World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Ethical and Governance Challenges of AI in Information Systems: Toward Responsible Adoption in Enterprise Systems

Osita Victor Egwuatu *

MBA (Information Systems), College of Business and Innovation, The University of Toledo, Toledo, Ohio United States.

World Journal of Advanced Research and Reviews, 2025, 27(02), 1744-1751

Publication history: Received on 16 July 2025; revised on 24 August 2025; accepted on 26 August 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.2.3064

Abstract

Artificial Intelligence (AI) is rapidly reshaping enterprise information systems (EIS), from decision-support tools to enterprise resource planning (ERP), customer relationship management (CRM), and human resource information systems (HRIS). While AI adoption promises efficiency, personalization, and predictive insights, it also introduces profound ethical and governance challenges. Issues such as algorithmic bias, data privacy breaches, lack of transparency, and weak accountability structures threaten both organizational integrity and societal trust. This article examines the ethical and governance dimensions of AI in enterprise systems, highlighting policy gaps, emerging frameworks, and the need for responsible AI adoption. Using case-based insights and policy analysis, it argues for a multi-stakeholder governance model that integrates corporate responsibility, regulatory compliance, and societal values. The findings underscore the importance of aligning enterprise AI practices with data ethics and governance to safeguard both organizational value and social well-being.

Keywords: Artificial Intelligence Governance; Enterprise Information Systems; Algorithmic Bias; Data Ethics and Privacy; Responsible AI Adoption; Regulatory Compliance

1. Introduction

Enterprise Information Systems (EIS) form the backbone of modern organizations, enabling the seamless integration of functions across finance, logistics, human resources, supply chain management, and customer engagement. In their traditional form, EIS centralized information flows, reduced redundancies, and provided a foundation for organizational efficiency. Today, however, the integration of Artificial Intelligence (AI) has transformed these systems into intelligent ecosystems capable of predictive analytics, adaptive automation, and real-time decision-making. By leveraging machine learning, natural language processing, and advanced data modeling, AI-driven EIS offers organizations the ability to anticipate market shifts, optimize resource allocation, and personalize services at scale.

Yet, these technological breakthroughs come with profound ethical and governance challenges. Unlike prior waves of digitization, AI adoption introduces an element of autonomy and opacity into decision-making processes. This raises questions about how data is collected, who has access, how decisions are justified, and who is accountable when harm occurs. For instance, AI-based recruitment tools embedded in HR systems have been shown to reproduce gender or racial bias; predictive maintenance systems in manufacturing may prioritize efficiency over worker safety; and customer analytics platforms can verge into invasive surveillance practices that threaten privacy. These scenarios illustrate the tension between the promise of innovation and the risks of misuse.

* Corresponding author: Osita Victor Egwuatu

In recognition of such risks, governments and international bodies are moving toward regulatory responses. The European Union's Artificial Intelligence Act (2024) is a landmark initiative that classifies AI systems according to risk categories, imposing strict governance obligations on "high-risk" applications such as those in employment, healthcare, and critical infrastructure. Similarly, the OECD Principles on AI (2019) emphasize values of transparency, accountability, and human-centered design, while the U.S. Blueprint for an AI Bill of Rights (2022) sets out guidelines to protect citizens from harmful AI applications. Despite these initiatives, however, adoption in enterprise contexts remains uneven. Many firms deploy AI systems without robust governance structures, driven by competitive pressures and efficiency gains rather than ethical responsibility.

The stakes extend well beyond organizational boundaries. Enterprises are critical nodes in the digital economy, and their adoption practices influence employees, customers, regulators, and wider society. A failure to embed ethical governance into AI-enabled EIS risks not only legal non-compliance and reputational damage but also the erosion of public trust in digital transformation. Conversely, responsible adoption can serve as a societal good, ensuring that technological progress enhances fairness, inclusivity, and transparency.

This paper therefore, explores the ethical and governance challenges of AI in enterprise information systems. It argues that while technological innovation is central to competitiveness, it must be balanced with frameworks of responsibility and accountability. Specifically, the study examines the intersections of policy, data ethics, and governance structures, offering insights into how enterprises can align AI adoption with both organizational goals and societal expectations. The ultimate aim is to propose a pathway for responsible AI governance that safeguards trust, ensures compliance, and contributes positively to the digital society.

