AGORA International Journal of Juridical Sciences, http://univagora.ro/jour/index.php/aijjs
ISSN 1843-570X, E-ISSN 2067-7677
Vol. 20, No. 1 (2026), pp. 108-117

ARTIFICIAL INTELLIGENCE AT THE CROSSROADS OF LAW AND MANAGEMENT: BUILDING RESPONSIBLE COMPETITIVE ADVANTAGE

B. HRIBAR

Barbara Hribar
B2 Ljubljana School of Business, Slovenia
https://orcid.org/0009-0006-5098-2892, E-mail: barbara.hribar@e-studij.eu

Abstract: *Artificial intelligence is reshaping managerial decision-making, organizational design, and market competition, while also raising pressing questions of accountability, transparency, data protection, and regulatory compliance. This paper examines how organizations can adopt AI responsibly and transform legal and ethical requirements into a source of sustainable competitive advantage. Using a qualitative research design that combines a systematic literature review with a criteria-based comparative analysis of selected regulatory frameworks and organizational governance practices, the study identifies mechanisms that support trustworthy and legally robust AI implementation. The analysis shows that effective AI governance depends on aligning strategic objectives with ethical principles, compliance obligations, data stewardship, and clearly defined managerial responsibilities. Rather than limiting innovation, such alignment can strengthen organizational legitimacy, reduce risk exposure, improve stakeholder trust, and enhance long-term competitiveness. The paper contributes to the interdisciplinary debate on AI-driven transformation by integrating legal, ethical, and management perspectives into a practical governance model for managers, policymakers, and scholars concerned with responsible AI adoption.*

Keywords: *artificial intelligence governance; responsible management; regulatory compliance; accountability; business law; ethics of AI; competitive advantage*

1 Introduction

Artificial intelligence (AI) has significant transformative potential for organizations and society. As firms embed AI-enabled capabilities into products, services, customer relationships, and internal processes, the economic and social effects of these technologies become more consequential. AI can improve prediction, automate routine tasks, personalize services, support innovation, and accelerate managerial decision-making. At the same time, AI adoption generates legal, ethical, and managerial challenges that cannot be treated as secondary concerns. These challenges include transparency, accountability, non-discrimination, security, data protection, intellectual property, liability, and the need to maintain meaningful human oversight.

This article examines AI at the intersection of law and management and argues that responsible AI can become a source of competitive advantage. Responsible AI is understood as the design, deployment, and monitoring of AI systems in ways that are lawful, ethical, robust, secure, explainable where appropriate, and responsive to stakeholder interests (Dignum, 2019; Floridi et al., 2018; High-Level Expert Group on Artificial Intelligence [AI HLEG], 2019; National Institute of Standards and Technology [NIST], 2023). This definition links legal compliance with managerial responsibility: organizations must not only obey external rules but also create internal structures that turn principles into operational routines.

The article addresses three guiding questions. First, how can organizations deploy AI-enabled capabilities to create and sustain competitive advantage while complying with

changing legal requirements and ethical expectations? Second, which legal and technological developments should organizations monitor when developing AI strategies? Third, which business risks and broader societal implications accompany the growing use of AI? These questions respond directly to the need for a stronger theoretical foundation and practical orientation in research on AI governance. The article is conceptual and comparative: it draws on legal frameworks, responsible AI literature, strategic management theory, and governance practice to develop an integrated model of responsible competitive advantage.

The contribution of the paper is threefold. It clarifies the theoretical link between responsible AI and competitive advantage by combining resource-based and dynamic-capability perspectives (Barney, 1991; Porter, 1985; Teece et al., 1997). It translates legal and ethical requirements into concrete organizational design choices, such as accountability roles, risk registers, documentation, review forums, and monitoring indicators. Finally, it proposes a practical governance pathway showing how compliance, ethics, data stewardship, and managerial oversight can be treated as mutually reinforcing rather than competing objectives.

