Author Accepted Manuscript (AAM)

Please cite the published version:
Erduran, M. (2025). Ethical and legal implications of AI-driven MIS solutions. In A. G. Yüksek & O. Kaynar (Eds.), *Information technologies in managerial decision-making: Foundations and application* (pp. 283–306). Livre de Lyon. https://doi.org/10.5281/zenodo.18039480

ETHICAL AND LEGAL IMPLICATIONS OF AI-DRIVEN MIS SOLUTIONS

Mehmethan ERDURAN
(Res. Assist.), İzmir Democracy University
mehmethanerduran@hotmail.com
ORCID: 0000-0003-1620-2523

1. INTRODUCTION

The modern business world is witnessing a significant paradigm shift in Management Information Systems (MIS). Older MIS systems, characterised as passive and descriptive, are now being replaced by more advanced, active, predictive systems. The integration of artificial intelligence (AI) into these systems is accelerating this paradigm shift. It can be said that there is a macro-trend for the integration of AI-driven solutions for the workflows in several sectors. AI acts as a general-purpose technology that is being adopted across the economy (Cockburn et al., 2018). Such technology became more than just a tool. As mentioned by Cockburn et al. (2018), AI is a method of innovation for the companies to re-evaluate their operational workflows to avoid being left behind. From healthcare and finance to government services, thanks to the continuous innovation of technology, AI-supported MIS solutions not only increase the productivity capacity of companies but also offer innovations in their decision-making processes. According to Gartner's (2025) projection of worldwide AI spending, nearly $1.5 trillion will be invested in 2025 alone for the different AI markets. Global investment in artificial intelligence is projected to see significant growth across all IT markets, with spending expected to increase from 2024 through 2026 (Gartner, 2025). A detailed breakdown is provided in Table 1.

As Qian et al. (2024) claim, AI applications now appear in education, healthcare, transportation, manufacturing and beyond. For example, AI systems can automate routine tasks, detect complex patterns in large datasets, and even generate content or predictions (McAfee & Brynjolfsson, 2017; Agrawal et al., 2019). It's impossible to consider these critically important business processes independently. AI-powered MIS

systems, which can optimise supply chain networks, analyse marketing strategies in real time to personalise them to customer needs, and perform all of this at an automated level, are creating strategic and significant changes in the business world. In the healthcare sector, as detailed by Jiang et al. (2017), specific applications range from using deep learning for diagnostic imaging to detect pathologies like tumours with remarkable speed and accuracy to leveraging machine learning for personalised medicine, where patient data is analysed to tailor individual treatment plans.

Table 1: AI Spending in IT Markets, Worldwide, 2024-2026 (Millions of U.S. Dollars)[1]

Market	**2024**	**2025**	**2026**
AI Services	259,477	282,556	324,669
AI Application Software	83,679	172,029	269,703
AI Infrastructure Software	56,904	126,177	229,825
GenAI Models	5,719	14,200	25,766
AI-optimised Servers (GPU and Non-GPU AI Accelerators)	140,107	267,534	329,528
AI-optimised IaaS	7,447	18,325	37,507
AI Processing Semiconductors	138,813	209,192	267,934
AI PCs by ARM and x86	51,023	90,432	144,413
GenAI Smartphones	244,735	298,189	393,297
Total AI Spending	**987,904**	**1,478,634**	**2,022,642**

Although these developments are exciting, the ethical, legal, and social implications of integrating artificial intelligence into MIS systems are also an important area to consider. This rapid development of artificial intelligence and its integration into MIS systems used in the business world has also raised many concerns about bias, accountability, transparency,

[1]The data presented in this table is from "Gartner Says Worldwide AI Spending Will Total $1.5 Trillion in 2025," by Gartner, 2025 (https://www.gartner.com/en/newsroom/press-releases/2025-09-17-gartner-says-worldwide-ai-spending-will-total-1-point-5-trillion-in-2025). Copyright 2025 by Gartner, Inc.

privacy, data confidentiality and social ethics. Considering all these developments, many studies conducted in academia suggest that the rapid impact of artificial intelligence on such MIS-driven systems could not only significantly change but also disrupt both labour markets and social structures. For example, Frey and Osborne (2017) stated that approximately 47% of US employment is at risk of being computerised, even before artificial intelligence has developed to this degree. While automation historically creates new industries, Acemoglu and Restrepo (2018) argue that the current displacement effect, where capital replaces labour, may outpace the reinstatement effect of new task creation, potentially leading to stagnating wages and a shrinking labour share of income. Research also indicates that these changes are not limited to a specific sector. Recent analysis by the International Monetary Fund suggests that nearly 40% of global employment is exposed to AI, a phenomenon likely to exacerbate inequality both within and between nations by disproportionately rewarding holders of capital over workers (Cazzaniga et al., 2024). At the same time, AI-driven systems have been demonstrated to tend to encode human biases, lack explainability, and make decisions with major consequences without adequate oversight (Pazzanese, 2020). Due to such situations, ethical, legal and social studies need to be carried out for the integration of artificial intelligence into MIS systems.

The number of studies in the literature that analyse the ethical, legal, and social implications of integrating AI into MIS-based systems has visibly increased due to ongoing developments. However, it can be argued that gaps remain in the literature, particularly due to laws and regulations not keeping pace with technological advancements. The difficulty of integrating ethical principles into practice is one of the other primary reasons contributing to this gap in the literature. Considering the impact of AI on every business sector globally, discussions of ethical, legal, and social structures in this area become even more important.

To address this gap in the literature, this chapter discusses the ethical and legal implications of solutions offered by AI-powered MIS-supported systems. This review is conducted from a global and intersectoral perspective. While it is known that the integration of AI into each sector occurs within different frameworks and at different speeds, I believe the underlying ethical and legal issues that emerge are common. Initially, this research began with a literature review to identify common themes. Then, issues such as algorithmic bias, transparency, data privacy, and human autonomy, which were identified as common themes, were discussed, and the ethical implications of AI integration in MIS were examined. The next section approaches the topic from the perspective of lawmakers and discusses the legal regulations in this area. Finally, in the

conclusion section, all discussions in the research are synthesised, and the interdisciplinary and global approach required for this integration to proceed more smoothly and beneficially in ethical, legal and social terms is emphasised.

