EU Digital Strategy: Governance, Innovation and Business. Proceedings of the International Conference EU-PAIR 2025

DOI:10.47743/eu-pair.2025-1-22

ARTIFICIAL INTELLIGENCE AND DIGITAL GOVERNANCE: THE IMPACT OF EMERGING POLICIES ON BUSINESS TRANSFORMATION IN THE ERA OF BIG DATA AND MACHINE LEARNING

CARMEN TODERAȘCU
Alexandru Ioan Cuza University of Iasi
Iasi, România
carmentoderascu@gmail.com

IERONIM ȘTEFAN
Institute of Financial Studies
Doctoral School of Economy Eugeniu Carada
Bucharest, România
stefan.ieronim.georgian@gmail.com

Abstract
The accelerated digital transformation driven by Artificial Intelligence (AI), Big Data, and Machine Learning (ML) is fundamentally reshaping governance models and the dynamics of the business environment. This paper explores how emerging public policies, adopted at both European and international levels, influence decision-making processes, innovation capacity, and corporate competitiveness in the context of the new digital economy. Focusing on initiatives such as the EU Artificial Intelligence Act, the European Data Strategy, and digital ethics regulations, the study highlights their impact on organizational adaptability and sustainability. Using an interdisciplinary and practice-oriented approach, the research identifies both opportunities and challenges these policies pose for the private sector, especially regarding algorithmic accountability, data protection, and equitable access to technology. The findings offer policy recommendations for inclusive digital governance that supports innovation and business resilience within a regulated yet enabling framework.

Keywords: *digital governance; public policy; Artificial Intelligence; Big Data; Machine Learning; digital transformation; algorithmic ethics; business environment.*
JEL Classification: M21; G28; O33; O38.

1. INTRODUCTION

The digital economy experiences a complete transformation because businesses implement Artificial Intelligence (AI), Big Data, and Machine Learning (ML) systems to manage their operations (Yadav and Dwivedi, 2023). These technologies create operational performance improvements by developing new competitive benefits according to Allam and Rodwal (2023). Organizations that implement them need to manage an expanding number of intricate regulatory requirements. Businesses need to take a forward-thinking stance regarding public policy because technological progress creates essential challenges for businesses to follow governance and compliance rules (Davis, 2014). The EU Artificial Intelligence Act (European Commission, 2023) and European Data Strategy (European Commission, 2020) demonstrate how contemporary regulatory systems require powerful policy frameworks to handle various problems that these technologies create. These programs work to unite innovation goals with requirements for data protection, equal technology access, and responsible use of technology (Davis, 2014). The current regulatory framework creates both chances and difficulties for businesses, which need strategic handling to achieve sustainable development and business stability.

The complete effects of these policies need to be understood by corporate decision-makers, according to Burri and von Bothmer (2021). As organizations adapt to these regulatory changes, they must reevaluate their governance structures and operational strategies to align with new compliance requirements. This research examines how organizations can benefit from regulatory frameworks that support flexibility and tackles the multiple obstacles they encounter in their path. We investigate how new policies affect corporate governance and help businesses succeed during digital transformation. Organizations must adopt frameworks that support innovation development by implementing effective oversight of algorithmic decision systems and data protection protocols. Our research promotes public-private sector dialogue to establish digital governance systems that benefit business operations while protecting social interests. Our goal is to propose digital economy solutions for businesses to maintain their market position within modern technological business operations.

2. METHODOLOGY

We investigate how businesses rely on technologies such as Artificial Intelligence (AI), Big Data, and Machine Learning (ML) adapt to new public policies by conducting an extensive literature review. This review aims to merge research evidence with policy documents and theoretical frameworks to analyze digital governance's impact on corporate strategic planning in contemporary business environments. The literature review evaluates present policies to determine major governance patterns and technological business operational developments in corporate governance.

The research started by conducting a thorough database search of Google Scholar, JSTOR, and Scopus to find peer-reviewed articles, white papers, and policy reports. We used "Artificial Intelligence Act," "European Data Strategy," "digital governance," "algorithmic accountability," and "business transformation" sources to gather comprehensive data about ongoing AI research. We utilized thematic analysis to organize its results and examine how regulations affect innovation potential and the difficulties of algorithmic accountability, data protection, and technology accessibility. The thematic structure enabled us to study how new policies affect corporate decision systems and operational approaches in detail.