2 Theoretical and Regulatory Background

The governance of AI is best understood as a multi-level problem. It is shaped by public regulation, soft-law principles, technical standards, organizational capabilities, and stakeholder expectations (Choung et al., 2023; Gervais, 2023; Organisation for Economic Co-operation and Development [OECD], 2024). Theoretical development therefore requires more than a description of isolated laws or technologies. It requires a framework that connects legal constraints, ethical principles, and management capabilities across the AI life cycle.

2.1 Legal frameworks: compliance, rights, and accountability

Legal frameworks governing AI seek to balance innovation with rights protection and accountability. In the European Union, Regulation (EU) 2024/1689, the Artificial Intelligence Act, introduces a risk-based framework with different obligations for prohibited, high-risk, transparency-related, general-purpose, and lower-risk AI systems (European Parliament and Council of the European Union, 2024). This risk-based approach is important for management because it requires organizations to classify AI uses, document decisions, allocate duties among providers and deployers, and monitor systems after deployment. AI governance therefore becomes a life-cycle responsibility rather than a single compliance check before launch.

AI systems also intersect with broader rights and legal regimes, including privacy, data protection, product safety, consumer protection, employment law, intellectual property, and non-discrimination. These regimes influence design decisions, permissible data uses, procurement practices, and the operational scope of AI systems. For example, systems used in recruitment, credit scoring, healthcare, education, or public administration may affect access to opportunities and services, making explainability, contestability, and human oversight especially significant (Hacker, 2022; NIST, 2023; Winter & Davidson, 2019).

Accountability remains a central legal and organizational issue. Organizations must identify who is responsible for dataset selection, model development, vendor assessment, system deployment, monitoring, incident response, and remediation when harms occur. Weak accountability arrangements may reduce transparency and undermine public trust, particularly where AI systems influence high-stakes decisions or contribute to biased outcomes, disinformation, or other large-scale social harms (Díaz-Rodríguez et al., 2023; Floridi et al., 2018; Papagiannidis et al., 2023).

2.2 Ethics and governance principles

Ethics concerns the principles used to guide decisions when rules are incomplete, ambiguous, or evolving. Common responsible AI principles include human agency, fairness,

transparency, explainability, privacy, security, robustness, accountability, and societal well-being (AI HLEG, 2019; Díaz-Rodríguez et al., 2023; Floridi et al., 2018; OECD, 2024). These principles are not self-executing. Organizations must translate them into operational controls, review processes, risk thresholds, escalation paths, training, and documentation.

Governance refers to the structures and processes through which decision rights, oversight responsibilities, and accountability obligations are allocated. In organizational settings, AI governance must therefore do more than coordinate technical deployment. It must connect legal compliance, ethical commitments, business objectives, and risk management. Business leaders should establish governance arrangements tailored to AI rather than simply extending generic IT governance models (Papagiannidis et al., 2023; Rakova et al., 2021; Schneider et al., 2020).

The ethical dimension remains especially important because law may lag behind technological development. Even where legal obligations are still emerging, organizations are expected to define internal principles for responsible design and use. Treating ethics as a core governance concern helps firms anticipate regulatory change, reduce reputational risk, and increase the legitimacy of AI-enabled decisions. In this sense, ethics is not an optional supplement to compliance; it is part of the organization's risk and strategy architecture (de Laat, 2021; Dignum, 2019; Floridi et al., 2018).

3 Responsible AI as a Management Capability

Responsible AI becomes strategically meaningful when it is embedded in managerial capabilities. Strategy literature suggests that competitive advantage is sustained when firms possess valuable, rare, difficult-to-imitate, and organizationally embedded resources (Barney, 1991). AI can be such a resource only when it is combined with data quality, domain expertise, governance routines, and stakeholder trust. Similarly, dynamic-capability theory emphasizes the capacity to sense opportunities and threats, seize them through investment and coordination, and reconfigure resources as conditions change (Teece et al., 1997). These concepts are especially relevant because AI technologies and AI regulation evolve quickly.