2. LITERATURE REVIEW

The rapid development of artificial intelligence has significantly increased the number of studies on this technology. The integration of artificial intelligence into information systems has been studied in many different fields, and these studies have been enriched by discussions in diverse disciplines, such as computer science, ethics, law, sociology, and business. Fundamental theoretical frameworks have been developed to support responsible AI development, and principles have been structured based on these frameworks. These frameworks in the literature have been found to converge on common themes. Across numerous guidelines, common principles include human oversight, transparency, accountability, safety, fairness, and privacy (Fjeld et al., 2020; Jobin et al., 2019). These principles are reflected in important documents such as the OECD AI Principles (Organisation for Economic Co-operation and Development [OECD], 2024) and UNESCO's Recommendation on the Ethics of AI (United Nations Educational, Scientific and Cultural Organization [UNESCO], 2022), which promote human rights, fairness, inclusiveness, and sustainability in AI use. For instance, the UNESCO recommendation can be accepted as the first global standard on AI ethics, and it emphasises protection of human rights and dignity, transparency, fairness, human oversight, and responsibility to ensure AI serves inclusive, sustainable, and peaceful objectives (UNESCO, 2022). The European Union's High-Level Expert Group on AI also set out seven requirements for trustworthy AI, such as human agency, privacy, non-discrimination, transparency, well-being, and accountability (High-Level Expert Group on Artificial Intelligence [AI HLEG], 2019). The upcoming EU AI Act embodies these values by aiming for AI that is safe, transparent, traceable, non-discriminatory, and environmentally friendly, with human oversight to prevent harmful outcomes (Regulation (EU) 2024/1689, 2024).

The difficulties in applying these principles, which are mentioned in many regulations and policies, have been noted in academic discussions. Coeckelbergh (2020) highlights the difficulties in effectively integrating "ethics by design" into the creation of artificial intelligence systems by pointing out the substantial operational gap between abstract ethical concepts and their actual application. To make these abstract principles more concrete and applicable to AI developers, researchers in the MIS field

are continuing to work on realistic guidelines. One approach, as demonstrated by Siau et al. (2022), is value-focused thinking, which can be defined as a qualitative method to identify fundamental objectives and means for ethical AI in organisations. These efforts essentially aim to clarify the ethical responsibilities of AI and minimise its social impacts. This will maximise ethical AI development. Essentially, these efforts in the literature provide the theoretical foundations for AI deployment while simultaneously integrating ethical values and legal obligations.

One of the most discussed topics in the literature related to AI integration is algorithmic bias and fairness. Algorithmic bias refers to systematic and repeatable errors in a computer system that create unfair outcomes, such as privileging one arbitrary group of users over others, often arising when historical social inequities are encoded into training data or model objectives (Friedman & Nissenbaum, 1996; Noble, 2018). For example, Sweeney (2013) found that regardless of a person's actual criminal record, online advertising algorithms have learnt to link black-identifying names to criminal activity and were displaying ads for arrest records much more frequently than for white-identifying names. A similar situation was later substantiated in another study by explaining that gender-based biases exist in artificial intelligence applications and that a man and a woman are represented with biases arising from social gender approaches (Bölükbaşı et al., 2016). Legal experts such as Barocas and Selbst (2016) have warned that without special interventions, the naive use of data mining of historical data will result in automated disparate impact, which increases the discrimination under the apparel of objective algorithmic efficiency.

Another significant topic is AI transparency and explainability. Unlike traditional MIS, which prioritised interpretable reporting for human decision-making, modern AI-driven systems operate as black boxes, and many users do not have the opportunity to access reasoning to see how predictions were generated (Rai, 2020). Such situations create important ethical and practical liabilities because stakeholders face difficulties in challenging or auditing algorithmic decisions (Burrell, 2016). That's why, in the literature, explainable AI (XAI) has emerged as an important research area that seeks to make AI systems more accountable. As Shin (2021) demonstrates, enhancing transparency through mechanisms such as feature importance visualisation or revealing data characteristics is essential for fostering user trust and perceived fairness.

In addition, data privacy is one of the leading topics of discussion that creates concern in this area. The fact that artificial intelligence systems need very large data sets to make inferences is discussed from many perspectives, such as data protection, open consent, and misuse of shared data. Researchers point out that AI can erode privacy in a variety of ways,

including the mass surveillance capabilities of advanced analytics, the aggregation of data from different sources, and the possibility of re-identification of individuals even in anonymised datasets (Ghosh, 2025). Besides, Ananny & Crawford (2016) and Floridi et al. (2018) argue for well-defined policies and governance measures to safeguard users in AI contexts. In short, considering studies in the literature, protecting data privacy, and ensuring transparency are stated as prerequisites for ethical integration of AI into information systems.

Additionally, the literature review shows that the legal experts have begun to explore how existing laws apply to AI and what new legal concepts might be needed. In this area, one of the most popular topics is liability for AI decisions. Traditional legal frameworks assign responsibility to individuals or organisations. AI challenges this traditional structure when autonomous systems cause harm or make wrong decisions: who is at fault? The answer for this question is still not clear. Legal experts have discussed several different ways to answer this question, including treating AI as a product (Vladeck, 2014; Buiten, 2024), necessitating new insurance arrangements (Bertolini, 2013; Faure & Li, 2022) and even recognising AI as having a type of legal personality in very limited settings (Pagallo, 2013; Moeliono & Simanjuntak, 2024).

