

Artificial Intelligence, Data Governance, and Legal Accountability in India: A Study in the Post-DPDP Era

Lokanath Patra

Research Scholar (Law), Berhampur University, Berhampur, Odisha, India

lokanath_aisect@rediffmail.com

Abstract: *The data ecosystem has been fundamentally transformed by the rapid integration of Artificial Intelligence (AI) into governance, commerce, and everyday life, thereby raising critical concerns about accountability, transparency, and privacy. The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) in India is a significant regulatory milestone that is designed to regulate the processing of personal data in an increasingly digital society. In the post-DPDP era, this paper investigates the changing relationship between data governance and AI technologies within the Indian legal framework.*

The research critically evaluates how AI-driven systems—characterized by algorithmic decision-making, automated profiling, and large-scale data processing—challenge conventional notions of legal responsibility and regulatory oversight. It assesses the effectiveness of the DPDP Act in solving problems such as algorithmic bias, opacity, assent validity, and cross-border data flows. In addition, the paper examines the role of data fiduciaries, the Data Protection Board, and emergent regulatory strategies to ensure accountability in the deployment of AI systems.

The paper emphasizes regulatory gaps and enforcement challenges in the Indian context by integrating comparative insights from global frameworks such as the General Data Protection Regulation (GDPR) and emergent AI governance models. It argues that a harmonized legal framework that integrates data protection, ethical AI principles, and institutional safeguards is necessary for effective AI governance. The paper concludes with policy recommendations to enhance legal accountability, safeguard individual rights, and promote responsible AI innovation in India's digital economy.

Keywords: Artificial Intelligence, Data Governance, Legal Accountability, Digital Personal Data Protection Act, 2023, Algorithmic Bias, Data Protection Law

I. INTRODUCTION

The digital era of today is distinguished by the unprecedented commodification, processing, and generation of data, which has established it as a critical economic and governance resource. AI has become a transformative force across sectors such as healthcare, finance, governance, and education, thanks to the development of sophisticated computational models and large-scale datasets. The adoption of data-driven technologies in India has been significantly accelerated by the rapid expansion of digital infrastructure, facilitated by initiatives such as Digital India, Aadhaar, and AI-enabled governance platforms.

The magnitude of this transformation has been underscored by recent empirical evidence. The NASSCOM AI Adoption Index (2024–2025) indicates that approximately 87% of Indian enterprises are actively deploying AI



technologies, suggesting pervasive institutional reliance on data-driven systems (Press Information Bureau, 2025). Furthermore, the utilization of AI tools in the professional activities of 92% of knowledge workers in India is significantly higher than the global average, indicating a profound societal integration of AI technologies (IndiaAI, 2024). These trends emphasize the centrality of data ecosystems in shaping India's digital economy.

Simultaneously, the rapid proliferation of AI has exacerbated apprehensions about data governance, surveillance, and privacy. AI systems are heavily reliant on continuous data streams, which often contain personal and sensitive information. Consequently, concerns arise regarding consent, purpose limitation, and ethical data use. Research suggests that the trajectory of AI development is increasingly influenced by data protection frameworks, as organizations are required to ensure that data collection, processing, and model training practices are lawful (EY, 2025). A regulatory framework capable of addressing both technological innovation and individual rights is required, given the interdependence between AI and data governance.

The Supreme Court recognized the right to privacy as a fundamental right under Article 21 in Justice K.S. Puttaswamy v. Union of India (2017), thereby firmly establishing the constitutional foundation for data protection in India. The legality, necessity, and proportionality principles were introduced as benchmarks for state action, and the judgment emphasized informational self-determination. Particularly in the context of state-imposed restrictions on digital access, the significance of proportionality and transparency in digital governance was further underscored by subsequent judicial developments, such as Anuradha Bhasin v. Union of India (2020).

In response to these constitutional imperatives and global regulatory trends, India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), which marks a significant milestone in its digital regulatory framework. The Act establishes a comprehensive framework for the processing of digital personal data, including provisions on data fiduciary obligations, consent, and enforcement mechanisms (MeitY, 2025). Its subsequent operationalization through the DPDP Rules in 2025 represents the transition from legislative intent to enforceable compliance obligations, thereby transforming the responsibilities of both public and private actors in the data ecosystem.