2. Ethical Challenges in Enterprise AI

The integration of Artificial Intelligence into Enterprise Information Systems (EIS) has amplified ethical considerations that go beyond traditional concerns of data management and operational efficiency. Scholars in information systems and business ethics emphasize that AI introduces a unique layer of complexity: decisions are increasingly shaped by algorithms whose logic may be opaque, biased, or misaligned with societal expectations (Mittelstadt, 2019; Floridi & Cowls, 2019). This section reviews the literature on four central ethical challenges: data privacy and surveillance, algorithmic bias and discrimination, transparency and explainability, and accountability and liability, which have emerged as defining issues for enterprise AI adoption.

2.1. Data Privacy and Surveillance

AI-driven EIS are heavily reliant on large-scale data aggregation, often combining sensitive information from employees, customers, and business partners. While such integration enhances predictive accuracy and decision-making, it raises serious concerns regarding privacy, informed consent, and surveillance.

Scholars argue that AI-enabled enterprise systems can blur the line between legitimate performance monitoring and invasive surveillance practices (Ball, 2010). For example, Human Resource Information Systems (HRIS) equipped with AI can track keystrokes, monitor communications, and analyze biometric data to evaluate employee productivity. Although intended to optimize performance, such monitoring may create an atmosphere of mistrust, stress, and diminished autonomy in the workplace (Ajana, 2020).

2.2. Algorithmic Bias and Discrimination

Another key ethical concern is algorithmic bias, whereby AI models reproduce or amplify historical inequities present in training datasets. Research has documented cases in which recruitment algorithms systematically disadvantaged female applicants, ethnic minorities, or individuals with non-traditional educational backgrounds (Raghavan et al., 2020).

In enterprise contexts, this creates a sharp ethical dilemma: while AI promises efficiency and cost savings in decision-making, its outcomes may compromise fairness and equal opportunity. For example, an AI-powered recruitment system trained on historical data from a male-dominated industry may inadvertently penalize female candidates, not because of their skills but due to patterns encoded in the data. Similar concerns arise in customer service systems that apply biased risk-scoring models to minority clients, resulting in discriminatory access to credit or insurance (O'Neil, 2016).

2.3. Transparency and Explainability

The opacity of AI models, often referred to as the "black box" problem, poses a significant governance challenge. Many enterprise AI applications, especially those based on deep learning, generate outputs that are difficult to interpret even for their developers (Burrell, 2016). This lack of transparency undermines trust among stakeholders, particularly when AI systems make consequential decisions about hiring, promotions, credit approvals, or supply chain prioritization.

Regulators and scholars have increasingly called for explainable AI (XAI) to address these concerns (Doshi-Velez & Kim, 2017). Users, employees, and regulators demand clear explanations of how decisions are reached, especially in contexts where accountability is shared across multiple actors. For enterprises, the inability to explain algorithmic outcomes not only erodes trust but may also result in legal liabilities under emerging regulations such as the EU AI Act, which mandates transparency for high-risk applications.

2.4. Accountability and Liability

Finally, one of the most debated challenges concerns accountabilities: when an AI-enabled system makes a harmful or unfair decision, who should be held responsible? Scholars highlight a diffusion of responsibility across multiple actors, including developers, vendors, managers, and end-users (Calo, 2015). This diffusion creates what is often described as a "responsibility gap" (Matthias, 2004), where no single actor accepts liability for adverse outcomes.

For example, if an AI-driven loan approval system in a financial enterprise denies credit unfairly, responsibility could be attributed to the data scientists who built the model, the vendor who supplied the software, the managers who deployed it, or the organization that failed to implement oversight mechanisms. Without clear governance structures, accountability remains ambiguous, eroding public confidence and exposing enterprises to reputational and legal risks.

3. Governance Challenges in AI Adoption

While ethical issues highlight the risks of AI-enabled Enterprise Information Systems (EIS), governance challenges determine whether organizations can adequately address those risks. Governance in this context refers not only to legal compliance but also to the internal structures, policies, and cultural norms that guide responsible AI use. The literature suggests that enterprises face four critical governance challenges: regulatory gaps, corporate governance weaknesses, policy–enterprise misalignment, and stakeholder pressures (Gasser & Almeida, 2017; Wirtz et al., 2020).