Overall, in light of these findings, it can be said that the literature review shows that AI-driven MIS solutions have created and continue to create paradigm shifts in both socio-technical and socio-economic terms. Classic MIS theories are evolving into new theories of human-AI collaboration. Rather than fully autonomous systems, several scholars agree with the use of hybrid models in which AI augments human judgement while ultimate decisions are still under human control. The main reasons for the tendency to preserve the human-based approach are ethical reasoning, which is related to preserving human agency, and practical considerations, which are related to how combining computational power with human context awareness can improve outcomes. As a result, current academic debates frequently concentrate on how to find the correct balance between harnessing AI's strengths and reducing its weaknesses through human oversight.

3. ETHICAL IMPLICATIONS

When discussing the ethical implications of integrating AI into MIS, diverse considerations are necessary. Mittelstadt et al. (2016) state that ethical implications of AI encompass complex issues of fairness, autonomy, transparency, and beyond. Therefore, the term ethics related to this field must be considered in evaluating both the design and use of AI (Dignum, 2019). Ethical rules, unlike laws, evaluate what is right and wrong through the lens of society, and they represent the norms related to

truths. Unlike laws, there is no compulsion in the application of ethics. AI-driven MIS solutions must navigate these norms to maintain public trust and do no harm. In this part several key ethical concerns are examined: algorithmic bias and fairness, transparency and explainability, privacy, autonomy and human agency, and accountability. These categories are interrelated and often overlapping, but it is important to examine each of them, as together they capture the primary moral questions posed by AI in organisational decision-making.

3.1. Algorithmic Bias and Fairness

The potential of algorithmic bias is a major ethical issue in AI-driven Management Information Systems (MIS), as machine learning algorithms commonly duplicate or amplify previous biases discovered in training data. This data bias causes discriminatory consequences that oppose protected groups in high-stakes domains such as recruitment, credit scoring, and criminal justice (Barocas & Selbst, 2016; Mehrabi et al., 2021). Such a situation is often characterised as "garbage in, garbage out". In addition to data quality, these inequalities are made worse by the lack of diversity in AI development teams. When engineering teams are made up of people from the same background, they may miss important details about how models will work in different situations because the developers do not have enough real-world experience (West et al., 2019).

Because of the relationship between ethics and the social and cultural sphere, eliminating algorithmic biases requires an approach shaped by different perspectives that includes not only technical regulations but also social governance. While technical interventions, such as preprocessing data to ensure representation or applying fairness constraints during training, are essential, scholars argue they must be paired with interdisciplinary audits and a human-in-the-loop perspective to ensure accountability (Raji et al., 2020). Furthermore, there is an agreement in the literature that diversifying AI teams and incorporating participatory design methods are critical to shifting the focus from efficiency to the ethical imperative of justice. Such diversification and incorporation can prevent automated systems from exacerbating existing societal inequalities (Costanza-Chock, 2020; Leslie et al., 2021).

3.2. Transparency and Explainability

Transparency and explainability are essential conditions for an AI integration to be considered ethical. The main reason why these two features are considered prerequisites for ethical AI is that the algorithms have a complex structure, and this creates a black box problem (Burrell, 2016; Rai, 2020). This black box mystery created by AI algorithms for users poses serious ethical risks. Users cannot access the errors, shortcomings, and, in some cases, the roots of discriminatory biases in

content generated by AI that are not transparent and explainable (Ananny & Crawford, 2016; Mittelstadt et al., 2016). Ghosh (2025) and Coeckelbergh (2020) argue that without visibility into how decisions are made, stakeholders cannot effectively challenge unjust outcomes, which violates fundamental rights to due process and autonomy. Consequently, scholars emphasise the need to move from "black box" models to "glass box" frameworks, where decision-making logic is either inherently interpretable or made understandable through post-hoc auditing methods (Rai, 2020).

To mitigate these risks, recent research and regulatory frameworks focus on technical and legal aspects to enforce transparency. Rai (2020) notes that techniques such as local interpretable model-agnostic explanation (LIME) have emerged to provide post-hoc explanations that approximate the decision logic of complex models so that it aids in the detection of bias. Furthermore, Shin (2021) argues that causability is a critical condition for creating user trust and confidence in AI systems since it works to the extent that an explanation provides a causal understanding of a decision. Additionally, Buiten (2024) warns that opacity complicates product liability claims, as proving a defect in an unclear AI system is legally problematic in the absence of mandatory disclosure. To address this, the EU AI Act explicitly mandates transparency obligations, such as requiring high-risk systems to be traceable and informing users when they interact with AI, codifying ethical transparency into binding law (AI HLEG, 2019; Regulation (EU) 2024/1689).

3.3. Privacy and Data Protection

Privacy concerns have become one of the most ethically concerned issues today with the integration of AI into information MIS. Personal data has a key importance for the AI-driven MIS solutions. It does not matter whether it is a retailer analysing shopping habits to personalise ads, a hospital processing patient records for diagnoses, or an HR department tracking employee performance. From an ethical perspective, it can be said that privacy is actually about individuals managing their own information and preventing this information from being used under undesirable conditions. This goes beyond mere data protection. It is a matter of human dignity and autonomy. When AI systems manage this data irresponsibly, they risk not only violating these fundamental rights but also causing tangible harm through the exposure of sensitive private information. There are multiple different dimensions related to the privacy implications of AI in MIS:

3.3.1. Data Collection and Consent Dilemma

The operational logic of modern AI systems is frequently predicated on the extensive extraction of behavioural data, a phenomenon

Zuboff (2019) characterises as "surveillance capitalism". In this context, the integration of AI into new generation information systems has crossed a significant threshold in disclosing data that individuals do not want to share about themselves. Kosinski et al. (2013) acknowledge that integrating diverse data sources enables organisations to create predictive profiles that frequently reveal sensitive characteristics far beyond what individuals would like to divulge. While the principle of ethics of informed consent remains the theoretical foundation of data governance, researchers claim that the conventional "notice-and-consent" structure is effectively old-fashioned (Andreotta et al., 2022; Solove, 2024). The currently existing mechanisms for obtaining informed consent are not sufficiently clear. Standard compliance mechanisms, such as privacy policies or simple checkboxes in the websites, fail to account for the limited rationality of users, who lack the cognitive capacity to assess the complex risks of algorithmic processing (Acquisti et al., 2015). As a result, critics warn that existing data practices frequently resemble privacy theatre, in which performative adherence to legal gaps conceals a systemic erosion of actual user autonomy.

