OPEN ACCESS

Volume: 3

Issue: 4

Month: December

Year: 2024

ISSN: 2583-7117

Published: 31.12.2024

Citation:

Mrs. Elavarasi Kesavan "A Review on Ethical and Legal Issues in Artificial Intelligence and Data Privacy" International Journal of Innovations in Science Engineering and Management, vol. 3, no. 4, 2024, pp. 94–99.

DOI:

10.69968/ijisem.2024v3i494-99

A Review on Ethical and Legal Issues in Artificial Intelligence and Data Privacy

Mrs. Elavarasi Kesavan[1]

[1]*Full Stack QA Architect, Cognizant*

Abstract

Existing data governance frameworks are facing issues due to the fast development of generative artificial intelligence (AI), which has garnered international attention. AI regulation is made more challenging by the growing technological complexity and size of data utilization, which also poses problems for the existing legal framework. The literature on ethical and legal concerns related to artificial intelligence and data privacy is reviewed in this article. It concluded that the rapid advancement of AI, particularly generative models, presents significant ethical and legal challenges related to data privacy, security, and personal rights. As AI increasingly relies on vast amounts of personal data, risks such as data leakage, misuse, and cyberattacks escalate. Existing privacy regulations struggle to keep pace with evolving technologies, highlighting the urgent need for robust frameworks, interdisciplinary collaboration, and ethical foresight. Addressing these concerns requires a balanced approach that safeguards individual privacy while fostering responsible innovation, ensuring that AI development aligns with societal values and legal protections in the digital age.

Keywords; Generative artificial intelligence (AI), Data leakage, Misuse, Cyberattacks, Ethical and legal issues, etc.

INTRODUCTION

However, when seen both legally and morally, privacy encompasses more than just the management of personal information; it also refers to the individual's control over their intimacy and the preservation of their dignity. The fast and simple benefits of speed and convenience shouldn't come at the expense of privacy. It is necessary to determine whether a data set used for machine learning is directly or indirectly the result of violations of individual or collective privacy rights [1]. While privacy is a significant concern in fields such as labor, transportation, technology, and health, privacy and deep learning are particularly crucial. Furthermore, we do not degrade ourselves by allowing authorities to assess a person's social risk using predictive analytics, such as whether they would attempt to get out of jail or even be more likely to commit further (violent) crimes [2]. Since altering one's identity and location is the only way to prevent such a privacy breach, our intelligence would not be artistic. Excellent human intellect operates in a manner that permits a fair allocation of power and freedom [3].

Artificial intelligence (AI) has advanced remarkably in recent years, and its significant effects can be seen in a wide range of industries, from healthcare and finance to transportation and agriculture. In addition to revolutionizing whole sectors, this exponential expansion has ingrained itself into our everyday lives [4]. AI has had a profound impact on society due to its capacity to handle enormous volumes of data and make well-informed judgments. In the future, it may have an impact on almost every facet of our lives. However, protecting individual privacy in the AI age has become a critical worry among the exciting developments in AI technology. Given how heavily AI systems depend on data, the widespread usage of these technologies raises serious concerns about the privacy protection of individuals and the possible exploitation of personal data.

Addressing these privacy issues is crucial given the rapid spread of AI applications, which include but are not limited to virtual assistants, driverless cars, tailored recommendations, and medical diagnostics [5], [6].

Artificial intelligence and its importance

The creation of "smart" machines that can carry out activities that normally require human intellect is the focus of the large field of computer science known as artificial intelligence. In the context of artificial intelligence, intelligence is defined as the ability to do any of the following tasks: "planning, reasoning, problem solving, perception, knowledge representation, creativity", etc. The development of diverse computer systems that can carry out activities that would need human intellect is known as artificial intelligence [7]. This indicates that by using a "non-human" intellect, science was able to guarantee the abolition of mechanical processes. Self-driving vehicles, navigation systems, computer or mobile apps that allow people to connect over the Internet, computer games, etc. are examples of artificial intelligence in action [8].