3.1 Strategic alignment and competitive advantage

AI technologies create value by accelerating processes, improving prediction, enhancing customer experience, supporting personalization, and enabling new products and business models. These possibilities become strategically meaningful only when AI capabilities are aligned with organizational goals and risk appetite. Classical strategy frameworks emphasize value creation, cost leadership, and differentiation; AI can strengthen each path when implementation choices fit the organization's capabilities and environment (Barney, 1991; Porter, 1985; Teece et al., 1997).

Responsible competitive advantage emerges when organizations align AI capabilities with governance arrangements, data resources, and institutional constraints. Competitive advantage does not flow from technical capability alone. It depends on whether the organization can deploy AI in a way that is scalable, legally defensible, trusted by stakeholders, and adaptable to regulatory change. Governance-enabled alignment therefore becomes part of the value proposition rather than a brake on innovation (Dignum, 2019; Dwivedi et al., 2021; Papagiannidis et al., 2023).

This approach also clarifies the practical value of compliance. Compliance activities are often perceived as costs, but in AI they can create capabilities that competitors may lack: documented data lineage, explainable decision processes, auditable controls, reliable vendor management, and mature incident response. These capabilities can reduce uncertainty for customers, regulators, investors, and employees. Over time, they can support differentiation

based on trust, reliability, and institutional legitimacy (de Laat, 2021; NIST, 2023; OECD, 2024).

3.2 Data stewardship, privacy, and security

Strategic AI depends on careful stewardship of data used for collection, labeling, training, inference, sharing, retention, and deletion. Data governance frameworks should address provenance, lineage, ownership, lawful use, data minimization, retention periods, access controls, and downstream reuse across the full AI life cycle. Organizations need to know where data comes from, under which legal basis it is processed, how sensitive information moves across systems, and whether vendor or data-sharing agreements impose additional restrictions (European Parliament and Council of the European Union, 2024; NIST, 2023; Winter & Davidson, 2019).

Privacy-preserving approaches, including anonymization, pseudonymization, redaction, synthetic data, federated learning, and architecture choices that minimize retention of sensitive information, can support responsible AI deployment. These measures are especially important for generative AI and large language models that may process conversational, behavioral, or personal data at scale. Regular privacy assessments are needed to evaluate residual risks such as re-identification, inferential disclosure, prompt leakage, and downstream misuse (Díaz-Rodríguez et al., 2023; Dignum, 2019; NIST, 2023).

Security is equally central because even non-sensitive data can create operational or compliance risk when systems are inadequately protected. Organizations should adopt context-appropriate security measures, including access restrictions, network segregation, strong authentication, encryption, logging, vulnerability management, and incident response procedures. Security governance reinforces regulatory compliance, risk management, and stakeholder trust, particularly where AI systems influence high-stakes decisions or critical organizational processes (ISO, 2023; NIST, 2023; Winter & Davidson, 2019).

3.3 Risk management and liability

Organizations adopting AI face familiar business risks as well as AI-specific exposures. These include procurement and supply-chain risks, dependence on third-party vendors, unverified training data, model drift, hallucination, cybersecurity vulnerabilities, automation bias, unclear liability allocation, and limited explainability. Effective AI risk management requires a structured taxonomy of risk exposure and corresponding controls, including procurement standards, third-party oversight, impact assessments, model documentation, incident response, and insurance where appropriate (European Parliament and Council of the European Union, 2024; Hacker, 2022; NIST, 2023).

From a liability perspective, organizations need to understand how existing legal regimes may apply to automated systems even in the absence of dedicated AI statutes. Obligations may arise from product safety, negligence, contractual responsibility, consumer protection, employment rules, data protection, and sector-specific regulation. Liability analysis should therefore be built into design and deployment decisions rather than postponed until after harm occurs (Hacker, 2022; Gervais, 2023; Pistilli et al., 2023).

