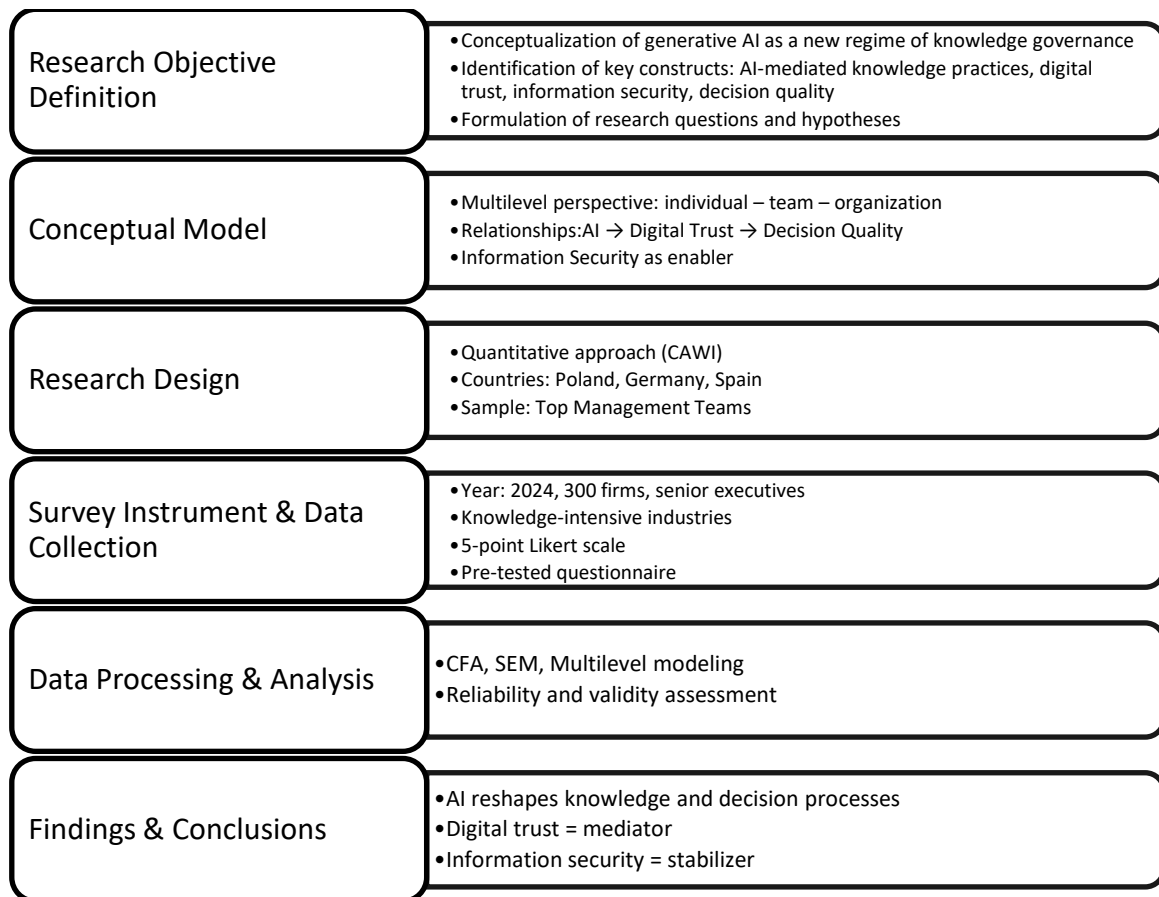


Figure 1: Research procedure

Figure 1 presents a structured overview of the research process, encompassing the stages from conceptualizing generative artificial intelligence as a knowledge governance mechanism, through the development of the multilevel research model and survey design, to data collection and advanced statistical analysis. This systematic approach enables a comprehensive examination of how AI-mediated knowledge practices, digital trust, and information security interact across individual, team, and organizational levels. The following section presents the empirical findings, providing insights into the role of generative AI in reshaping epistemic authority, enhancing or constraining decision quality, and redefining governance mechanisms within contemporary organizations. To assess the potential impact of common method bias, Harman's single-factor test was conducted. The results indicated that a single factor did not account for the majority of the variance, suggesting that common method bias is unlikely to be a serious concern. Additionally, procedural remedies such as ensuring respondent anonymity and careful questionnaire design were applied to minimize potential bias.

3. Results

The results of the study provide empirical evidence on how generative artificial intelligence operates as a new regime of knowledge governance, reshaping epistemic processes across individual, team, and organizational levels. The analysis focuses on the relationships between AI-mediated knowledge practices, digital trust, information security maturity, and perceived decision quality. Particular attention is given to the reconfiguration of epistemic authority, managerial sensemaking, and knowledge ownership in environments where algorithmically generated knowledge increasingly complements and, in some cases, substitutes human cognition.