Nevertheless, the emergence of AI introduces complexities that extend beyond the traditional scope of data protection laws, despite these advancements. Automated profiling, adaptive learning mechanisms, and algorithmic opacity ("black-box" decision-making) are frequently used to describe AI systems, which present a challenge to traditional legal and accountability frameworks. For example, the growing reliance on algorithmic decision-making in governance processes is evident in the increasing deployment of AI in areas such as predictive policing, surveillance, and criminal investigations in India (IFEX, 2025).

Additionally, recent legal and policy analyses indicate that the DPDP Act, despite its exhaustive regulation of personal data, fails to adequately protect against AI-specific risks, including algorithmic bias, explainability, and liability for automated decisions. In a data-rich environment where AI systems are increasingly influencing socio-economic outcomes, this regulatory divide becomes particularly significant. The absence of explicit provisions for algorithmic accountability raises concerns regarding the preservation of fundamental rights, discrimination, and fairness.

India has implemented an AI governance framework that is relatively adaptable from a policy standpoint. The IndiaAI Mission's initiatives and the AI Governance Guidelines (2025) underscore the importance of ethical principles, including transparency, accountability, and impartiality. However, these frameworks are primarily non-binding and rely on voluntary compliance, in contrast to stricter regulatory models such as the European Union's General Data Protection Regulation (GDPR) and the proposed AI Act. This results in regulatory asymmetry, as the rapid adoption of technology is not matched by equally robust legal safeguards.



Additionally, AI's dual-use nature—as both an instrument for innovation and a potential vector for harm—increases its complexity. Emerging research is highlighting the risks associated with AI-enabled cyber threats, such as data breaches, deepfakes, and algorithmic manipulation. These threats challenge existing legal frameworks and require new approaches to regulation and accountability. The need for robust governance mechanisms in AI-driven systems is further underscored by the escalating prevalence of data breaches and cyber vulnerabilities.

In light of this, the current investigation endeavors to conduct a critical analysis of the intersection of legal accountability, data governance, and artificial intelligence in India during the post-DPDP era. It is designed to assess the efficacy of the current legal framework in addressing the challenges posed by AI technologies and to investigate the need for a comprehensive regulatory strategy that balances constitutional protections, technological innovation, and data protection.

II. LITERATURE REVIEW

The convergence of legal accountability, data governance, and artificial intelligence (AI) has been the subject of extensive scholarly discourse, particularly in the context of swiftly evolving digital ecosystems. Literature that has been published can be essentially classified into five thematic areas: (i) the evolution of data protection frameworks, (ii) AI governance and accountability, (iii) algorithmic bias and ethical concerns, (iv) Indian legal and policy developments, and (v) comparative regulatory approaches.

A. The Evolution of Data Protection Frameworks in the Era of AI

Scholars have consistently contended that conventional data protection laws are becoming increasingly insufficient to address the intricacies introduced by AI systems. Solove (2021) emphasizes that traditional privacy paradigms, which prioritize individual consent and data control, disregard the collective harms arising from predictive analytics and large-scale data aggregation. Zuboff (2019) similarly conceptualizes the emergence of "surveillance capitalism," in which personal data is commodified, leading to asymmetrical power dynamics between digital corporations and individuals.

Recent research has further underscored that AI systems depend on continuous, dynamic data processing, which challenges fundamental principles such as data minimization and purpose limitation. A 2025 study on AI conducted under the DPDP framework indicates that AI data lifecycles often exceed the initial consent boundaries, complicating compliance with statutory requirements. Moreover, a growing body of research indicates that the DPDP Act may treat publicly available data as personal data, thereby extending AI developers' regulatory responsibilities.

B. Legal Accountability and AI Governance

The issue of accountability in AI systems has emerged as a critical concern in legal scholarship. Accountability, transparency, and explainability are identified as essential components of effective regulatory frameworks in a systematic review of Responsible AI Governance. However, the absence of comprehensive models that address these concerns holistically is also noted.