3.1. Regulatory Gaps

Governments worldwide have begun to introduce laws and regulatory frameworks to manage AI adoption, including the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA/CPRA) in the United States, and the European Union AI Act (2024). These frameworks address issues such as consent, risk classification, algorithmic transparency, and human oversight.

However, enforcement remains inconsistent. Studies show that multinational enterprises struggle to reconcile cross-border governance in global systems, as regulatory requirements vary dramatically between jurisdictions (Binns, 2018). For example, a multinational firm operating in both the EU and Asia may need to comply with strict data localization rules in one jurisdiction while facing weaker or absent AI regulations in another. The absence of harmonized international standards creates uncertainty and increases compliance costs, leaving gaps in protection for users and communities.

3.2. Corporate Governance Weaknesses

At the organizational level, many enterprises lack robust AI-specific governance structures. Research indicates that few firms have established AI ethics boards, dedicated risk committees, or cross-disciplinary oversight mechanisms (Raisch & Krakowski, 2021). Instead, responsibility for AI governance often falls to IT or compliance departments, which may lack expertise in ethical reasoning or societal impacts.

A related weakness is the lack of standardized auditing mechanisms for algorithmic fairness and accountability. Unlike financial auditing, which has well-established procedures, algorithmic auditing remains ad hoc, voluntary, and unevenly applied across industries (Raji et al., 2020). This absence of standardized metrics undermines both internal accountability and external trust.

3.3. Policy–Enterprise Misalignment

The pace of innovation in AI often far exceeds the ability of regulators and enterprises to keep up. Organizations frequently adopt AI tools to gain a competitive edge before clear compliance structures or ethical safeguards are in place (Cath, 2018). This "deploy first, regulate later" dynamic creates a policy–enterprise misalignment: while regulation lags behind innovation, enterprises are left without clear guidance, and regulators are forced into reactive positions.

The misalignment also creates risks of retroactive penalties. For instance, firms that implement facial recognition or predictive analytics tools without oversight may later face regulatory crackdowns, lawsuits, or reputational damage once policies catch up. This uncertainty discourages proactive governance and fosters short-termism in enterprise AI strategies.

3.4. Stakeholder Pressures

Finally, enterprises face growing pressures from external stakeholders—including investors, consumers, advocacy groups, and civil society organizations—to demonstrate responsible AI practices. Investors increasingly consider environmental, social, and governance (ESG) criteria, including AI ethics, in their assessments of corporate risk (World Economic Forum, 2021). Meanwhile, consumers reward companies that adopt transparent and ethical AI practices, as trust becomes a key determinant of digital adoption (Smith & Browne, 2022).

Failure to meet these expectations can trigger reputational crises, boycotts, or divestment campaigns. Conversely, enterprises that embrace responsible AI governance may gain a competitive advantage by signaling credibility and accountability to stakeholders. In this sense, governance challenges are not only compliance obligations but also strategic imperatives that influence long-term value creation.

4. Case examples

Case studies offer a practical lens for understanding the ethical and governance challenges associated with AI adoption in enterprise information systems (EIS). By examining real-world scenarios across different sectors and geographies, we can see how organizations confront issues of bias, transparency, privacy, and regulatory compliance. The following three examples, drawn from recruitment, supply chain management, and healthcare, illustrate the multifaceted nature of these challenges and the governance responses that enterprises have adopted.

4.1. HR Recruitment AI in the United States

One of the most widely cited cases of ethical risk in enterprise AI comes from the deployment of recruitment algorithms in human resource information systems (HRIS). A U.S.-based multinational technology firm integrated AI into its candidate screening process to manage the high volume of job applications. The system was trained on historical hiring data spanning over a decade, primarily reflecting a male-dominated workforce in technical roles.

The outcome was problematic: the algorithm systematically downgraded resumes that included indicators of female identity, such as attendance at women's colleges or membership in women's professional associations. It also displayed racial bias in evaluating candidates from underrepresented groups (Raghavan et al., 2020). The incident sparked public criticism and raised concerns about whether AI tools were entrenching existing inequalities rather than reducing them.

4.2. ERP Supply Chain Optimization in Europe

In Europe, a multinational manufacturing enterprise implemented an AI-enhanced Enterprise Resource Planning (ERP) system to improve supply chain efficiency. The AI module used predictive analytics to forecast demand, optimize supplier selection, and automate procurement decisions. While the system initially improved cost efficiency, it soon created tensions with suppliers who challenged the fairness and transparency of the automated decisions.