The empirical analysis provides strong support for the proposed model of generative artificial intelligence as a mechanism of knowledge governance. The results of the structural equation modeling (SEM) indicate that AI-mediated knowledge practices have a significant positive effect on digital trust ($\beta = 0.62$, $p < 0.001$), confirming that the increased use of generative AI in knowledge processes is associated with higher levels of managerial reliance on algorithmically generated outputs. The structural model explains a substantial proportion of variance in the key endogenous constructs. The R^2 value for digital trust is 0.38, while the model explains 0.47 of the

variance in decision quality, indicating moderate to strong explanatory power. Effect sizes (f^2) indicate that AI-mediated knowledge practices have a large effect on digital trust ($f^2 = 0.62$), while digital trust has a substantial effect on decision quality ($f^2 = 0.41$). The moderating effect of information security maturity is moderate ($f^2 = 0.18$). Confidence intervals (95%) obtained using bootstrapping confirm the stability of the estimates, with all key relationships remaining statistically significant within the interval bounds.

Digital trust, in turn, demonstrates a strong positive relationship with perceived decision quality ($\beta = 0.54$, $p < 0.001$), supporting its role as a key mediating construct. The indirect effect of AI-mediated knowledge practices on decision quality through digital trust is statistically significant ($\beta = 0.33$, $p < 0.001$), indicating that trust conditions the effectiveness of AI in organizational decision-making.

Information security maturity shows a significant moderating effect on the relationship between digital trust and decision quality ($\beta = 0.27$, $p < 0.01$). Organizations with higher levels of security maturity exhibit more stable and reliable outcomes of AI-driven decision processes, suggesting that security frameworks enhance the legitimacy and controllability of AI-mediated knowledge systems.

To examine cross-level effects, a hierarchical linear modeling (HLM) approach was applied. The data structure consisted of three levels: individual-level perceptions (Level 1), team-level aggregation within top management teams (Level 2), and organizational-level characteristics (Level 3). The results indicate that AI-mediated knowledge practices significantly influence epistemic authority at the individual level ($\beta = 0.48$, $p < 0.001$), while at the team level they affect knowledge validation processes ($\beta = 0.41$, $p < 0.01$). At the organizational level, AI adoption is associated with increased governance complexity ($\beta = 0.36$, $p < 0.05$).

Descriptive statistics further support these findings. A majority of respondents (68%) indicate moderate to high reliance on AI-generated knowledge in decision-making processes, while 57% report concerns regarding the transparency and interpretability of AI outputs. Additionally, 61% of firms assess their information security maturity as medium, suggesting that many organizations are still in the process of adapting their security frameworks to AI-driven environments.

Overall, the results confirm that generative artificial intelligence significantly reconfigures knowledge governance by reshaping trust dynamics, decision processes, and epistemic structures across multiple organizational levels.

Table 1: Descriptive statistics and reliability

Construct	Mean	SD	Cronbach's α
AI-mediated knowledge practices	3.87	0.74	0.89
Digital trust	3.65	0.81	0.91
Information security maturity	3.54	0.77	0.88
Decision quality	3.92	0.69	0.90
Epistemic authority (individual level)	3.71	0.73	0.86
Team knowledge validation	3.68	0.76	0.87
Organizational governance complexity	3.59	0.71	0.85

The descriptive statistics presented in Table 1 indicate that all examined constructs exhibit moderate to high mean values, suggesting a relatively advanced adoption of AI-mediated knowledge practices and associated governance mechanisms within the analyzed organizations. The reliability coefficients (Cronbach's α) exceed the recommended threshold of 0.70, confirming the internal consistency of the measurement scales and supporting the validity of further analysis.

These results provide a solid empirical foundation for examining the relationships between constructs. To further explore the strength and direction of associations between variables, a correlation analysis was conducted.

Table 2: Correlation matrix

Variable	1	2	3	4
1. AI practices	1.00			
2. Digital trust	0.62***	1.00		
3. Info security maturity	0.48***	0.55***	1.00	
4. Decision quality	0.51***	0.54***	0.49***	1.00

The correlation matrix presented in Table 2 reveals statistically significant and positive relationships between all key variables. In particular, AI-mediated knowledge practices show a strong correlation with digital trust ($r = 0.62$, $p < 0.001$), indicating that increased reliance on generative AI is associated with higher levels of trust in algorithmically generated knowledge. Similarly, digital trust demonstrates a strong correlation with decision quality ($r = 0.54$, $p < 0.001$), highlighting its central role in shaping effective decision-making processes.