The efficient use of artificial intelligence is one of the biggest scientific advances and accomplishments of our time. Human-like activities, experience-based learning, and adaptability to new inputs are all made feasible by artificial intelligence (SAS, 2021). In a variety of fields, including economics, law, and technical jargon, science has enabled the use of artificial intelligence to do a variety of jobs [9]. Such an AI programming system is an example of a higher degree of intelligence that has surpassed human ability. The application of artificial intelligence is made between machines or pre-programmed systems. AI also makes it feasible to solve complicated issues between challenging computations and further reduces the likelihood of mistakes since the machine operates based on previously entered data [10], [11].

Figure 1 various ethical and legal conundrums involved with the usage of artificial intelligence in healthcare. [8]

Challenges to Data Privacy in AI

While intriguing, AI raises a number of data privacy concerns. The following are some of the most well-known:

Data Collection on an Enormous Scale: The datasets are often large enough to operate and train AI systems. Businesses use a variety of avenues to collect data, including applications, social media, and Internet of Things sensors. The majority of the time, users are unaware of the extent of the information they are divulging. Long-winded terms and conditions obscure consent mechanisms, leaving users with little power or clarity [12].

Re-identification risks: In a common statement, companies say they anonymize data before using it. Nevertheless, re-identification of individuals from ostensibly anonymous datasets is made possible by developments in data analysis and AI algorithms. For instance, it could be simple to identify someone by fusing publicly accessible information with location data that is considered anonymous [13].

Bias and Discrimination: Only as unbiased as the data they were educated on can AI systems be. The AI model may provide discriminating outcomes if it is given biased data. Algorithms used in employment, for instance, may prejudice against certain groups on the basis of race or gender. Such misuse of data violates the person's right to privacy in addition to causing harm [14].

Cybersecurity Risks: Cyberattacks may target AI systems just as they do any other technology. Vulnerabilities will always be discovered by hackers, who will then exploit them

to get private information like financial or medical records. Data breaches often result in fraud, identity theft, or even the public disclosure of personal data.

Weak Regulation: Artificial intelligence's subtleties are often outside the scope of current privacy rules. Legislators tend to lag behind the rapid advancement of AI technology, and although regulations like the CCPA and GDPR provide guidelines, legal enforcement is far from consistent [15].

Black-Box Nature of AI: AI systems are often mysterious, especially those powered by deep learning. Certain input decisions cannot be traced back. It is challenging to evaluate interpretability in relation to the utilization of data. Misuse and accountability are the problems.

Data Privacy Concerns: Significant privacy concerns are brought up by AI's dependency on massive datasets for both training and operation. Particularly concerning is the use of personal information without express authorization, which may violate privacy regulations [16].

Liability in AI Decision-Making: The issue of accountability for an AI system's choices or acts is becoming more and more relevant. For example, depending on the situation, the user, the software developer, or the manufacturer may be held liable if an AI-driven car is involved in an accident.

Transparency and Explainability Requirements: Lawmakers are increasingly requiring AI systems to be open and transparent, and to provide an explanation for their decision-making processes. In industries where AI judgments have a big influence, like banking and healthcare, this is especially important [17].

Combating AI Bias and Discrimination: Biases in training data may be inherited and amplified by AI systems if they are not properly constructed. Legal issues result from this, particularly when there is discrimination in financing, employment, or law enforcement.

LITERATURE REVIEW

(Al-kfairy et al., 2024) [18] The study integrates viewpoints from a number of fields, such as media, healthcare, and education, and emphasizes the need of AI systems that uphold social justice and do not reinforce existing disparities. The study urges a multidisciplinary discussion between academics, technologists, and politicians to guarantee ethical and responsible AI development that complies with social norms. It makes a substantial contribution to the conversation on handling AI's ethical ramifications in the contemporary digital age by highlighting the need to address these ethical issues immediately and promoting the development of generative AI in a way that is both morally and socially sound. The report outlines many potential avenues for further research while highlighting the theoretical and practical ramifications of these issues.

(Devineni, 2024) [19] The revolutionary effects of artificial intelligence on data security and privacy are examined in this study. In order to have a thorough grasp of AI, a quick analysis of the ethical difficulties is conducted. This includes the following: surveillance energy as a problem, data management challenges, and probable biases, notwithstanding the enormous potential advantages of AI. In addition to restating the key ideas covered, the conclusion highlights the importance of AI in advancing data security and privacy and calls for further study and advancement. This paper aims to give a thorough overview of the key elements of artificial intelligence (AI), emphasizing both the technology's present and future potential in terms of defences against new threats, moral use, and practical solutions that could be created to secure the digital future.