Recent research conducted in the Indian context has demonstrated that the DPDP Act and other extant legal frameworks, which primarily focus on data protection, are unable to regulate AI-specific operational risks, including algorithmic failures and autonomous decision-making. This results in a substantial regulatory lacuna, particularly in the allocation of liability for AI-driven outcomes.

Additionally, research suggests that AI systems obscure conventional legal distinctions among actors, complicating the assignment of responsibilities among developers, deployers, and users. This "diffusion of accountability" requires the development of new legal doctrines that can effectively resolve distributed liability in algorithmic environments.



C. Social Implications, Ethics, and Algorithmic Bias

The ethical challenges presented by AI, particularly algorithmic bias and discrimination, have been the subject of a significant corpus of literature. O'Neil (2016) refers to algorithmic systems as "weapons of math destruction," illustrating how biased datasets can yield discriminatory outcomes.

These concerns are further substantiated by recent empirical and policy discussions. Experts emphasize that algorithmic bias, data privacy, and user autonomy are critical ethical challenges in the deployment of AI, necessitating immediate regulatory attention. In addition, contemporary research underscores the potential for AI models to perpetuate systemic inequalities, particularly in diverse societies such as India, when they are trained on non-representative datasets.

The necessity of "Indianised datasets" to guarantee contextual accuracy and impartiality in AI systems is further underscored by emerging Indian scholarship. AI models may be unable to accurately represent socio-cultural realities without localized data, thereby increasing the likelihood of biased decision-making.

D. Developments in Indian Law and Policy

The Digital Personal Data Protection Act, 2023, has significantly altered the Indian regulatory landscape. Scholars recognize the Act as a fundamental step toward data governance; however, they criticize its restricted scope in addressing AI-specific issues.

Recent legal analyses contend that the DPDP Act's efficacy in regulating AI-driven systems is restricted by the absence of explicit provisions for algorithmic accountability, transparency, or explainability. In the same vein, research on India's data governance policies indicates that the Act establishes general obligations for data fiduciaries, but it does not provide sector-specific guidelines for high-risk AI applications.

According to policy reports, India has adopted a cautious, adaptable approach to AI regulation. In contrast to the European Union, India has not enacted a specific AI law and continues to rely on sectoral regulations and advisory frameworks. The IndiaAI Mission and AI Governance Guidelines, government initiatives that prioritize ethical principles, are primarily non-binding.

India's framework has been more closely aligned with global standards as a result of recent developments, such as the implementation of the DPDP Rules (2025), which mandate data minimization, user consent, and breach notification. Nevertheless, scholars contend that these measures are insufficient to address the distinctive challenges presented by AI technologies.

E. Global Comparative Perspectives

The comparative literature emphasizes the substantial disparities between global regulatory frameworks and those of India. The proposed AI Act and GDPR of the European Union are comprehensive strategies that integrate AI governance with data protection.

Recent comparative studies have observed that the EU employs a risk-based regulatory model, which involves classifying AI systems according to their potential for injury and imposing more stringent obligations on high-risk applications. Conversely, India's regulatory framework is characterized as "fragmented and evolving," as it lacks a unified approach.

Global scholarship also underscores the significance of incorporating ethical AI principles, including transparency, accountability, and impartiality, into legal frameworks (Floridi et al., 2018). These principles have influenced international regulatory developments and are used as benchmarks for evaluating national frameworks.

F. Research Gap

Despite the expanding corpus of literature, there are still numerous gaps:

1. India lacks a legal framework that is specifically tailored to artificial intelligence.
2. Insufficient emphasis on accountability and liability mechanisms
3. The incorporation of ethical AI principles into enforceable law is restricted.



4. The absence of empirical and doctrinal studies that integrate AI governance and DPDP
Currently available studies either focus on AI governance or on data protection in isolation. An integrated analysis is required to investigate the practical interactions between data protection laws and AI systems.