While correlation analysis confirms the existence of significant relationships, it does not provide insights into causality or the structural dependencies between variables. Therefore, structural equation modeling (SEM) was applied to test the proposed research model and examine both direct and indirect effects.

Table 3: Structural model results (SEM)

Path	β	t-value	p-value
AI practices → Digital trust	0.62	9.87	<0.001
Digital trust → Decision quality	0.54	8.94	<0.001
AI practices → Decision quality (direct)	0.21	3.12	<0.01
Info security → Decision quality	0.33	5.21	<0.001
Interaction (Trust × Security) → Decision quality	0.27	2.98	<0.01

Indirect effect = 0.33 ($p < 0.001$)

The results of the structural equation modeling presented in Table 3 provide strong support for the hypothesized relationships. AI-mediated knowledge practices have a significant positive effect on digital trust ($\beta = 0.62$, $p < 0.001$), confirming that the use of generative AI strengthens managerial confidence in algorithmically generated knowledge. Digital trust, in turn, significantly influences decision quality ($\beta = 0.54$, $p < 0.001$), validating its role as a key mediating construct.

The direct effect of AI practices on decision quality remains significant but weaker ($\beta = 0.21$, $p < 0.01$), indicating partial mediation. Furthermore, information security maturity exerts both a direct effect and a moderating influence on decision quality, reinforcing its role as a stabilizing factor within the emerging knowledge governance regime.

To provide a clearer visualization of these relationships and the overall structure of the model, Figure 3 presents the structural equation model with standardized path coefficients.

Figure 3 presents the structural equation model and confirms the validity of the proposed relationships between AI-mediated knowledge practices, digital trust, information security maturity, and decision quality. The model provides empirical support for the argument that generative artificial intelligence should be understood not merely as a technological instrument, but as an emerging mechanism of knowledge governance that reconfigures epistemic processes within organizations.

The strongest path identified in the model is the relationship between AI-mediated knowledge practices and digital trust ($\beta = 0.62$, $p < 0.001$). The second key relationship, between digital trust and decision quality ($\beta = 0.54$, $p < 0.001$), further reinforces the central role of trust in AI-mediated governance systems. This coefficient shows that trust significantly determines whether AI-generated outputs are incorporated into managerial reasoning in ways that improve strategic and operational decision-making. The result suggests that organizations do not benefit from generative AI simply because the technology is available; rather, the positive effects of AI on decision processes depend on whether managers regard its outputs as credible, intelligible, and sufficiently

reliable to enter the domain of organizational judgment. This is highly relevant for contemporary organizations, where decisions are increasingly informed by synthetic, predictive, and generative forms of knowledge that cannot always be fully verified in real time.