The review used a critical evaluation method to combine multiple perspectives from the literature base for an objective assessment. The evaluation process required assessment of some research findings, which demonstrated positive effects of regulatory frameworks, together with studies that exposed adverse effects and constraints these policies create for businesses. The research combines these viewpoints to develop a complete understanding of regulatory system operations through two distinct mechanisms.

3. THE IMPACT OF EMERGING POLICIES ON INNOVATION CAPACITY

The assessment of new policies and innovation capacity has become crucial because governments and regulatory organizations across the world must manage rapid technological progress while maintaining ethical standards and safeguarding public safety. The EU Artificial Intelligence Act and European Data Strategy demonstrate how regulatory frameworks affect the development of innovation.

The European Commission introduced the EU Artificial Intelligence Act to create a complete set of rules for AI system development. The Act establishes a risk-based framework for AI systems through categories, starting from minimal up to unacceptable, to enforce strict transparency, safety, and accountability standards for high-risk applications (“EU’s AI Act Proposal Foregrounds Risks and Rights,” 2023). The regulatory framework produces various advantages and challenges that affect innovation capacity development. On one hand, the development of AI systems receives more funding because organizations establish specific guidelines that create trust in AI systems. On the other hand, the implementation of excessive regulations restricts innovation by limiting creative freedom and creating obstacles for new businesses and small organizations to handle intricate legal frameworks (Li *et al.,* 2018). The European Data Strategy supports data sharing and interoperability as key factors to boost digital economy innovation, according to Custers and Bachlechner (2017). It aims to create data governance systems and open data programs, which will establish an environment that supports data-driven innovation. The policy framework enables businesses to develop new products and services through shared data resource utilization, which drives up their innovation capacity. Data sharing systems need privacy and security solutions to overcome current obstacles that threaten future technological development.

Intellectual Property (IP) policies act as fundamental drivers that establish the level of innovation capacity. Strong IP protection can incentivize innovation by ensuring that creators and inventors can reap the financial rewards of their efforts. The implementation of overly restrictive IP laws, however, leads to monopolistic conduct, which prevents market competition and restricts innovation (Sherwood, 1990). The present need for IP policy reform in AI technology development requires policymakers to create an equilibrium between fostering innovation and protecting legal rights (Chesterman, 2025).

Also, national policies that match international standards serve as a crucial factor for obtaining a competitive advantage within the current global economic framework. The implementation of different regulatory frameworks by nations leads to obstacles that prevent international cooperation between businesses and technological advancement. For example, regulatory systems of AI between the EU, the United States, and China create barriers for innovators who want to enter foreign markets, according to Savage (2020). The development of policies requires an assessment of their effects on home-based innovation and their effects on global market position.

New policy development shows that society now understands the ethical implications of technology better. The integration of ethical considerations into policy frameworks – such as those outlined in the EU's Ethics Guidelines for Trustworthy AI – can enhance innovation capacity by ensuring that technological advancements align with societal values and public interest (Green and Clayton, 2021). The method supports sustainable development through its requirement for new technologies to deliver economic value and social advantages.

4. CHALLENGES OF ALGORITHMIC ACCOUNTABILITY AND DATA PROTECTION

As organizations increasingly integrate Artificial Intelligence (AI) and Machine Learning (ML) into their operations, the challenges surrounding algorithmic accountability and data protection have emerged as critical concerns. The complicated nature of these technologies makes it difficult to understand the decision-making processes, which leads to multiple ethical, legal, and operational issues.

The main challenge to achieving algorithmic accountability arises because many AI systems function through unexplained internal processes. The decision-making operations of deep learning models, together with other machine learning models, remain unclear because their functioning operates as a "black box" (Coyle and Weller, 2020). Organizations struggle to verify accountability because algorithmic decision systems produce unexplained results, which makes it impossible for them to understand their decision-making logic. They encounter problems with their AI systems because they fail to detect the root causes of discriminatory hiring practices, medical misdiagnoses, and unfair lending decisions (Coyle and Weller, 2020). The lack of transparency in AI systems leads to stakeholder distrust because users, including customers and employees, and regulators cannot follow the automated decision-making process (Dinka *et al.*, 2006).