3.3.2. Data Protection and Purpose Limitation

Once collected, the centralisation of massive datasets required for deep learning creates significant security vulnerabilities, making AI repositories into high-value targets for cyberattacks. Beyond security, the ethical principle of purpose limitation, a core tenet of the General Data Protection Regulation (GDPR), dictates that data collected for one context cannot be arbitrarily repurposed for another (Regulation (EU) 2016/679, 2016). However, AI's "data-hungry" nature conflicts with the notion of data minimisation, frequently resulting in function creep, in which sensitive data (e.g., health records) is used for secondary purposes (e.g., commercial marketing) without explicit consent (Koops, 2021). Although the main negativity of such practices is related to the violation of legal frameworks, there is also a side effect. They violate the contextual integrity of the user's trust by shifting the flow of information outside of the rules applicable to the original transaction (Nissenbaum, 2011).

3.3.3. Re-identification Risks and The Illusion of Anonymity

While organisations frequently rely on anonymisation to mitigate privacy risks, recent works demonstrate that traditional de-identification techniques are increasingly ineffective against modern machine learning capabilities. Rocher et al. (2019) evaluated this risk and predicted that 99.98% of Americans could be successfully re-identified in any available anonymised dataset using only 15 demographic attributes. This phenomenon happens when AI models use different datasets to recreate individual identities (Ohm, 2010). As a result, anonymisation is accepted

as a process that has lost its credibility in the literature. The continued reliance on anonymisation in society actually creates a false sense of security.

To sum up, all these three dimensions are strongly related to privacy and data collection. To provide effective privacy protection in the age of AI, it is critical to go beyond static compliance and incorporate protection throughout an AI system's full lifecycle, from initial data collecting to ultimate deployment. This requires a dual approach: using advanced technical solutions such as differential privacy and federated learning to reduce data exposure while implementing strong governance frameworks which require proportionality in surveillance. Finally, preserving privacy is not only a legal requirement for permission and data rights but also a fundamental ethical duty for upholding human dignity and maintaining public trust in management information systems.

3.4. Autonomy and Human Agency

The integration of AI into decision-making processes poses a significant challenge to human autonomy. Human autonomy can be ethically defined as the capacity of individuals to make informed, uncoerced decisions about their lives (Beauchamp & Childress, 2019; Rubel et al., 2021). As MIS architectures evolve from data repositories to decision support systems with today's developments, changes in existing control dynamics are inevitable. Floridi et al. (2018) believe that retaining human agency is a critical ethical necessity for AI society, guaranteeing that we do not hand over decision-making authority to black-box algorithms, turning humans into passive data subjects rather than moral agents.

This tension is most clear in high-stakes professional settings, like healthcare. AI diagnostic tools can see patterns better than ever before, but there is a real moral concern that relying too much on these systems could lead to deskilling, which is when professionals slowly lose the ability to make their own decisions. Jiang et al. (2017) note that while AI aims to assist clinicians, there is a potential risk of reducing their active involvement, effectively turning physicians into mere validators of algorithmic outcomes. Automation bias occurs when professionals uncritically adhere to AI recommendations, and Coeckelbergh (2020) argues that because of it, the holistic, empathetic judgement that defines human care could be eroded.

The threat to autonomy includes not only professionals but also end-users, particularly through the mechanism of algorithmic “nudging”. AI systems designed to influence engagement or modify behaviour can inadvertently or deliberately infringe upon individual autonomy. Leslie et al. (2021) warn that technologies that control people's actions without their

permission threaten the basic ideas of freedom and democracy. The EU AI Act says that AI practices that use subliminal techniques or other sneaky ways to change behaviour in ways that hurt people are unacceptable risks to autonomy (Regulation (EU) 2024/1689, 2024). To reduce these risks, global frameworks advocate for a human-centric approach. There is a consensus that technology should empower individuals rather than diminish their agency. The UNESCO Recommendation on the Ethics of AI says that AI systems must be under real human control so that people can always make the final decisions (UNESCO 2022). This means that human-in-the-loop architecture is needed.

Preserving autonomy hinges on ethical boundaries. As AI capabilities expand, a debate has emerged regarding whether certain judgements must remain exclusively human. Pazzanese (2020) underscores the viewpoint of political philosopher Michael Sandel, who asserts that the role of human judgement constitutes a vital ethical element that cannot be replicated by data processing. As a result, the ethical design of MIS must follow the principle of enhancement rather than substitution. Artificial intelligence should seek to improve human cognitive capabilities and provide evidence, while the final act of judgement must remain distinctly human-based (Cazzaniga et al., 2024; McAfee & Brynjolfsson, 2017).

4. LEGAL IMPLICATIONS

The rapid integration of AI into MIS is also generating legal debate. There are views in the literature that this integration challenges traditional legal systems. Vladeck (2014) and Pagallo (2013) claim that such legal challenges create a regulatory gap where existing statutes struggle to address the autonomy and opacity of machine learning systems. This misalignment has led to a lot of legal confusion, especially over whether AI entities have legal personality or how standard concepts of negligence apply when algorithmic decisions hurt someone (Moeliono & Simanjuntak, 2024; Buiten, 2024). When we look at global legal regulations in response to this situation, it can be seen that rigid regulatory frameworks have been created to eliminate flexibility in order to make this integration compatible with human rights (Leslie et al., 2021). This section examines these legal implications from a global perspective. Beyond specific regional regulations, the broader efforts by international bodies to establish governance standards, such as the OECD's recommendations on AI governance (OECD, 2024), will be analysed. Furthermore, the discussion addresses critical unresolved issues in civil liability and compulsory insurance schemes (Faure & Li, 2022; Bertolini, 2013), as well as the legal concerns related to intellectual property in an era of cross-border algorithmic flows.