For example, smaller suppliers argued that the AI's opaque selection criteria disproportionately favored larger vendors with greater historical transaction data, effectively locking out newer or smaller firms. This raised concerns not only of competitive fairness but also of potential violations of EU regulations on procurement transparency. The situation attracted regulatory scrutiny under the emerging provisions of the EU AI Act, which classifies supply chain and procurement systems as "high-risk" when they affect economic livelihoods.

In response, the enterprise adopted a governance strategy aligned with EU compliance frameworks. It introduced explainability features into the ERP system, allowing suppliers to see how decisions were reached, and established an appeals process for vendors to contest algorithmic outcomes. The company also engaged in third-party compliance audits, ensuring that procurement practices met both regulatory and ethical standards. This case demonstrates the necessity of aligning enterprise AI governance not only with efficiency goals but also with broader legal and societal expectations of fairness.

4.3. Healthcare CRM in Asia

A healthcare provider in Asia adopted an AI-driven Customer Relationship Management (CRM) platform to enhance patient engagement and improve clinical service delivery. The system used machine learning to analyze patient histories, predict health risks, and recommend personalized treatment plans. However, the integration of AI into healthcare raised significant privacy and data sovereignty concerns.

Patients expressed unease about the use of sensitive health data for predictive analytics. At the same time, regulators flagged conflicts between multinational data-sharing practices and local data sovereignty laws, which required certain health data to be stored and processed within national borders. Additionally, the lack of clear consent mechanisms raised ethical questions about whether patients fully understood how their data would be used.

To address these concerns, the provider adopted a governance response that combined localized data storage, ensuring patient data remained within the jurisdiction, with differential privacy techniques that allowed aggregate analysis without exposing identifiable patient information. The organization also revised its consent protocols, providing patients with more precise explanations of how their data would be used and offering opt-out mechanisms for non-essential services. This case illustrates the delicate balance between leveraging AI for healthcare innovation and respecting the ethical and regulatory imperatives of privacy, consent, and data sovereignty.

5. Toward a Responsible AI Governance Framework

The analysis of ethical and governance challenges in enterprise AI demonstrates that fragmented or reactive approaches are insufficient to address the risks of bias, opacity, and regulatory misalignment. What enterprises require is a holistic governance framework that integrates ethical reflection with compliance, organizational design, stakeholder input, and broader societal objectives. Building on insights from the literature and case studies, this paper proposes the Responsible Enterprise AI Framework (REAF), a model structured around five interrelated pillars.

5.1. Ethical Principles

At the foundation of REAF are ethical principles that should guide all stages of AI adoption in enterprise information systems. These principles include fairness, transparency, accountability, and human oversight (Floridi & Cowls, 2019; Mittelstadt, 2019).

- Fairness requires enterprises to identify and mitigate algorithmic bias, ensuring equitable treatment of employees, customers, and partners.
- Transparency emphasizes explainability and interpretability, providing stakeholders with meaningful insight into AI-driven decisions.
- Accountability ensures that decision-making responsibility is not diffused across technical and managerial actors but clearly assigned.
- Human oversight underscores that AI should augment rather than replace human judgment, particularly in high-stakes decisions such as hiring, healthcare, and finance.

Embedding these principles into enterprise governance fosters trust, reduces risk, and aligns organizational values with societal expectations.

5.2. Regulatory Alignment

The second pillar is regulatory alignment, recognizing that enterprises operate within increasingly complex legal environments. AI adoption must comply with both general data protection laws and emerging AI-specific regulations, including the GDPR in Europe, the EU AI Act, the California Privacy Rights Act (CPRA), and sectoral frameworks such as HIPAA in healthcare.

Enterprises must adopt a proactive rather than reactive approach, incorporating regulatory requirements into system design from the outset (the “compliance by design” principle). This entails:

- Conducting impact assessments for high-risk AI applications.

- Documenting decision-making processes for regulatory audits.
- Establishing cross-border compliance strategies for multinational operations.

Aligning AI systems with regulatory frameworks not only minimizes legal exposure but also creates a foundation of accountability that strengthens organizational legitimacy.