Organizations must address algorithmic bias as one of their main technology problems (Mone, 2016). AI systems learn from historical data that includes biases that stem from social inequalities in society. The absence of bias mitigation systems allows these prejudices to continue and possibly become more severe in employment, financial, and criminal justice systems (Ntoutsi *et al.*, 2020). The technology receives criticism because, for example, facial recognition systems produce more identification errors for people with darker skin tones, which results in discriminatory results (Drozdowski *et al.*, 2020). Organizations face the dual challenge of recognizing and mitigating these biases within their algorithms while also navigating the legal and ethical implications of deploying biased systems. If algorithmic bias is ignored, companies will face major consequences such as damage to their reputation and legal risks under anti-discrimination laws (Ferrer *et al.*, 2021).

The process of collecting and processing large data sets needed for AI model training also creates major problems regarding data protection. Organizations must follow various regulatory requirements such as GDPR in Europe, which requires them to maintain strict data management practices (Li *et al.*, 2019). They must follow three essential principles to implement AI systems: they need to minimize data collection, define and limit specific purposes, and obtain user consent and they need to establish strong data governance systems that will defend their sensitive information from unauthorized access and data breaches. The situation becomes even more difficult because cyber threats have become more complex, which requires organizations to keep investing in cybersecurity protection systems to defend their data (Miryala and Gupta, 2022).

The process of establishing who should be held responsible for AI system decisions remains a difficult problem to solve. The responsibility for harmful algorithm outcomes remains unclear because it can fall on either the organization that created the algorithm, the data provider, or the AI system itself (Baldi and Oliveira, 2022). The lack of defined AI system boundaries leads to major legal problems since numerous jurisdictions lack specific regulations for AI system management (Kumar, 2023). Organizations need to establish particular accountability systems that outline the responsibilities of each role regarding algorithmic decision management. AI systems need auditing and monitoring to verify their compliance with ethical standards and regulatory requirements.

5. STRATEGIES FOR ORGANIZATIONAL ADAPTABILITY AND COMPLIANCE

Organizations encounter a persistent problem because the rules that govern AI systems and data protection continue to shift. Businesses need to stay alert to new policies and guidelines that governments and international bodies continue to develop. Organizations need to take active steps for compliance by providing continuous employee training, using compliance technology systems, and working with legal specialists to handle new regulatory requirements. They need to stay adaptable because AI systems must follow present legal and ethical standards, which change in the regulatory environment.

The regulatory framework for Artificial Intelligence (AI) and data protection undergoes continuous transformation because of rapid technological advancements and evolving public expectations (Spiecker and Döhmann, 2022). Organizations need to take part in compliance and become adaptable because governments and international bodies keep introducing new policies and guidelines. As a result, they require a strong compliance framework to operate successfully in the intricate environment of AI and data protection, according to Villegas-Ch and García-Ortiz (2023). The framework needs to establish specific rules that explain how the organization will follow GDPR and the EU Artificial Intelligence Act regulations. Key components of an effective compliance framework include:

- Full policies that promote data protection while upholding ethical standards and ensuring their AI systems remain accountable. The policies need periodic updates to match new laws and industry standards (Syifa, 2024).
- Performing risk assessments on a regular basis to detect both security vulnerabilities and compliance weaknesses. This proactive method allows organizations to establish preventive measures that reduce the risk of problems growing out of control (Esayas *et al.*, 2015).
- Compliance Audits: Routine compliance audits should be conducted to evaluate the effectiveness of existing policies and procedures. Organizations perform audits to identify areas of improvement and maintain regulatory compliance standards (Wolosz, 2007).

Organizations need to spend their resources on employee training and education programs that establish an ethical workplace culture that follows compliance standards. The training program must encompass all core AI elements, data protection standards, and regulatory compliance requirements:

- The organization needs to provide employees with full details about all applicable laws and regulations that impact their job responsibilities. Organizations can stay compliant with their daily activities through their understanding of these regulations, according to Thomasma (1992).
- The training programs need to teach participants about why ethical practices matter throughout the entire AI development and deployment process. The

education of employees about algorithmic bias, transparency, and accountability issues will help them make better decisions (Kamila and Jasrotia, 2025).