4.1. Emerging AI Regulations and Policies

There is now a shift from soft law to hard law, enshrined in binding national legislation, regarding the governance of AI. As Jobin et al. (2019) point out, regulations are shaped by principles such as transparency, fairness, and non-maleficence. However, the implementation of these principles varies significantly across jurisdictions. At this point, I believe multinational organisations should guide AI regulation.

First, the European Union has established itself as the global pioneer in comprehensive AI regulation. The EU AI Act (Regulation (EU) 2024/1689, 2024) represents the world's first omnibus AI law, grounded in a precautionary, risk-based framework. This statute categorises AI systems into four levels of risk:

Unacceptable Risk: Systems deemed a clear threat to fundamental rights, such as social scoring or real-time remote biometric identification in public spaces, are banned outright.

High-Risk: Critical applications (e.g., medical devices, recruitment algorithms, critical infrastructure) are permitted but subject to strict compliance obligations, including data governance, detailed documentation, human oversight, and robustness requirements.

Limited & Minimal Risk: Most AI applications (e.g., spam filters, video games) face minimal restrictions, though systems interacting with humans (like chatbots) must fulfil transparency obligations to ensure users know they are communicating with a machine.

The EU's strategy effectively codifies ethical values into law, supported by significant penalties, such as fines of up to €35 million or 7% of global revenue, resulting in a "Brussels Effect" that establishes a de facto global standard for compliance (Buiten, 2024).

Second, in contrast to the EU's centralised legislation, the United States has traditionally preferred a decentralised strategy aimed at encouraging innovation. There is currently no unified federal AI law; instead, governance is carried out through a patchwork of sector-specific regulations and administrative actions. For example, the AI Bill of Rights (Office of Science and Technology, 2022) and the National Institute of Standards and Technology (NIST) AI Risk Management Framework (2023) offer optional guidance that emphasises safety, privacy, and non-discrimination. More recently, Executive Order 14110 on "Safe, Secure, and Trustworthy AI" signalled a shift towards increased oversight, utilising executive authority to mandate safety tests for dual-use foundation models and directing federal agencies to establish AI procurement and safety standards (The White House, 2023). At the state level, however, legislative action is more robust. For example, Colorado's AI Act (Colorado General

Assembly, 2024) specifically prohibits algorithmic discrimination in high-stakes decisions such as employment and insurance. This results in a mosaic of compliance requirements, with corporations facing stricter responsibility in certain states than at the federal level (Qian et al., 2024).

Third, China's regulatory framework is distinguished by strict state supervision. Following the New Generation AI Development Plan (State Council of China, 2017), which established the objective of global AI leadership by 2030, China has implemented specific rules ahead of many Western counterparts. Recent rules are explicitly targeting recommendation algorithms (Cyberspace Administration of China (CAC), 2022) and deep synthesis technology (CAC, 2022). These regulations mandate that generative AI services adhere to basic socialist ideals, practise strong content management, and register algorithms with the Cyberspace Administration of China (CAC, 2023). While strict on content and political alignment, China also fosters industrial progress, aiming for a balance in which AI thrives within the confines of state-guided ethics.

Furthermore, international organisations play an important role in harmonising these different approaches. The OECD AI Principles emphasise stewardship and trustworthiness, which influence G20 policies (OECD, 2024). Similarly, the G7's Hiroshima AI Process seeks to create a code of conduct for advanced AI developers (G7, 2023). The Recommendation on the Ethics of Artificial Intelligence is a normative framework approved by 193 member nations that prioritises human rights and environmental sustainability (UNESCO, 2022).

4.2. Liability and Accountability in Law

Another issue legal scholars debate regarding the integration of AI into computing is liability. Who is responsible for autonomous AI systems? Attributing liability for harm caused by autonomous AI systems presents a significant legal challenge because traditional tort and product liability frameworks are often inadequate to address the unique complexities of machine learning. Unlike conventional product defects, errors in AI, whether resulting from opaque black box decision-making or post-deployment learning, blur the traditional lines of responsibility between developers, data providers, and end-users (Vladeck, 2014). According to Bertolini (2013), the autonomy and unpredictability of these systems strain conventional legal concepts of negligence, posing significant evidential challenges for victims attempting to prove responsibility or pinpoint a single defect within complex algorithmic designs.

In response to these accountability gaps, regulatory frameworks, particularly in the European Union, are evolving to find a solution for liability claims. Buiten (2024) argues that current guidelines seek to establish a presumption of causality for high-risk AI, essentially shifting

the burden of proof to providers to demonstrate that their systems were not inadequate. To avoid the problem of many hands, legislation such as the EU AI Act requires strict human-in-the-loop governance, which ensures that legal accountability remains anchored in human decision-making rather than being transferred to technical systems (Regulation (EU), 2024/1689; Raji et al., 2020). The reality of the ever-increasing autonomy of artificial intelligence is undeniable. Despite AI's increasing autonomy, the legal community has strongly opposed the concept of AI personhood. There is a consensus that responsibility must ultimately belong to the natural or corporate entities who implement the technology (Moeliono & Simanjuntak, 2024; Pagallo, 2013).

As a result, businesses remain liable for algorithmic results such as unintentional discrimination or differential impact caused by biased data (Barocas & Selbst, 2016). To address these legal and ethical issues, the literature recommends a complete governance framework that goes beyond financial hedging. First, scholars stress the importance of shifting from opaque models to Explainable AI (XAI) or glass box frameworks in order to be sure that users can articulate decision logic and detect errors before they do harm (Rai, 2020; Shin, 2021). Second, mitigation must begin at the design phase with inclusive methods like design justice by involving multiple stakeholders in identifying possible harms for marginalised groups early in the development lifecycle (Costanza-Chock, 2020; Dignum, 2019). Finally, these efforts should be supported with end-to-end algorithmic auditing to ensure continuous compliance (Raji et al., 2020) and the implementation of mandatory insurance schemes to address the financial uncertainties because of unavoidable AI-driven harms (Faure & Li, 2022).