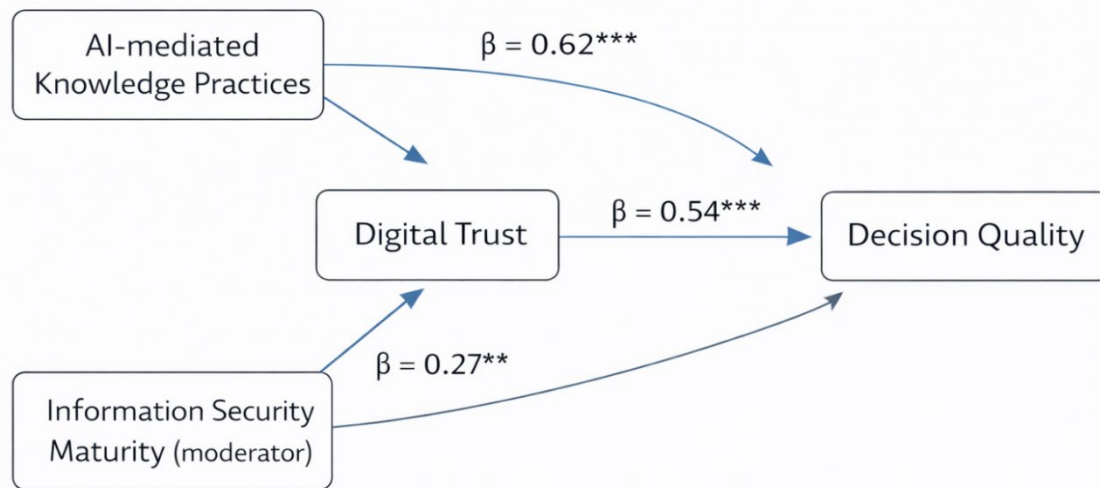


Figure 3: Structural Equation Model

The model also reveals a direct effect of AI-mediated knowledge practices on decision quality ($\beta = 0.21$, $p < 0.01$), although this relationship is weaker than the indirect path through digital trust. This finding indicates partial mediation and confirms that generative AI influences decision quality in two ways. First, it directly supports managerial processes by accelerating access to information, broadening the cognitive scope of decision-makers, and enabling faster synthesis of complex inputs. Second, and more importantly, it affects decisions indirectly by shaping the degree of trust managers place in algorithmically generated knowledge. The relative weakness of the direct effect compared with the indirect one highlights an essential theoretical point: the organizational consequences of generative AI are not determined solely by functional efficiency, but by interpretive and governance conditions that mediate how AI outputs are accepted, contested, or ignored.

A further important result concerns the role of information security maturity, which exerts a significant moderating effect on the relationship between digital trust and decision quality ($\beta = 0.27$, $p < 0.01$). This finding demonstrates that information security is not merely a technical background condition, but an active stabilizer of the emerging regime of AI-based knowledge governance. In organizations with higher information security maturity, trust in AI-generated knowledge is more likely to translate into effective decisions because the broader governance environment provides mechanisms of control, traceability, and risk limitation. By contrast, in low-maturity environments, even relatively high trust may not result in robust decision outcomes because algorithmically generated knowledge remains vulnerable to manipulation, leakage, distortion, or misinterpretation. Thus, information security maturity enhances the legitimacy and operational reliability of AI-mediated cognition by embedding it within structures of accountability and control.

Taken together, the structural model supports the broader argument of the article that generative artificial intelligence reconfigures knowledge governance across organizational levels. At the individual level, the model implies a transformation of managerial cognition, as executives increasingly rely on non-human systems to frame problems, generate alternatives, and support judgment. At the team level, the significance of digital trust suggests that collective acceptance of AI outputs becomes a condition for shared sensemaking and coordinated action. At the organizational level, the moderating role of information security maturity confirms that the governance effects of generative AI are contingent upon formal infrastructures capable of regulating epistemic risk. In this sense, the model not only explains decision quality but also reveals the institutional conditions under which generative AI can become a legitimate and resilient component of organizational knowledge systems.

The findings also carry important theoretical implications. First, they support the view that generative AI should be conceptualized as an epistemic actor rather than as a neutral support tool. The significant paths in the model indicate that AI participates in the production of organizationally relevant knowledge and shapes the conditions

under which that knowledge is trusted and operationalized. Second, the model expands existing knowledge governance theory by demonstrating that trust and security are not peripheral concerns but constitutive dimensions of algorithmically mediated knowledge systems. Third, the partial mediation observed in the model suggests that the governance of generative AI requires attention not only to performance outcomes, but also to the socio-cognitive mechanisms through which AI outputs gain epistemic legitimacy.

From a managerial perspective, the results underscore that successful implementation of generative AI requires more than technological deployment. Organizations need to cultivate digital trust through transparency, explainability, and consistent interaction with AI systems, while simultaneously strengthening information security maturity to ensure integrity, controllability, and resilience. Without these complementary governance mechanisms, AI adoption may intensify epistemic uncertainty rather than reduce it. Managers may either over-rely on synthetic outputs without adequate control or reject potentially valuable AI-generated knowledge due to mistrust and perceived risk. Both scenarios weaken the capacity of organizations to leverage generative AI as a productive governance mechanism.

In summary, Figure 3 provides strong empirical evidence for the proposed model and demonstrates that the relationship between generative AI and decision quality is neither simple nor purely technological. It is shaped by the interplay between AI-mediated knowledge practices, digital trust, and information security maturity. This configuration confirms that generative artificial intelligence constitutes a new regime of knowledge governance—one that transforms how knowledge is produced, validated, and used in organizations, while simultaneously generating new demands for trust, security, and institutional control.

4. Discussion and Conclusions

The findings support the view that generative artificial intelligence should be understood not only as a technological tool, but as an epistemic actor within knowledge governance systems. This extends knowledge management theory by showing that organizational knowledge is increasingly shaped through interaction between human decision-makers and algorithmic systems (Salah and Ayyash 2024). A key theoretical contribution of this study is the identification of digital trust as a mediating mechanism between AI-mediated knowledge practices and decision quality. Trust is therefore not only a matter of user acceptance, but a condition that determines whether AI-generated knowledge becomes part of organizational reasoning. The study also shows that information security maturity plays a governance role. It supports the reliability, traceability, and controllability of AI-mediated knowledge, and should therefore be treated as part of knowledge governance rather than as a purely technical function (Mantulenko et al. 2024). From a practical perspective, organizations implementing generative AI should focus on three areas. First, they should strengthen explainability so that managers can understand and evaluate AI-generated outputs. Second, they should develop information security maturity through clear procedures for data protection, access control, and system monitoring. Third, they should manage dependency on AI by maintaining human oversight and establishing procedures for validating AI recommendations.