- The handling of sensitive data by employees requires specific training about data protection principles, which must include data minimization, purpose limitation, and consent management. The training program teaches staff members about proper data management techniques and legal requirements (Tahim *et al.*, 2012).

Organizations can achieve better regulatory compliance through the implementation of technological solutions. Businesses need to purchase compliance technology solutions that help manage data through governance systems and enable monitoring and reporting functions. Key technologies include:

- Data Governance Platforms function as organizational tools that enable proper data resource management through standardized collection, storage, and processing operations, which follow regulatory requirements. The tools enable organizations to monitor data origins and establish access restrictions for tracking their data management operations (Mahanti, 2021).
- AI monitoring tools are used to monitor organizations' AI systems' performance and detect algorithmic accountability and bias problems through these systems. These tools help organizations track decision-making activities, which enables them to address problems at their early stages before they escalate into major issues (Brown *et al.*, 2021).
- Compliance Management Software enables organizations to automate their compliance tasks through automated documentation and reporting, and audit management functions. By reducing the administrative burden associated with compliance, organizations can focus on strategic initiatives (Abdullah, 2019).

The implementation of new regulatory requirements requires legal specialists to work together with compliance professionals. Organizations need to form connections with external consultants, legal advisors, and industry associations to receive updates about regulatory changes and industry-leading practices. The following strategies enable teams to reach successful collaboration:

- Participating in industry forums and associations, because they provide access to peer knowledge about dealing with comparable organizational issues. The platforms enable users to exchange information about AI and data protection compliance standards and innovative methods (Chukwurah and Aderemi, 2024).
- Using policy advocacy to shape regulatory frameworks that affect their business activities. Businesses can help establish regulatory systems that protect innovation and fulfill social needs through their partnership with industry groups, according to Davis (2014).

The organizations should establish their core culture based on ethical responsibility because this method supports both regulatory compliance and innovation development. They need to integrate this culture into their core values, leadership structure, and decision-making framework. Strategies for promoting ethical responsibility include:

- Leaders showing their dedication to ethical conduct and regulatory adherence. Leaders must implement ethical principles into their planning, and they must face consequences when their decisions break compliance rules (Buell, 2009).
- Encouraging Open Dialogue: Organizations should cultivate an environment where employees feel comfortable discussing ethical dilemmas and compliance concerns. Open dialogue enables teams to detect potential problems and establish mutual comprehension of ethical duties (Thomasma, 1992).
- Recognition and incentives for ethical behavior. Those can motivate employees to prioritize compliance and responsible innovation, ultimately enhancing the organization's reputation and fostering trust among stakeholders (Gurzawska *et al.*, 2017).

6. CONCLUSIONS AND RECOMMENDATIONS

Business operations have entered a transformative period because of Artificial Intelligence (AI), Big Data, and Machine Learning (ML), which have evolved at a fast pace. Organizations must study public policy modifications because these changes affect their corporate strategies and determine their capacity to maintain growth and innovation. This research demonstrates how the EU Artificial Intelligence Act and European Data Strategy create substantial effects on corporate governance and innovation capacity, algorithmic accountability, and data protection. We show that these policies work to create an ethical environment for technology development, yet organizations face major obstacles when implementing them. Organizations need to modify their operations because algorithmic decision systems need transparent operations and data privacy safeguards but encounter various difficulties during execution. They need to understand that compliance serves as a strategic business advantage that goes beyond legal requirements.

The following recommendations emerge from these findings to help organizations handle digital economy challenges while following new public policy requirements:

- Organizations need to create an entire compliance system that meets all requirements of AI and data protection regulations. The framework requires detailed policies and procedures that prove the organization follows GDPR and the EU Artificial Intelligence Act requirements. Organizations can identify and reduce compliance gaps by using risk assessments, compliance audits, and policy updates.
- The allocation of funds for employee training and awareness programs leads to a culture of compliance because it provides continuous educational opportunities for staff members. Organizations need to establish training initiatives that teach employees about regulatory compliance, ethical AI methods, and data protection standards. Organizations can enhance their

decision-making abilities while upholding ethical standards through employee training programs that focus on AI and data governance competencies.