4.3. Data Protection and AI

Current laws constitute a significant framework for AI-powered MIS. Integrating AI into these systems fundamentally results in the use of personal data. When we look at the legal frameworks related to this outcome, we can say that one of the most influential is the European Union's General Data Protection Regulation (GDPR), which is a pioneer in this area. GDPR is legislation that regulates how data is collected, processed, and used and imposes strict obligations (Qian et al., 2024).

The primary operational requirement of artificial intelligence is the existence of big data sets. Related to this, there is a strong discussion between this requirement and legal principles such as purpose limitations and data minimisation. According to Barocas and Selbst (2016), the exploratory character of data mining, in which correlations and patterns arise after collection, frequently conflicts with the legal necessity of stating explicit processing aims in advance. As a result, organisations must create

a legal basis for the processing of data. Every user or customer must be provided with a guarantee which ensures that data initially gathered for one service is not unlawfully repurposed for AI training without valid consent or a compatible legitimate interest.

When we examine the GDPR, we see that this regulation grants very strong rights to individuals who share data. For example, individuals sharing data are protected against the automated decision-making, which is a core architecture of artificial intelligence (Regulation (EU) 2016/679, 2016). Such a situation creates a legal debate on how to interpret it. Mittelstadt et al. (2016) suggest that, while the scope of a right to explanation is uncertain, there is a clear obligation to provide data subjects with relevant information about the reasons behind high-stakes actions. This requires organisations to avoid opaque black box models in important areas such as employment or credit scoring, which frequently necessitates human-in-the-loop measures to maintain accountability and auditability (Raji et al., 2020).

Beyond such procedure, data protection rules have become increasingly linked with questions of fairness and accuracy. Processing biased data that results in discriminatory profiling may be seen as a violation of the fairness principle in data processing. As Sweeney (2013) notes, algorithmic biases are rooted in historical patterns. These historical patterns are present in the datasets used to train AI. The algorithmic biases that emerge from such patterns negatively impact AI-based information systems, essentially creating a strong need for a legal regulatory backdrop. To address these risks, Leslie et al. (2021) emphasise that privacy must be viewed as a fundamental human right. Dignum (2019) also argues that "Privacy by Design" approaches must be followed, where security measures and compliance officers are integrated into the AI development lifecycle from the outset.

4.4. Intellectual Property and AI

Before concluding the legal discussions, it's also beneficial to focus on the debates surrounding intellectual property. Intellectual property issues are currently overshadowed by ethical and other legal issues in current laws and regulations. However, the integration of artificial intelligence into management information systems carries the potential to create numerous issues regarding intellectual property. The generative capabilities of AI have implications that are difficult to discuss in this area. We can address uncertainties related to various issues such as copyright, patenting, and data ownership.

4.4.1. Copyright in AI-Generated Works

A primary jurisprudential debate concerns the ownership of AI outputs. In most jurisdictions, copyright statutes are predicated on human creativity. For example, in the landmark U.S. decision Thaler v. Perlmutter (2023), the court declared that works made solely by artificial intelligence without human participation are ineligible for copyright protection because human authorship is a fundamental element of the law. Based on this example, it's clear that this situation poses a strategic risk for MIS. If an individual or organisation uses AI or an AI-based MIS for software development, marketing reports, or business designs, the outputs generated could actually be considered public property when assessed legally. While some jurisdictions like the UK offer a computer-generated works provision (attributing authorship to the person who made the arrangements for the AI), the global standard currently sees AI as a tool without legal personality or authorship rights (Moeliono & Simanjuntak, 2024).

4.4.2. Copyright and Training Data

Looking at the other side of the equation, discussions of intellectual property in AI inputs are just as important as discussions of intellectual property in AI outputs. How would this be assessed from an intellectual property perspective if AI tools were trained using copyrighted materials? This has resulted in a wave of lawsuits about whether such data acquisition constitutes infringement or falls under exceptions such as fair use in the United States or text and data mining in the European Union. According to Samuelson (2023), the resolution of these conflicts will significantly impact the AI economy; if training is found to be infringing, MIS architectures that rely on scraped data may face existential legal obligations. The European Union attempted to find a solution with the Digital Single Market Directive, which includes a text and data mining exception for research but permits rights holders to opt out of having their data used for commercial AI training (Directive (EU) 2019/790, 2019). In addition, the EU AI Act requires artificial intelligence developers to publish detailed reports on the data they trained their systems on in order to address copyright concerns of third-party individuals and companies (Regulation (EU) 2024/1689, 2024).

4.4.3. Patents, Trade Secrets, and the Transparency Paradox

When we look at patent debates, we see similar results to the case of intellectual property. Patent offices worldwide do not recognise AI as an inventor. Just as with copyright, patent law requires a human inventor to be named, meaning companies must attribute AI-assisted discoveries to human teams to secure protection (Moeliono & Simanjuntak, 2024). A more significant tension arises between trade secret law and the moral duty for transparency. Companies try to protect their algorithms as trade secrets to maintain a competitive advantage. However, this legal protection

conflicts with explainable AI requirements, which necessitate that the black box be opened for inspection (Rai, 2020). In the current legal system, companies have to make a two-option choice: they can maximise legal secrecy (trade secrets) or maximise trust and regulatory compliance (transparency), but achieving both simultaneously is legally and technically difficult.

5. CONCLUSION

The integration of artificial intelligence into management information systems represents a paradigm shift that extends far beyond technical optimisation. This integration process shapes the decision-making processes of institutions in both ethical and legal terms. As this chapter has shown, deploying AI-driven MIS solutions includes a complicated duality: although it provides important opportunities for data analysis and automation, it also poses systemic concerns such as bias, opacity, and the erosion of human agency. The ethical analysis emphasises that the efficiency of black box algorithms cannot be at the expense of transparency and justice. Whether tackling the illusion of anonymity in data privacy or limiting the hazards of algorithmic discrimination, it is obvious that ethical AI demands a change from passive compliance to proactive design which ensures that systems are explicable, equitable, and respectful of human autonomy.