(Joshi & Kharola, 2024) [20] Significant privacy problems are brought up by the widespread use of artificial intelligence (AI) in many industries, necessitating a sophisticated knowledge and calculated approach to privacy protection. This article explores the complex issues of protecting privacy in the era of artificial intelligence, examining the dynamic relationship between privacy rules and technical breakthroughs. AI's ability to gather and analyze vast amounts of data raises privacy concerns, underscoring the need for ethical and open data standards. The paper emphasizes the vital role that strong legal frameworks and decentralized AI platforms play in protecting privacy by looking at case studies and regulatory reactions. In order to achieve a future where AI technologies are researched and used responsibly, with a strong commitment to protecting individual privacy and dignity, it encourages stakeholders to work together to weigh the advantages of AI against privacy rights.

(Solove, 2024) [21] This article tries to provide the groundwork for a fundamental understanding of the relationship between artificial intelligence (AI) and privacy by describing the present threats AI presents to privacy and offering possible paths for future legal development in this field. These privacy issues are often rehashed versions of longer-standing issues. However, AI ingeniously and

intricately reimagines current privacy issues. Existing regulatory frameworks are challenged by the way some issues are combined. Artificial intelligence often makes already-existing issues worse and poses a danger to escalate them to previously unheard-of degrees. In the end, several concerns need to be resolved in order to address the privacy difficulties that AI is causing, whether via updates to existing legislation or as a component of new legislation. Give an outline of the main problems that the legislation has to address in this article, along with advice on which strategies will succeed and which will not.

(Vignesh & Nagarjun, 2024) [22] This study focuses on two important issues that need immediate attention: data privacy and algorithmic accountability. While data privacy focuses on protecting personal information from unethical AI use, algorithmic accountability addresses the need for openness and the capacity to track decision-making processes. The study provides a more convincing explanation of how AI might abuse data and promote prejudices, especially in a vast and varied society like India, in addition to legislative reform. As a result, the study highlights the need of swift and targeted changes to create a solid regulatory framework that considers the complexity of AI. To ensure that AI technologies are created and used responsibly, protecting people's digital rights and trust, this entails putting in place stringent data protection laws and mandatory transparency standards for AI systems.

(Ye et al., 2024) [23] Starting with the training data and concepts of ChatGPT, this essay explores the unique privacy, data leakage, and personal data vulnerabilities associated with generative AI. It also examines the most recent privacy and personal data protection policies in China. According to this article, China's legal system has flaws even if its regulation of privacy and personal data protection uses a private-and-public law integration strategy as well as a macro-micro integration approach. The goal of "trustworthy AI" requires immediate institutional innovation because private law is insufficient to protect data privacy and the current individual control-based personal data protection system is inappropriate for the ways that generative AI processes data.

(Zafar, 2024) [24] The incorporation of artificial intelligence in legal practice is examined in this study, along with the practical and ethical challenges that emerge and how it impacts established legal practices. With an emphasis on bias and transparency, this conversation significantly draws attention to the moral dilemmas raised by the incorporation of artificial intelligence. This strategy is essential to ensuring equity and maintaining openness in all legal procedures. To ensure AI works as a supplement rather than a replacement, the study promotes a "human in the loop" approach that blends human expertise and AI methods to reduce biases and ensure customized legal outcomes. The paper ends by highlighting the importance of maintaining the human element in legal practices.

(Murdoch, 2021) [25] This presents privacy concerns about data security and deployment. Major body: Access, usage, and management of patient data in private hands are among the initial set of problems. Poor privacy protection has been the outcome of several recent public-private collaborations for AI implementation. Greater systemic control of big data health research has been called for as a result. To protect patient agency and privacy, the right measures must be in place. Right now, we are in a similar scenario where monitoring and regulation run the danger of lagging behind the technology they are supposed to regulate. Regulation should promote more complex techniques of data anonymization and protection while highlighting patient agency and permission.