- Organizations can improve their regulatory requirement management through the implementation of compliance technologies. They need to purchase data governance platforms, AI monitoring tools, and compliance management software to achieve efficient compliance operations, enhanced data oversight, and legal requirement fulfillment. Administrative work can also be reduced through technology system implementation, which allows them to focus on strategic projects that generate innovation.
- The organizations need outside consultants, legal advisors, and industry associations to develop relationships for acquiring regulatory updates and industry standards. Organizations need continuous legal expert advice to understand new regulations and execute necessary strategic changes. Organizations that participate in industry forums gain access to compliance information, which enables them to build stronger collective abilities for managing regulatory challenges.
- The base for achieving compliance success and innovation requires organizations to establish ethical responsibility and maintain open dialogue. Organizations need to incorporate ethical principles into their core values, leadership methods, and decision-making frameworks. Leadership's dedication to ethical practices drives staff members to work on both regulatory compliance and ethical product development. Organizations can identify problems and create shared understanding about ethical duties through open discussions about ethical challenges and compliance issues.
- Organizations must participate in policy advocacy work to influence the development of regulatory systems that impact their operational activities. Businesses should work with industry organizations to develop fair regulatory systems that promote innovation through dialogue with government officials. This proactive method enables the development of rules that support digital economy innovation and competitive growth.
- Organizations must stay informed about regulatory changes because the environment continues to evolve. Organizations need to create systems that track regulatory changes and evaluate their effects on business activities for a successful, proactive response to new requirements. They must create fast adaptation capabilities because they need to stay compliant with regulations while keeping their AI systems in line with ethical frameworks.

The combination of Artificial Intelligence, Big Data, and Machine Learning systems with new public policies creates dual benefits and obstacles for business organizations. Organizations need to handle digital economy complexities through active compliance methods, employee training programs, technological implementations, team collaboration, ethical standards promotion and policy support. Organizations will enhance their market position and digital innovation capabilities through this method, which will also support the creation of inclusive digital governance systems that benefit all members of society. As the landscape continues to evolve, organizations that prioritize these strategies will be well-positioned to thrive in an era defined by technological advancement and regulatory scrutiny.

References

1) Abdullah, H. (2019). Analyzing the technological challenges of Governance, Risk and Compliance (GRC). *ICEECCOT*. [online]. Available at: https://doi.org/10.1109/ICEECCOT46775.2019.9114642 [Accessed 28.09.2025].
2) Allam, K. and Rodwal, A. (2023). AI-driven big data analytics: unveiling insights for business advancement. [online]. Available at: https://doi.org/10.53555/ephijse.v9i3.219 [Accessed 28.09.2025].
3) Baldi, V. and Oliveira, L. (2022). Challenges to incorporate accountability into artificial intelligence. *Procedia Computer Science,* 204, pp. 519-523. [online]. Available at: https://doi.org/10.1016/j.procs.2022.08.063 [Accessed 28.09.2025].
4) Brown, S., Davidovic, J. and Hasan, A. (2021). The algorithm audit: Scoring the algorithms that score us. *Big Data & Society*, 8(1). [online]. Available at: https://doi.org/10.1177/2053951720983865 [Accessed 28.09.2025].
5) Buell, J.M. (2009). Ethics and leadership: setting the right tone and structure can help other in their decision making. *Healthcare Executive*, 24 (3). [online]. Available at: https://europepmc.org/article/MED/19514224 [Accessed 28.09.2025].
6) Burri, T. and von Bothmer, F. (2021). The New EU Legislation on Artificial Intelligence: A Primer. *Social Science Research Network.* [online]. Available at: https://doi.org/10.2139/SSRN.3831424 [Accessed 28.09.2025].
7) Chesterman, S. (2025). Good models borrow, great models steal: intellectual property rights and generative AI. *Policy and Society,* 44 (1), pp. 23-37. [online]. Available at: https://doi.org/10.1093/polsoc/puae006 [Accessed 28.09.2025].
8) Chukwurah, E.G. and Aderemi, S. (2024). Harmonizing teams and regulations: strategies for data protection compliance in U.S. technology companies. *Computer Science & IT Research Journal*, 5 (4), pp. 824-838. [online]. Available at: https://doi.org/10.51594/csitrj.v5i4.1044 [Accessed 28.09.2025].
9) Coyle, D. and Weller, A. (2020). “Explaining” machine learning reveals policy challenges. *Science,* 368 (6498), pp. 1433-1434. [online]. Available at: https://doi.org/10.1126/SCIENCE.ABA9647 [Accessed 28.09.2025].
10) Custers, B. and Bachlechner, D. (2017). Advancing the EU data economy: Conditions for realizing the full potential of data reuse. *Information Polity,* 22 (4). [online]. Available at: https://doi.org/10.3233/IP-170419 [Accessed 28.09.2025].
11) Davis, K. (2014). Bridging the Innovation-Policy Gap. *SAIS Review,* 34 (1), pp. 87-92. [online]. Available at: https://doi.org/10.1353/SAIS.2014.0015 [Accessed 28.09.2025].
12) Dinka, D., Nyce, J.M. and Timpka, T. (2006). The need for transparency and rationale in automated systems. *Interacting with Computers*, 18 (5), pp. 1070-1083. [online]. Available at: https://doi.org/10.1016/J.INTCOM.2006.01.001 [Accessed 28.09.2025].