When we look at this integration and technological developments from a legal perspective, we see that regulations and legal processes have begun in different countries. The worldwide regulatory framework is fast developing. There is a rapid transition from voluntary soft law guidelines to enforced hard law regulations, as demonstrated by the risk-based approach of the EU AI Act. This transition signals that accountability is no longer optional. The legal uncertainties related to accountability for autonomous harms, the protection of intellectual property in generative works, and the requirements for data protection are converging into a stringent compliance framework. Organisations can no longer claim ignorance of the accountability gap because new legal principles, such as the presumption of causality and mandatory human oversight, are effectively eliminating gaps that formerly permitted responsibility shifts to machines.

The ethical and legal issues discussed in this section constitute a strategic governance framework for MIS professionals. Addressing ethical issues and legal obligations will be a fundamental factor in the success of this integration. The framework attempted to present in this section illustrates the necessity of governance and technology evolving together from a socio-technical perspective. Because both legal and ethical considerations are addressed as core functional features through the socio-

technical approach, it becomes possible for MIS professionals to go beyond ad hoc measures to integrate privacy-by-design principles into integration processes, conduct routine algorithmic audits, and institutionalise human-in-the-loop protocols for high-stakes decisions. By using this strategic approach, companies may do more than just avoid liability: they can create AI systems that are legally strong, ethically sound, and worthy of public trust, fulfilling the technology's promise as a tool for empowerment rather than a mechanism of unchecked control.

6. ACKNOWLEDGEMENT

I would like to express my gratitude to my spouse, Deniz ALTIOK ERDURAN, for her unwavering support during the preparation of this work.

7. CONFLICT OF INTEREST STATEMENT

There is no conflict of interest regarding the publication of this chapter.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Agrawal, A., Gans, J., & Goldfarb, A. (2018). *Prediction machines: The simple economics of artificial intelligence*. Harvard Business Review Press.

Ananny, M., & Crawford, K. (2016). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, *20*(3), 973–989. https://doi.org/10.1177/1461444816676645 (Original work published 2018)

Andreotta, A. J., Kirkham, N., & Rizzi, M. (2022). AI, big data, and the future of consent. *AI & Society*, *37*(4), 1715–1728. https://doi.org/10.1007/s00146-021-01262-5

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, *104*(3), 671–732. https://doi.org/10.15779/Z38BG31

Beauchamp, T. L., & Childress, J. F. (2019). *Principles of biomedical ethics* (8th ed.). Oxford University Press.

Bertolini, A. (2013). Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules. *Law, Innovation and Technology*, *5*(2), 214–247. https://doi.org/10.5235/17579961.5.2.214

Bölükbaşı, T., Chang, K. W., Zou, J. Y., Saligrama, V., & Kalai, A. T. (2016). Man is to computer programmer as woman is to homemaker? Debiasing word embeddings. *Advances in Neural Information Processing Systems*, *29*, 4349–4357. https://doi.org/10.48550/arXiv.1607.06520

Buiten, M.C. (2024) Product liability for defective AI. *Eur J Law Econ* 57, 239–273. https://doi.org/10.1007/s10657-024-09794-z

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

Cazzaniga, M., Jaumotte, F., Li, L., Melina, G., Panton, A. J., Pizzinelli, C., Rockall, E. J., & Vengoechea, M. M. (2024). *Gen-AI: Artificial intelligence and the future of work* (Staff Discussion Note SDN/2024/001). International Monetary Fund. https://www.imf.org/en/Publications/Staff-Discussion-

Notes/Issues/2024/01/14/Gen-AI-Artificial-Intelligence-and-the-Future-of-Work-542379

Cockburn, I. M., Henderson, R., & Stern, S. (2018). *The impact of artificial intelligence on innovation* (National Bureau of Economic Research Working Paper No. 24449). National Bureau of Economic Research. https://doi.org/10.3386/w24449

Coeckelbergh, M. (2020). *AI Ethics*. The MIT Press. https://mitpress.mit.edu/9780262538190/ai-ethics/

Colorado General Assembly. (2024). *Senate Bill 24-205: Consumer protections for artificial intelligence*. https://leg.colorado.gov/bills/sb24-205

Costanza-Chock, S. (2020). *Design justice: Community-led practices to build the worlds we need*. The MIT Press. https://doi.org/10.7551/mitpress/12255.001.0001

Cyberspace Administration of China (CAC). (2022). *Internet information service algorithmic recommendation management provisions*. http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm

Cyberspace Administration of China (CAC). (2022). *Provisions on the administration of deep synthesis of internet information services*. http://www.cac.gov.cn/2022-12/11/c_1672221949318230.htm

Cyberspace Administration of China (CAC). (2023). *Interim measures for the management of generative artificial intelligence services*. https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

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

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC. (2019). *Official Journal of the European Union, L 130*, 92–125. http://data.europa.eu/eli/dir/2019/790/oj

Faure, M., & Li, S. (2022). Artificial intelligence and (compulsory) insurance. *Journal of European Tort Law*, *13*(3), 233–277. https://doi.org/10.1515/jetl-2022-0001

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's 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

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A., & Srikumar, M. (2020). *Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI*. Berkman Klein Center for Internet & Society. https://dash.harvard.edu/handle/1/42160420

Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerisation? *Technological Forecasting and Social Change*, *114*, 254–280. https://doi.org/10.1016/j.techfore.2016.08.019

Friedman, B., & Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems*, *14*(3), 330–347. https://doi.org/10.1145/230538.230561

G7. (2023). *Hiroshima process international code of conduct for organizations developing advanced AI systems*. mofa.go.jp/files/100573473.pdf

Gartner. (2025, September 17). *Gartner says worldwide AI spending will total $1.5 trillion in 2025* [Press release]. https://www.gartner.com/en/newsroom/press-releases/2025-09-17-gartner-says-worldwide-ai-spending-will-total-1-point-5-trillion-in-2025