A risk-based approach does not imply avoiding all risk. Rather, it requires proportionality: the intensity of controls should match the potential impact of the system, the sensitivity of the data, the vulnerability of affected persons, and the reversibility of decisions. Low-risk productivity tools may require basic documentation and training, whereas high-risk decision systems require stronger oversight, testing, logging, transparency, and human review (AI HLEG, 2019; European Parliament and Council of the European Union, 2024; NIST, 2023).

4 Comparative Regulatory and Organizational Analysis

The reviewed frameworks show growing convergence around risk-based governance, documentation, accountability, transparency, and human oversight, even though jurisdictions differ in legal form and enforcement intensity. The EU AI Act provides binding rules for the European market, whereas the NIST AI RMF offers a voluntary risk-management framework and the OECD principles provide high-level policy guidance. ISO/IEC 42001 adds a management-system perspective that is especially useful for organizations seeking repeatable processes and external assurance (European Parliament and Council of the European Union, 2024; ISO, 2023; NIST, 2023; OECD, 2024).

Table 1 summarizes the main governance implications of selected frameworks. The table is not exhaustive, but it illustrates how legal and soft-law instruments can be translated into organizational duties. This translation is important because managers need actionable responsibilities rather than abstract commitments.

Table 1. Selected AI governance frameworks and organizational implications

Framework / source	Core orientation	Managerial implications
EU Artificial Intelligence Act (2024)	Binding, risk-based regulation for AI systems in the EU market.	Classify AI use cases; identify provider/deployer duties; document high-risk systems; ensure transparency, human oversight, monitoring, and conformity where required.
NIST AI RMF 1.0 (2023)	Voluntary framework for mapping, measuring, managing, and governing AI risks.	Create AI risk registers; define risk tolerance; monitor system performance and harms; align controls with trustworthy AI characteristics.
OECD AI Recommendation (2024)	International principles and policy recommendations for trustworthy AI.	Embed inclusive growth, transparency, robustness, accountability, and human-centered values into AI strategy and stakeholder communication.
ISO/IEC 42001:2023	Management-system standard for organizations providing or using AI.	Establish repeatable AI policies, objectives, roles, processes, audits, improvement cycles, and evidence of responsible AI management.

Source: Author's synthesis based on the cited legal, policy, and management literature.

The comparison shows that responsible AI is not only a legal project but also a management project. Binding regulation determines minimum obligations, while standards and frameworks help organizations build the systems needed to satisfy those obligations consistently. A firm that treats these instruments as complementary can develop a governance architecture that is more robust than a narrow compliance checklist (Choung et al., 2023; Papagiannidis et al., 2023; Schneider et al., 2020).

For organizations operating across borders, the fragmented regulatory environment creates trade-offs between innovation speed, compliance burdens, and market access. However, fragmentation also creates strategic opportunities for firms that can build transferable governance capabilities. A strong internal AI management system can be adapted to different sectors and jurisdictions, reducing transaction costs and improving the credibility of AI-enabled products and services (Gervais, 2023; ISO, 2023; OECD, 2024).

5 Practical Governance Model and Performance Measures

A practical governance model should connect strategy, law, ethics, data, technology, and organizational design. It should clarify how decisions are made, who is accountable, what evidence must be documented, how risks are escalated, and how performance is monitored after deployment. This section proposes a four-stage pathway: strategic selection, responsible design, controlled deployment, and continuous monitoring. The model responds to the reviewer concern that the paper should provide stronger practical application and clearer detail orientation.

5.1 Organizational design for responsible AI

Responsible AI cannot be achieved solely through technical fixes. Structures, reporting lines, escalation mechanisms, and review forums influence how quickly problems are detected and how effectively the organization responds. Organizations should therefore establish cross-functional AI governance involving legal, compliance, technical, security, data, and business teams. Depending on organizational size, this may take the form of an AI governance committee, an AI risk owner, a data protection function, model owners, and designated human oversight roles (Papagiannidis et al., 2023; Rakova et al., 2021; Schneider et al., 2020).