(Stahl, 2021) [26] Explores the moral dilemmas ethical questions brought up by the creation, application, and usage of artificial intelligence. A summary of the (ethical) advantages of AI is presented first, followed by the results of the SHERPA project, which identified what individuals believed to be ethical difficulties via case studies and a Delphi survey. Matters of ethics. Using the previously mentioned classification of AI technology, they are explored. In-depth explanations of ethical concerns are provided. Moral dilemmas brought on by artificial learning both machine learning and artificial general intelligence, as well as more general socio-technical systems, artificial intelligence-based socio-technical systems.

CONCLUSION

In conclusion, the integration of artificial intelligence into data-intensive sectors, particularly those involving personal and sensitive information, raises urgent ethical and legal concerns. AI’s evolving capabilities, especially in self-improvement and generative models like ChatGPT and Sora, pose significant risks to privacy, including data leakage, misuse, and erosion of personal data rights. These challenges are exacerbated by the rapid pace of AI development, often outstripping the formulation of appropriate ethical guidelines and legal frameworks. In fields such as AI-driven marketing and healthcare, the misuse of personal data for profit, cyberattacks, and algorithmic bias intensify these

issues, threatening individual autonomy and societal equity. The interdisciplinary nature of current approaches, while beneficial, may still overlook critical domain-specific ethical dimensions. A robust and comprehensive strategy is essential—combining technological safeguards, organizational accountability, and updated regulatory measures—to protect personal data in the era of AI. As the digital landscape continues to evolve, ensuring transparency, fairness, and privacy in AI systems must be prioritized to align innovation with human rights and ethical governance. Addressing these complexities is imperative to mitigate risks and build a trustworthy, secure future for AI applications.

REFERENCES

[1] R. Rodrigues, "Legal and human rights issues of AI: Gaps, challenges and vulnerabilities," J. Responsible Technol., vol. 4, 2020, doi: 10.1016/j.jrt.2020.100005.

[2] Y. Qian, K. L. Siau, and F. F. Nah, "Societal impacts of artificial intelligence: Ethical, legal, and governance issues," Soc. Impacts, vol. 3, 2024, doi: 10.1016/j.socimp.2024.100040.

[3] D. K. D. S. Nonju and A. B. Ihua-Maduenyi, "The Impact of Artificial Intelligence on Privacy Laws," Int. J. Res. Innov. Soc. Sci., vol. VII, no. 2454, pp. 1175–1189, 2024, doi: 10.47772/IJRISS.

[4] P. Radanliev, "AI Ethics: Integrating Transparency, Fairness, and Privacy in AI Development," Appl. Artif. Intell., vol. 39, no. 1, 2025, doi: 10.1080/08839514.2025.2463722.

[5] H. K. Alhitmi, A. Mardiah, K. I. Al-Sulaiti, and J. Abbas, "Data security and privacy concerns of AI-driven marketing in the context of economics and business field: an exploration into possible solutions," Cogent Bus. Manag., vol. 11, no. 1, p., 2024, doi: 10.1080/23311975.2024.2393743.

[6] S. A. Z. Zaidi, E. Ahmad, and N. Shukla, "Ethical Considerations in the Use of Artificial Intelligence (AI) for Education and Research : A Review," Int. J. Innov. Sci. Eng. Manag., pp. 156–167, 2024, doi: 10.69968/ijisem.2024v3si2156-167.

[7] S. Bouhouita-Guermech, P. Gogognon, and J. C. Bélisle-Pipon, "Specific challenges posed by artificial intelligence in research ethics," Front. Artif. Intell., vol. 6, 2023, doi: 10.3389/frai.2023.1149082.

[8] N. Naik et al., "Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?," Front. Surg., vol. 9, no. March, pp. 1–6, 2022, doi: 10.3389/fsurg.2022.862322.

[9] M. Abdallah and M. Salah, "Artificial Intelligence and Intellectual Properties: Legal and Ethical Considerations," Int. J. Intell. Syst. Appl. Eng., vol. 12, no. 1, pp. 368–376, 2023.

[10] S. Yu, F. Carroll, and B. L. Bentley, "Insights Into Privacy Protection Research in AI," IEEE Access, vol. 12, no. February, pp. 41704–41726, 2024, doi: 10.1109/ACCESS.2024.3378126.