13) Drozdowski, P., Rathgeb, C., Dantcheva, A., Damer, N. and Busch, C. (2020). Demographic Bias in Biometrics: A Survey on an Emerging Challenge. *IEEE Transactions on Technology and Society*, 1 (2), pp. 89 – 103. [online]. Available at: https://doi.org/10.1109/TTS.2020.2992344 [Accessed 28.09.2025].

14) Esayas, S.Y., Mahler, T., Seehusen, F., Bjornstad, F. and Brubakk, V. (2015). An integrated method for compliance and risk assessment. *Communications and Networking Symposium*, 1 September. [online]. Available at: https://doi.org/10.1109/CNS.2015.7346870 [Accessed 28.09.2025].

15) EU's AI Act proposal foregrounds risks and rights (2023). *Emerald Expert Briefings.* [online]. Available at: https://doi.org/10.1108/oxan-es279879 [Accessed 28.09.2025].

16) European Commission (2020). *European Data Strategy*. Brussels: European Commission.

17) European Commission (2023). *Artificial Intelligence Act (EU AI Act): Proposal for a Regulation of the European Parliament and of the Council*. Brussels: European Commission.

18) Ferrer, X., van Nuenen, T., Such, J.M., Coté, M. and Criado, N. (2021). Bias and Discrimination in AI: A Cross-Disciplinary Perspective. *IEEE Technology and Society Magazine,* 40 (2), pp. 72-80. [online]. Available at: https://doi.org/ 10.1109/MTS.2021.3056293 [Accessed 28.09.2025].

19) Green, C. and Clayton, A. (2021). Ethics and AI Innovation. *The International Review of Information Ethics*, 29 [online]. Available at: https://doi.org/10.29173/IRIE417 [Accessed 28.09.2025].

20) Gurzawska, A., Mäkinen, M. and Brey, P. (2017). Implementation of Responsible Research and Innovation (RRI) Practices in Industry: Providing the Right Incentives. *Sustainability*, 9 (10), p. 1759 [online]. Available at: https://doi.org/10.3390/SU9101759 [Accessed 28.09.2025].

21) Kamila, M.K. and Jasrotia, S.S. (2025). Ethical issues in the development of artificial intelligence: Recognizing the risks. *International Journal of Ethics and Systems*, 41 (1), pp. 45-63. [online]. Available at: https://doi.org/10.1108/ijoes-05-2023-0107 [Accessed 28.09.2025].

22) Kumar, P. (2023). Determination of Civil and Criminal Liability of Artificial intelligence. *DME Journal of Law*, 4 (1), pp. 48-55. [online]. Available at: https://doi.org/10.53361/dmejl.v4i01.06 [Accessed 28.09.2025].