G. The Present Study's Contribution

The deficiencies mentioned above are addressed in this paper by:

1. Offering a comprehensive examination of legal accountability, data governance, and AI
2. Assessing the DPDP Act in the context of AI technologies
3. Incorporating comparative insights, policy developments, and recent empirical data
4. Suggesting a comprehensive regulatory framework for India

III. METHODOLOGY

The current investigation employs a doctrinal and analytical research methodology to investigate the intersection of legal accountability, data administration, and Artificial Intelligence in India within the post-Digital Personal Data Protection Act, 2023 (DPDP Act) framework. The research is primarily qualitative and grounded in the systematic analysis of secondary sources, including judicial decisions, policy reports, statutory instruments, and scholarly literature. The doctrinal approach is particularly appropriate for this study because it enables a comprehensive analysis of current legal frameworks and their capacity to address emerging technological challenges posed by AI systems (Singh, 2021).

The study extensively utilizes primary legal sources, including the Digital Personal Data Protection Act, 2023, and landmark judicial pronouncements such as Justice K.S. Puttaswamy v. Union of India (2017) and Anuradha Bhasin v. Union of India (2020), to comprehend the constitutional and legal underpinnings of data protection and digital rights in India. Additionally, secondary sources, including books, peer-reviewed journal articles, government publications (including reports by NITI Aayog, MeitY, and NASSCOM), and international regulatory frameworks such as the General Data Protection Regulation (GDPR) and the proposed European Union Artificial Intelligence Act, have been critically analyzed to offer a comparative and contextual perspective (Kuner et al., 2020; NITI Aayog, 2024).

The research also employs a comparative analytical approach to assess India's regulatory strategy against global best practices. This entails the examination of critical principles, including transparency, accountability, and risk-based regulation, in various jurisdictions, with a particular emphasis on the European Union framework. This comparative analysis enables the identification of regulatory gaps and informs the development of context-specific recommendations for India. Furthermore, a thematic analysis has been conducted to organize the discourse on fundamental concerns, including algorithmic bias, data governance challenges, legal accountability, and regulatory deficiencies in AI systems.

The study is predominantly doctrinal and does not involve empirical fieldwork or quantitative data collection, despite incorporating recent statistical data and policy developments to support its analysis. This is a limitation of the research, as it may necessitate additional empirical investigation due to practical implementation challenges and stakeholder perspectives. However, the methodology offers a thorough, legal and policy-oriented understanding of the subject, enabling a critical assessment of the DPDP Act in the context of swiftly evolving AI technologies.

In summary, the methodological framework aims to enhance the broader discourse on AI governance and data protection in India by ensuring analytical depth, doctrinal clarity, and policy relevance.



IV. FINDINGS

A. The Development of a Data-Driven Economy and the Adoption of AI

The present study's results indicate that India is currently experiencing rapid and extensive integration of Artificial Intelligence (AI) into its economic, administrative, and social systems, thereby heightening the importance of legal accountability and data governance. According to recent empirical data, nearly 87% of Indian enterprises have implemented AI technologies, with many achieving operational maturity. Additionally, 92% of knowledge workers report utilizing AI tools in their daily professional activities, a level of adoption that surpasses the global average (Press Information Bureau, 2025; IndiaAI, 2024). AI's transformative potential for national development is underscored by its projected contribution of approximately \$500–600 billion to India's GDP by 2035 (NITI Aayog, 2025). These advancements are further reinforced by government initiatives, including the IndiaAI Mission, which seeks to establish a resilient AI infrastructure, foster innovation, and improve data ecosystems through substantial public investment (MeitY, 2024). Collectively, these trends illustrate that data has emerged as a critical asset in India's digital economy, requiring robust regulatory frameworks to guarantee its responsible utilization.

B. Development of Data Ecosystems and Digital Infrastructure

Parallel to this expansion, India's digital infrastructure has grown substantially, leading to unprecedented levels of data generation and processing. In 2024, the Unified Payments Interface (UPI) became a fundamental component of India's digital economy, processing transactions worth more than ₹18 trillion in a single month and accounting for a significant share of digital payments (NPCI, 2024). Furthermore, India is now home to more than 900 million internet consumers, making it one of the world's largest data-generating societies (IAMAI & Kantar, 2024). The rapid expansion of cloud infrastructure and data centers further evidences the growing dependence on data-driven technologies. Although these advancements improve efficiency and accessibility, they also exacerbate concerns about data privacy, security, and governance, particularly in the context of AI systems that depend on algorithmic decision-making and continuous data processing.