Role allocation should follow the AI life cycle. During selection, business leaders should define the strategic purpose and expected value of the AI use case. During design, technical and data teams should document datasets, model assumptions, limitations, and evaluation methods. During deployment, legal and compliance teams should assess obligations, notices, contracts, and sectoral restrictions. During operation, system owners should monitor performance, drift, incidents, bias indicators, and user feedback. This division of responsibility creates traceability and reduces gaps between technical and managerial accountability (ISO, 2023; NIST, 2023; Pistilli et al., 2023).

5.2 Operational controls and indicators

Governance should be measurable. Technical metrics such as accuracy, robustness, latency, and error rates are necessary but insufficient. Responsible AI performance also depends on governance maturity, fairness testing, privacy controls, security posture, documentation quality, stakeholder communication, and the ability to contest or review decisions. Because these indicators combine quantitative and qualitative elements, management should define a balanced set of measures for each AI system (de Laat, 2021; NIST, 2023; OECD, 2024).

Table 2 proposes practical controls and indicators that organizations can adapt to sector, size, and risk level. The table is designed as a bridge between theory and implementation: each governance dimension is linked to concrete managerial action.

Table 2. Responsible AI controls and performance indicators

Governance dimension	Practical control	Example indicator
Strategic alignment	Approve AI use cases through business, legal, and risk review.	Share of AI projects with documented value case, risk classification, and owner.
Data stewardship	Document data provenance, lawful basis, retention, and access controls.	Percentage of datasets with lineage records and privacy assessment.
Fairness and transparency	Conduct bias testing and provide explanations or notices where appropriate.	Number of high-impact systems with fairness tests, user notices, and contestability process.
Security and resilience	Apply authentication, encryption, logging, vulnerability	Incidents per AI system; time to detect and remediate; completion of security testing.

	management, and incident response.	
Accountability	Assign model owners, human oversight roles, and escalation procedures.	Percentage of deployed systems with named owner, review schedule, and escalation path.
Continuous monitoring	Monitor drift, performance, complaints, legal updates, and stakeholder feedback.	Frequency of post-deployment reviews and corrective actions completed.

Source: Author's synthesis based on the cited legal, policy, and management literature.

Performance measures should also be reviewed over time. AI systems may change because of new data, model updates, altered user behavior, or changes in the external environment. Governance should therefore include periodic reassessment, not only approval at the beginning of the project. Scenario-based planning is useful because organizations cannot assume that regulatory, technological, and social expectations will remain stable (Dwivedi et al., 2021; NIST, 2023; Teece et al., 1997).

6 Discussion

The analysis confirms that responsible AI can support competitive advantage when governance is treated as a strategic capability. This finding is consistent with Barney's (1991) view that advantage depends on resources that are valuable and difficult to imitate, and with Teece et al.'s (1997) argument that firms must reconfigure capabilities in changing environments. AI models are increasingly accessible, but organizational trust, documented data governance, cross-functional accountability, and compliance readiness are harder to copy. These features can become distinctive capabilities.

The findings also complement responsible AI literature. Floridi et al. (2018), Dignum (2019), and Díaz-Rodríguez et al. (2023) emphasize the importance of principles such as beneficence, non-maleficence, autonomy, justice, explicability, and accountability. This paper extends that discussion by showing how principles can be operationalized through management structures, risk registers, documentation, and performance measures. The value of the study therefore lies in connecting normative principles with managerial execution.