23) Li, H., Yu, L. and He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, 22 (1), pp. 1-6. [online]. Available at: https://doi.org/10.1080/1097198X.2019.1569186 [Accessed 28.09.2025].

24) Li, J., Liu, Y., Yue, L., Jin, F., Guo, Q. and Xu, C. (2018). Artificial Intelligence Governed by Laws and Regulations. In: Jin, D. (eds) *Reconstructing Our Orders*. Springer, Singapore. [online]. Available at: https://doi.org/10.1007/978-981-13-2209-9_3 [Accessed 28.09.2025].

25) Mahanti, R. (2021). Data Governance and Compliance. In: *Data Governance and Compliance*. Springer, Singapore. [online]. Available at: https://doi.org/10.1007/978-981-33-6877-4_5 [Accessed 28.09.2025].

26) Miryala, N.K. and Gupta, D. (2022). Data Security Challenges and Industry trends. *International Journal of Advanced Research in Computer and Communication Engineering,* 11 (11), pp. 300-309. [online]. Available at: https://doi.org/10.17148/ijarcce.2022.111160 [Accessed 28.09.2025].

27) Mone, G. (2016). Bias in technology. *Communications of the ACM*, 60 (1), pp. 19-20. [online]. Available at: https://doi.org/10.1145/3014388 [Accessed 28.09.2025].

28) Ntoutsi, E., Fafalios, P., Gadiraju, U., Iosifidis, V., Nejdl, W., Vidal, M.-E., Ruggieri, S., Turini, F., Papadopoulos, S., Krasanakis, E., Kompatsiaris, I., Kinder-Kurlanda, K., Wagner, C., Karimi, F., Fernandez, M., Alani, H., Berendt, B., Berendt, B., Kruegel, T., … Staab, S. (2020). Bias in data-driven artificial intelligence systems – An introductory survey. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery,* 10 (3), e1356. [online]. Available at: https://doi.org/10.1002/WIDM.1356 [Accessed 28.09.2025].

29) Savage, N. (2020). The race to the top among the world's leaders in artificial intelligence. *Nature,* [online]. Available at: https://doi.org/10.1038/D41586-020-03409-8 [Accessed 28.09.2025].

30) Sherwood, R.M. (1990). *Intellectual Property and Economic Development*. New York: Routledge. [online]. Available at: https://doi.org/10.4324/9780429045530 [Accessed 28.09.2025].

31) Spiecker, I. and Döhmann, G. (2022). AI and data protection. in DiMatteo, L.A., Poncibò, C. and Cannarsa, M. (eds.). *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, pp. 132–145. Cambridge: Cambridge University Press.

32) Syifa, A.F. (2024). Ethics in the Age of AI: Principles and Guidelines for Responsible Implementation in Workplace. *IJATSS,* [online]. Available at: https://doi.org/10.59890/ijatss.v2i2.1398 [Accessed 28.09.2025].

33) Tahim, A., Sabharwal, S., Dhokia, R., Bajekal, R. and Kyriacou, S. (2012). Data protection training improves data handling. *The Clinical Teacher,* 9 (6), pp. 403-407. [online]. Available at: https://doi.org/10.1111/J.1743-498X.2012.00557.X [Accessed 28.09.2025].

34) Thomasma, D. (1992). Ethical duties to employees. *Healthcare Executive,* 7 (3), p. 26.

35) Villegas-Ch, W. and García-Ortiz, J. (2023). Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence. *Electronics*, 12(18), 3786. [online]. Available at: https://doi.org/10.3390/electronics12183786 [Accessed 28.09.2025].

36) Wolosz, L. (2007). Sound policies and procedures: The basis of a sound compliance program. *Journal of Investment Compliance,* 8 (4), pp. 7-11. [online]. Available at: https://doi.org/10.1108/15285810710839471 [Accessed 28.09.2025].

37) Yadav, M.K. and Dwivedi, N. (2023). Impact of AI on Business. *International Journal for Multidisciplinary Research,* 5 (3). [online]. Available at: https://doi.org/10.36948/ijfmr.2023.v05i03.2791 [Accessed 28.09.2025].