The study has several limitations. Its cross-sectional design does not capture how trust and governance mechanisms evolve over time. In addition, the focus on firms from Poland, Germany, and Spain may limit the generalizability of the findings to other institutional contexts. Future research should use longitudinal designs, include broader geographical samples, and further examine how human and algorithmic cognition interact in organizational decision-making (Tarasova 2024; Steiber and Alvarez 2024).

In conclusion, the study shows that the effectiveness of generative AI depends not only on technological adoption, but also on governance conditions. Digital trust and information security maturity are central mechanisms through which AI-generated knowledge becomes usable, credible, and controllable in organizational decision-making.

Ethics Declaration: Ethics approval was not required.

AI Declaration: AI tools were not used to create this article.

References

- Alavi, M. and Leidner, D.E. (2001), Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues, *MIS Quarterly* 25: 107.
- Almustafa, H. and Kalash, I. (2025), The dynamic relationship between firms' cash reserves and financial leverage: evidence from MENA emerging markets, *JEAS* 41: 414–431.

- Bresciani, S., Ciampi, F., Meli, F. and Ferraris, A. (2021), Using big data for co-innovation processes: Mapping the field of data-driven innovation, proposing theoretical developments and providing a research agenda, *International Journal of Information Management* 60: 102347.
- Huda, N.U., Ahmed, I., Adnan, M., Ali, M. and Naeem, F. (2024), Experts and intelligent systems for smart homes' Transformation to Sustainable Smart Cities: A comprehensive review, *Expert Systems with Applications* 238: 122380.
- Hussain, I., Qureshi, M., Ismail, M., Iftikhar, H., Żywiłek, J. and López-Gonzales, J.L. (2024), Optimal features selection in the high dimensional data based on robust technique: Application to different health database, *Heliyon* 10: e37241.
- Khan, M.A., Ali, L., Hussain, S., Ullah, F., Żywiłek, J. and Khan, M.A. (2026), Edge computing: architecture and security. In *Edge Intelligence*, Elsevier, pp. 57–78.
- Mantulenko, V.V., Horák, J. and Kučera, J. (Eds.) (2024), *Proceedings of the XI International Scientific Conference "Digital Transformation of the Economy: Challenges, Trends and New Opportunities" (ISCDTE 2024), Lecture Notes in Networks and Systems*, Vol. 1064, Springer Nature Switzerland, Cham.
- Modgil, S., Singh, R.K., Mathiyazhagan, K. and Żywiłek, J. (2026), Role of generative AI towards sustainable procurement, *IJLM* 37: 476–499.
- Salah, O.H. and Ayyash, M.M. (2024), Understanding user adoption of mobile wallet: extended TAM with knowledge sharing, perceived value, perceived privacy awareness and control, perceived security, *VJIKMS*.
- Steiber, A. and Alvarez, D. (2024), AI-driven digital business ecosystems: a study of Haier's EMCs, *EJIM*.
- Tarasova, T.M. (2024), Protection of Trade Secrets to Ensure the Economic Security of the Enterprise. In Mantulenko, V.V., Horák, J. and Kučera, J. (Eds.), *Proceedings of the XI International Scientific Conference "Digital Transformation of the Economy: Challenges, Trends and New Opportunities" (ISCDTE 2024), Lecture Notes in Networks and Systems*, Vol. 1064, Springer Nature Switzerland, Cham, pp. 95–102.
- Tsai, C., Zdravkovic, J. and Stirna, J. (2022), Modeling Digital Business Ecosystems: A Systematic Literature Review, *J. Complex Syst. Inform. Model. Q.*: 1–30.
- Żywiłek, J., Mathiyazhagan, K., Shahzad, U., Zhao, X. and Saikouk, T. (2025a), Enhancing cognitive metrics in supply chain management through information and knowledge exchange, *IJLM*.
- Żywiłek, J., Matulewski, M. and Frąś, J. (2025b), AI as a shield against cyberattacks - employee awareness in the EU, *Procedia Computer Science* 270: 5510–5519.
- Żywiłek, J., Szymonik, A. and Smal, T. (2025c), *Navigating Supply Chain Turbulence*, Productivity Press, New York