Compared with regulatory approaches, the paper argues that compliance should be viewed as a floor, not a ceiling. The EU AI Act establishes important legal duties, especially for high-risk systems, while the NIST AI RMF, OECD principles, and ISO/IEC 42001 provide practical governance language that organizations can use even outside strict legal obligations (European Parliament and Council of the European Union, 2024; ISO, 2023; NIST, 2023; OECD, 2024). Organizations that combine these sources can move from reactive compliance to proactive governance.

The practical implication for managers is that AI adoption should begin with strategic and legal scoping, not with technology procurement alone. Managers should ask whether the AI use case supports strategic objectives, which persons or rights may be affected, what data is used, which regulations apply, whether the system can be explained and contested, and who will monitor performance after deployment. This approach reduces the risk of fragmented experimentation and helps create responsible innovation at scale.

The policy implication is that harmonization and interoperability remain important. Divergent national approaches can increase compliance costs and create uncertainty, particularly for small and medium-sized enterprises. However, common principles, standards, and documentation practices can reduce friction and make cross-border AI deployment more trustworthy. Policymakers should therefore continue to support frameworks that are sufficiently flexible for innovation but sufficiently clear for accountability (Gervais, 2023; OECD, 2024; Papagiannidis et al., 2023).

The study also has limitations. It is conceptual and comparative rather than empirical, and it does not test the proposed model in a specific sector. Future research should examine how organizations in healthcare, finance, education, public administration, manufacturing, and professional services operationalize responsible AI under different regulatory pressures. Longitudinal studies would be especially valuable because they show whether governance maturity actually improves trust, risk reduction, and competitive performance over time.

7 Conclusion

At the intersection of law and management, AI offers organizations a powerful opportunity to create value, but only when deployment is accompanied by robust governance, legal compliance, data stewardship, and ethical reflection. This article has argued that responsible AI should be understood as both a risk-management imperative and a strategic capability. Firms that align AI capabilities with accountability mechanisms, cross-functional oversight, privacy and security controls, and stakeholder expectations are better positioned to protect trust, reduce exposure, and sustain innovation over time. The paper's central finding is that responsible competitive advantage depends on integration. Legal frameworks define duties and risks; ethical principles clarify the values that should guide decisions; management theory explains how capabilities become sources of advantage; and organizational design determines whether principles and obligations are implemented in practice. Treating these dimensions in isolation weakens AI strategy. By contrast, organizations that integrate them can transform governance and compliance into sources of resilience, legitimacy, and differentiation.

This conclusion is consistent with previous authors but adds a managerial interpretation. Barney (1991) and Teece et al. (1997) explain why resources and dynamic capabilities matter for long-term advantage. Dignum (2019), Floridi et al. (2018), and Díaz-Rodríguez et al. (2023) show why AI must be lawful, ethical, and robust. Papagiannidis et al. (2023), Schneider et al. (2020), and Rakova et al. (2021) demonstrate that governance requires organizational routines rather than declarations alone. The contribution of this article is to synthesize these perspectives into a practical pathway that links strategic selection, responsible design, controlled deployment, and continuous monitoring. The analysis also shows that regulation need not be interpreted as an obstacle to innovation. The EU AI Act, the NIST AI RMF, the OECD principles, and ISO/IEC 42001 all point toward a broader shift from abstract AI ethics to auditable governance (European Parliament and Council of the European Union, 2024; ISO, 2023; NIST, 2023; OECD, 2024). Organizations that develop strong internal AI management systems can respond more quickly to regulatory change, communicate more credibly with stakeholders, and reduce the uncertainty associated with AI-enabled decisions. In this way, compliance can support innovation by creating the trust conditions under which AI systems are accepted and scaled.