Ghosh, M. (2025). Artificial intelligence (AI) and ethical concerns: a review and research agenda. *Cogent Business & Management*, *12*(1). https://doi.org/10.1080/23311975.2025.2551809

High-Level Expert Group on Artificial Intelligence (AI HLEG). (2019). *Ethics guidelines for trustworthy AI*. European Commission. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., Wang, Y., Dong, Q., Shen, H., & Wang, Y. (2017). Artificial intelligence in healthcare: Past, present and future. *Stroke and Vascular Neurology, 2*(4), 230–243. https://doi.org/10.1136/svn-2017-000101

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

Koops, B.-J. (2021). The concept of function creep. *Law, Innovation and Technology*, *13*(1), 29–56. https://doi.org/10.1080/17579961.2021.1898299

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802–5805. https://doi.org/10.1073/pnas.1218772110

Leslie, D., Burr, C., Aitken, M., Cowls, J., Katell, M., & Briggs, M. (2021). *Artificial intelligence, human rights, democracy, and the rule of law: A primer*. The Alan Turing Institute. https://edoc.coe.int/en/artificial-intelligence/10206-artificial-intelligence-human-rights-democracy-and-the-rule-of-law-a-primer.html

McAfee, A., & Brynjolfsson, E. (2017). *Machine, platform, crowd: Harnessing our digital future*. W. W. Norton & Company.

Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM Computing Surveys*, *54*(6), 1–35. https://doi.org/10.1145/3457607

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), 1–21. https://doi.org/10.1177/2053951716679679

Moeliono, T. P., & Simanjuntak, M. B. B. (2024). Legal personality of artificial intelligence. *Melintas*, *40*(2), 174–196. https://doi.org/10.26593/mel.v40i2.8648

National Institute of Standards and Technology (NIST). (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

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48. https://doi.org/10.1162/DAED_a_00113

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press. https://doi.org/10.2307/j.ctt1pwt9w5

Office of Science and Technology Policy. (2022). *Blueprint for an AI Bill of Rights*. The White House. https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, *57*, 1701–1777.

Organisation for Economic Co-operation and Development (OECD). (2024). *Recommendation of the Council on artificial intelligence*

(OECD/LEGAL/0449). OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

Pagallo, U. (2013). *The laws of robots: Crimes, contracts, and torts*. Springer. https://doi.org/10.1007/978-94-007-6564-1

Pazzanese, C. (2020, 26 Ekim). Ethical concerns mount as AI takes bigger decision-making role in more industries. *Harvard Gazette*. https://news.harvard.edu/gazette/story/2020/10/ethical-concerns-mount-as-ai-takes-bigger-decision-making-role/

Rai, A. (2020). Explainable AI: From black box to glass box. *Journal of the Academy of Marketing Science*, *48*, 137–141. https://doi.org/10.1007/s11747-019-00710-5

Raji, I. D., Smart, A., White, R. N., 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* (pp. 33–44). ACM. https://doi.org/10.1145/3351095.3372873

Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016). *Official Journal of the European Union*, L119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. (2024). *Official Journal of the European Union*, *L*, 2024/1689. http://data.europa.eu/eli/reg/2024/1689/oj

Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*, *10*(1), 3069. https://doi.org/10.1038/s41467-019-10933-3

Rubel, A., Castro, C., & Pham, A. (2021). *Algorithms and autonomy: The ethics of automated decision systems*. Cambridge University Press. https://doi.org/10.1017/9781108895057

Samuelson, P. (2023). Generative AI meets copyright. *Science, 381*(6654), 158–161. https://doi.org/10.1126/science.adi0656

Shin, D. (2021). The effects of explainability and causability on perception, trust, and adoption of explainable artificial intelligence. *International Journal of Human-Computer Studies*, *157*, 102712. https://doi.org/10.1016/j.ijhcs.2020.102551

Siau, K., Nah, F. F.-H., Eschenbrenner, B., Chen, L., & Qian, Y. (2022). AI in accounting: A value-focused thinking study. In *PACIS 2022*

proceedings (pp. 1–4). Association for Information Systems. https://ink.library.smu.edu.sg/sis_research/9966

Solove, D. J. (2024). Murky consent: An approach to the fictions of consent in privacy law. *Boston University Law Review*, *104*(3), 593–660. https://www.bu.edu/bulawreview/files/2024/04/SOLOVE.pdf

State Council of China. (2017). *New generation artificial intelligence development plan*. https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm

Sweeney, L. (2013). Discrimination in online ad delivery. *Communications of the ACM*, *56*(5), 44–54. https://doi.org/10.1145/2447976.2447990

Thaler v. Perlmutter. (2023). *Case No. 1:22-cv-01564* (D.D.C. Aug. 18, 2023). copyright.gov/ai/docs/district-court-decision-affirming-refusal-of-registration.pdf

The White House. (2023). *Executive Order 14110: Safe, secure, and trustworthy development and use of artificial intelligence*. Federal Register. https://www.federalregister.gov/d/2023-24283

United Nations Educational, Scientific and Cultural Organization (UNESCO). (2022). *Recommendation on the ethics of artificial intelligence*. https://unesdoc.unesco.org/ark:/48223/pf0000381137

Vladeck, D. C. (2014). Machines without principals: Liability rules and artificial intelligence. *Washington Law Review*, *89*(1), 117–150. https://digitalcommons.law.uw.edu/wlr/vol89/iss1/6

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

West, S. M., Whittaker, M., & Crawford, K. (2019). *Discriminating systems: Gender, race and power in AI*. AI Now Institute. https://ainowinstitute.org/publication/discriminating-systems-gender-race-and-power-in-ai-2

Qian, Y., Siau, K. L., & Nah, F. F. (2024). Societal impacts of artificial intelligence: Ethical, legal, and governance issues. *Societal Impacts*, *3*, 100040. https://doi.org/10.1016/j.socimp.2024.100040