[11] A. Singh and N. Shanker, "Redefining Cybercrimes in light of Artificial Intelligence : Emerging threats and Challenges," pp. 192–201, 2024, doi: 10.69968/ijisem.2024v3si2192-201.

[12] S. Gerke, T. Minssen, and G. Cohen, Ethical and legal challenges of artificial intelligence-driven healthcare. 2020. doi: 10.1016/B978-0-12-818438-7.00012-5.

[13] C. Gilbert and M. A. Gilbert, "The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations," Int. J. Sci. Res. Mod. Technol., no. September, 2024, doi: 10.38124/ijsrmt.v3i9.45.

[14] G. Lupo, The ethics of Artificial Intelligence: An analysis of ethical frameworks disciplining AI in justice and other contexts of application, vol. 12, no. 3. 2022. doi: 10.35295/OSLS.IISL/0000-0000-0000-1273.

[15] S. Bankins and P. Formosa, "The Ethical Implications of Artificial Intelligence (AI) For Meaningful Work," J. Bus. Ethics, vol. 185, no. 4, pp. 725–740, 2023, doi: 10.1007/s10551-023-05339-7.

[16] M. Maiti, P. Kayal, and A. Vujko, "A study on ethical implications of artificial intelligence adoption in business: challenges and best practices," Futur. Bus. J., 2025, doi: 10.1186/s43093-025-00462-5.

[17] M. Karliuk, "Ethical and Legal Issues in Artificial Intelligence," Int. Soc. Impacts Artif. Intell. Technol. Work. Pap, no. 44, 2018, [Online]. Available: https://ssrn.com/abstract=3460095

[18] M. Al-kfairy, D. Mustafa, N. Kshetri, M. Insiew, and O. Alfandi, "Ethical Challenges and Solutions of Generative AI: An Interdisciplinary Perspective," Informatics, vol. 11, no. 3, p. 58, 2024, doi: 10.3390/informatics11030058.

[19] S. K. Devineni, "AI in Data Privacy and Security," Int. J. Artif. Intell. Mach. Learn., vol. 3, no. 1, pp. 35–49, 2024, [Online]. Available:

https://iaeme.com/Home/journal/IJAIML35editor@iaeme.comAvailableonlineathttps://iaeme.com/Home/issue/

[20] N. Joshi and D. M. Kharola, “Emerging Challenges in Privacy Protection with Advancements in Artificial Intelligence,” Int. J. Law Policy, vol. 2, no. 4, pp. 55–77, 2024, doi: 10.59022/ijlp.171.

[21] D. J. Solove, “Artificial Intelligence and Privacy,” SSRN Electron. J., pp. 1–73, 2024, doi: 10.2139/ssrn.4713111.

[22] S. Vignesh and D. N. Nagarjun, “Legal Challenges of Artificial Intelligence in India’s Cyber Law Framework: Examining Data Privacy and Algorithmic Accountability via a Comparative Global Perspective.,” Int. J. Multidiscip. Res., vol. 6, no. 6, pp. 1–12, 2024, doi: 10.4324/9781315552997.

[23] X. Ye, Y. Yan, J. Li, and B. Jiang, “Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective,” Telecomm. Policy, vol. 48, no. 10, p. 102851, 2024, doi: 10.1016/j.telpol.2024.102851.

[24] A. Zafar, “Balancing the scale: navigating ethical and practical challenges of artificial intelligence (AI) integration in legal practices,” Discov. Artif. Intell., vol. 4, no. 1, 2024, doi: 10.1007/s44163-024-00121-8.

[25] B. Murdoch, “Privacy and artificial intelligence: challenges for protecting health information in a new era,” BMC Med. Ethics, vol. 22, no. 1, pp. 1–5, 2021, doi: 10.1186/s12910-021-00687-3.

[26] B. C. Stahl, “Ethical Issues of AI,” Res. Innov. Governance, pp. 35–53, 2021, doi: 10.1007/978-3-030-69978-9_4.

[27] Dubey, P. 2023. The Role of Artificial Intelligence in Modern Human Resource Management: A Review. International Journal of Innovations in Science, Engineering And Management. 2, 4 (Nov. 2023), 59–64. DOI:https://doi.org/10.69968/ijisem.2023v2i459-64.