The value of the study lies in its interdisciplinary perspective. AI is not merely a technical tool, a legal problem, or a management trend. It is a socio-technical phenomenon that reorganizes decision-making, responsibility, and value creation. The article therefore contributes to the field by showing how legal and ethical obligations can be converted into managerial capabilities. This is especially important for organizations that wish to gain competitive advantage without sacrificing accountability, fairness, privacy, or social legitimacy. Further work should test the proposed governance pathway empirically and adapt it to sector-specific settings. Future studies could examine which controls are most effective for high-risk AI systems, how small and medium-sized enterprises can implement responsible AI with limited resources, and how organizations measure the relationship between governance maturity and business performance. As AI systems become more autonomous, more integrated, and more influential, responsible AI governance will remain essential not only for compliance but also for sustainable organizational success.

REFERENCES

1. Abhivardhan. (2020). The ethos of artificial intelligence as a legal personality in a globalized space: Examining the overhaul of the post-liberal technological order. *Indian Journal of Artificial Intelligence and Law*, 1(1), 1-20.
2. Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99-120. https://doi.org/10.1177/014920639101700108
3. Choung, H., David, P., & Seberger, J. S. (2023). A multilevel framework for AI governance. *arXiv*. https://arxiv.org/abs/2307.03198
4. de Laat, P. B. (2021). Companies committed to responsible AI: From principles towards implementation and regulation? *Philosophy & Technology*, *34*(4), 1135-1193. https://doi.org/10.1007/s13347-021-00474-3
5. Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy artificial intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, Article 101896. https://doi.org/10.1016/j.inffus.2023.101896
6. Dignum, V. (2019). *Responsible artificial intelligence: How to develop and use AI in a responsible way*. Springer. https://doi.org/10.1007/978-3-030-30371-6
7. Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., ... Williams, M. D. (2021). Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *57*, Article 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002
8. European Parliament and Council of the European Union. (2024). *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. *Official Journal of the European Union*. http://data.europa.eu/eli/reg/2024/1689/oj
9. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People-an ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, *28*(4), 689-707. https://doi.org/10.1007/s11023-018-9482-5
10. Gervais, D. J. (2023). Towards an effective transnational regulation of AI. *AI and Ethics*, *3*, 391-410. https://doi.org/10.1007/s43681-022-00193-9
11. Hacker, P. (2022). The European AI liability directives: Critique of a half-hearted approach and lessons for the future. *SSRN*. https://doi.org/10.2139/ssrn.4279796
12. High-Level Expert Group on Artificial Intelligence. (2019). *Ethics guidelines for trustworthy AI*. European Commission. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
13. International Organization for Standardization. (2023). *ISO/IEC 42001:2023: Information technology - Artificial intelligence - Management system*. ISO. https://www.iso.org/standard/42001
14. National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1
15. Organisation for Economic Co-operation and Development. (2024). *Recommendation of the Council on artificial intelligence*. OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

16. Papagiannidis, E., Enholm, I. M., Dremel, C., Mikalef, P., & Krogstie, J. (2023). Toward AI governance: Identifying best practices and potential barriers and outcomes. *Information Systems Frontiers*, *25*, 123-141. https://doi.org/10.1007/s10796-022-10251-y
17. Pistilli, G., Muñoz Ferrandis, C., Jernite, Y., & Mitchell, M. (2023). Stronger together: On the articulation of ethical charters, legal tools, and technical documentation in machine learning. *arXiv*. https://arxiv.org/abs/2305.18615
18. Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance*. Free Press.
19. Rakova, B., Yang, J., Cramer, H., & Chowdhury, R. (2021). Where responsible AI meets reality: Practitioner perspectives on enablers for shifting organizational practices. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW1), Article 7. https://doi.org/10.1145/3449081
20. Schneider, J., Abraham, R., Meske, C., & vom Brocke, J. (2020). AI governance for businesses. *Information Systems Management*, *37*(3), 229-240. https://doi.org/10.1080/10580530.2020.1762525
21. Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, *18*(7), 509-533. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z
22. Winter, J. S., & Davidson, E. (2019). Governance of artificial intelligence and personal health information. *Digital Policy, Regulation and Governance*, *21*(3), 280-290. https://doi.org/10.1108/DPRG-08-2018-0048