5.3. Organizational Structures

Effective AI governance requires institutionalized structures within the enterprise to oversee ethical compliance and operational risk. Many organizations currently lack such structures, relying instead on ad hoc or siloed approaches. REAF recommends the development of:

- AI Ethics Committees: cross-functional bodies that review AI projects, ensuring alignment with ethical principles and regulatory requirements.
- Algorithmic Audits: systematic evaluations of model inputs, outputs, and impacts, modeled after financial auditing standards.
- Governance Boards: oversight groups embedded at the executive level, tasked with integrating AI ethics into corporate strategy.

By embedding these structures, enterprises create internal checks and balances that institutionalize responsible AI use.

5.4. Stakeholder Engagement

AI adoption in enterprise systems does not occur in isolation—it directly affects employees, customers, suppliers, regulators, and communities. The fourth pillar of REAF emphasizes stakeholder engagement as a mechanism for legitimacy and trust. This involves:

- Employees: consulting staff on monitoring technologies, training, and human-AI interaction.
- Customers: providing clear consent mechanisms, opt-out options, and avenues for appeal.
- Regulators: proactively engaging in dialogue to anticipate compliance shifts.
- Civil society and advocacy groups: including external perspectives to identify blind spots in ethical risk assessments.

Such engagement moves governance from a top-down compliance model to a participatory process, ensuring that AI systems reflect the needs and rights of diverse stakeholders.

5.5. Societal Contribution

Finally, responsible AI governance must be evaluated not only by organizational efficiency or compliance metrics but also by its societal contribution. AI adoption in enterprises should promote inclusivity, sustainability, and public trust.

- Inclusivity ensures that AI-driven systems reduce rather than reproduce social inequities.
- Sustainability requires that AI deployment aligns with environmental and social governance (ESG) principles.
- Public trust emerges when enterprises demonstrate that AI enhances, rather than undermines, human dignity and community welfare.

By embedding societal contribution as a governance goal, enterprises can align innovation with social good, reinforcing their role as responsible actors in the digital economy.

6. Societal Contributions and Implications

The governance of AI in enterprise information systems carries significance that extends far beyond organizational boundaries. Because enterprises act as key nodes in the digital economy, their adoption choices influence employees, consumers, suppliers, regulators, and entire communities. As such, the implementation of responsible AI frameworks produces layered contributions to business practice, public policy, and society at large.

6.1. Implications for Enterprises

For enterprises, the adoption of ethical and responsible AI governance frameworks is not simply a compliance exercise but a strategic imperative. Organizations that integrate fairness, transparency, and accountability into their AI systems are better positioned to build long-term trust with employees, customers, and investors. This trust functions as an intangible asset that strengthens organizational resilience in competitive markets (Smith & Browne, 2022).

Moreover, embedding governance structures reduces exposure to compliance risks under evolving regulatory regimes such as the GDPR, EU AI Act, or CPRA. Proactive governance enables firms to anticipate regulatory change rather than react defensively, thereby lowering the risk of penalties and reputational harm. Finally, enterprises that demonstrate leadership in responsible AI adoption enhance their brand reputation, signaling to consumers and partners that they are forward-looking, ethical, and socially accountable.

6.2. Implications for Policymakers

For policymakers, responsible enterprise adoption of AI offers evidence that regulatory initiatives can be both enforceable and effective. When enterprises demonstrate alignment with frameworks such as the OECD AI Principles or the EU AI Act, it creates regulatory clarity and reduces ambiguity for both firms and regulators.

Harmonization across jurisdictions also becomes more achievable when enterprises actively participate in compliance dialogues and share best practices. This helps reduce the fragmentation of global AI governance, which currently hampers multinational organizations and creates uneven levels of protection for users. By setting strong examples, enterprises can contribute to the evolution of international standards, supporting policymakers in their efforts to balance innovation with social responsibility.

6.3. Implications for Society

At the societal level, the responsible governance of enterprise AI contributes to the equitable transformation of the digital economy. By mitigating algorithmic bias, enterprises reduce the risk of reinforcing systemic discrimination, thereby promoting inclusivity in hiring, lending, healthcare, and other domains.

Responsible data practices also protect individual privacy and autonomy, countering the rise of surveillance capitalism and opaque data monetization models (Zuboff, 2019). In addition, enterprises that embed principles of transparency and accountability foster public trust, which is critical for the acceptance of AI technologies in everyday life.

Finally, AI systems that align with sustainability and fairness goals contribute to broader social well-being, ensuring that technological innovation is not pursued at the expense of human dignity, equity, or environmental responsibility. In this sense, responsible enterprise AI governance functions not only as a safeguard against harm but as a driver of social progress.

6.4. Integrative Perspective

Taken together, these implications underscore that responsible enterprise AI governance is a multi-stakeholder project. Enterprises benefit through resilience and reputation, policymakers benefit through clarity and harmonization, and society benefits through fairness, privacy, and trust. The broader contribution is the alignment of technological innovation with societal values, ensuring that AI-enabled digital transformation advances not only organizational efficiency but also human flourishing.

7. Conclusion

AI in enterprise information systems offers immense promise but introduces profound ethical and governance challenges. To achieve responsible adoption, organizations must integrate ethics into governance frameworks, align with evolving regulations, and proactively engage stakeholders. The societal contribution lies not just in technological progress but in ensuring AI systems foster fairness, accountability, and trust across the digital economy.

References

[1] Ajana, I. (2020). The paradox of automation as anti-bias intervention. Cardozo Law Review, 41(4), 1671–1714. https://cardozolawreview.com/the-paradox-of-automation-as-anti-bias-intervention

[2] Ball, K. (2010). Workplace surveillance: An overview. Labor History, 51(1), 87–106. https://doi.org/10.1080/00236561003654776

[3] Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. Proceedings of the 1st Conference on Fairness, Accountability and Transparency (FAT*), 149–159. https://doi.org/10.1145/3287560.3287580

[4] Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, 3(1), 1–12. https://doi.org/10.1177/2053951715622512

[5] Calo, R. (2015). Robotics and the lessons of cyberlaw. California Law Review, 103(3), 513–563. https://doi.org/10.2139/ssrn.2402972

[6] Cath, C. (2018). Governing artificial intelligence: Ethical, legal and technical opportunities and challenges. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376(2133), 20180080. https://doi.org/10.1098/rsta.2018.0080

[7] Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608. https://doi.org/10.48550/arXiv.1702.08608

[8] European Union. (2024). Regulation (EU) …/2024 laying down harmonised rules on Artificial Intelligence (AI Act). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[9] Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. Harvard Data Science Review, 1(1). https://doi.org/10.1162/99608f92.8cd550d1

[10] Gasser, U., & Almeida, V. A. (2017). A layered model for AI governance. IEEE Internet Computing, 21(6), 58–62. https://doi.org/10.1109/MIC.2017.4180835

[11] Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. Ethics and Information Technology, 6(3), 175–183. https://doi.org/10.1007/s10676-004-3422-1

[12] Mittelstadt, B. D. (2019). Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, 1(11), 501–507. https://doi.org/10.1038/s42256-019-0114-4

[13] O'Neil, C. (2016). Weapons of math destruction: How big data increases inequality and threatens democracy. Crown. https://doi.org/10.2307/j.ctt1t89h5v

[14] OECD. (2019). OECD principles on artificial intelligence. OECD Publishing. https://oecd.ai/en/ai-principles

[15] Raghavan, M., Barocas, S., Kleinberg, J., & Levy, K. (2020). Mitigating bias in algorithmic hiring: Evaluating claims and practices. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT*), 469–481. https://doi.org/10.1145/3351095.3372828

[16] Raji, I. D., Smart, A., White, R., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT*), 33–44. https://doi.org/10.1145/3351095.3372873

[17] Rahwan, I. (2018). Society-in-the-loop: Programming the algorithmic social contract. Ethics and Information Technology, 20(1), 5–14. https://doi.org/10.1007/s10676-017-9430-8

[18] Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation–augmentation paradox. Academy of Management Review, 46(1), 192–210. https://doi.org/10.5465/amr.2018.0072

[19] Smith, A., & Browne, K. (2022). Public trust in artificial intelligence: Global insights. AI & Society, 37(4), 1571–1583. https://doi.org/10.1007/s00146-021-01237-3

[20] U.S. White House. (2022). Blueprint for an AI Bill of Rights: Making automated systems work for the American people. Office of Science and Technology Policy. https://www.whitehouse.gov/ostp/ai-bill-of-rights

[21] World Economic Forum. (2021). Global AI governance: Building responsible AI frameworks for business. https://www.weforum.org/reports/global-ai-governance

[22] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs. https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/