C. Constitutional Safeguards and State Surveillance

The expansion of state-led data ecosystems and the associated surveillance risks are a critical dimension that has emerged from the study. The consolidation of personal data across multiple domains, including banking, telecommunications, and travel, is facilitated by large-scale data integration initiatives, such as NATGRID and Aadhaar-linked governance mechanisms. It is suggested in reports that these systems may contain data related to a significant portion of India's population, which raises concerns about the potential misuse of personal information and mass surveillance. The constitutional safeguards established by the Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017) must be considered in the context of these developments. The court recognized privacy as a fundamental right and mandated that any restriction must meet the criteria of legality, necessity, and proportionality. Additionally, the Court underscored the significance of transparency and proportionality in digital governance, particularly in the context of digital access restrictions, in Anuradha Bhasin v. Union of India (2020). The escalating use of AI-driven surveillance technologies, such as facial recognition systems, has prompted inquiries regarding the efficacy of current legal protections in preventing arbitrary or excessive state intrusion.

D. Socio-Legal Consequences of Algorithmic Bias

The issue of algorithmic bias and its socio-legal implications is another significant discovery. Studies suggest that Indian languages and socio-cultural contexts are considerably underrepresented in global datasets, potentially leading to biases in AI outputs. AI systems are inherently dependent on the quality and representativeness of training data (ArXiv, 2025). Algorithmic decisions may disproportionately impact marginalized communities in areas such as recruitment, credit scoring, and law enforcement, where such biases can have severe consequences. Recent Indian policy discussions have reaffirmed the necessity of localized datasets and inclusive AI development, as scholars such as



O'Neil (2016) have long cautioned that algorithmic systems can perpetuate systemic inequalities. The DPDP Act fails to expressly address algorithmic fairness or discrimination, thereby highlighting a critical gap in India's regulatory framework.

E. Challenges of Transparency and Explainability

The study also identifies significant challenges regarding transparency and explainability in AI systems. Numerous artificial intelligence models operate as "black boxes," which complicates the understanding of the decision-making process. This lack of transparency limits individuals' ability to challenge automated decisions and undermines accountability. Despite global frameworks like the GDPR acknowledging a "right to explanation," India's DPDP Act does not explicitly include such provisions, which impedes its ability to regulate AI-driven decision-making (Kuner et al., 2020). High-stakes domains, such as healthcare, criminal justice, and financial services, are particularly problematic because of the lack of explainability requirements, as algorithmic decisions can have significant effects on individual rights.

F. Legal Accountability and Liability Concerns

The results highlight a fundamental challenge in assigning legal accountability for AI-driven outcomes. In contrast to conventional systems, AI entails a multitude of stakeholders, such as data providers, developers, and deploying entities, which leads to a dispersion of accountability. Recent research suggests that India's current legal framework fails to adequately address liability for algorithmic injury or system failures (ArXiv, 2025). The DPDP Act does not provide explicit guidelines for assigning liability in AI-specific contexts, even though it imposes obligations on data fiduciaries. This can impede effective enforcement and generate uncertainty, particularly in cases involving multinational technology companies and cross-border data flows.

G. Comparative Global Regulatory Approaches

A comparative analysis also indicates that India's regulatory approach is relatively underdeveloped compared to global standards. The proposed AI Act and GDPR of the European Union adopt a more comprehensive, risk-based approach, emphasizing transparency, accountability, and human oversight while imposing stricter obligations on high-risk AI systems. These frameworks offer India valuable insights, particularly in the integration of data protection with AI governance. In contrast, India's strategy remains fragmented, as it continues to rely on generic data protection principles and non-binding ethical guidelines, such as those proposed by NITI Aayog in its "Responsible AI for All" framework (NITI Aayog, 2024). Although these initiatives demonstrate increasing awareness of AI-related risks, their effectiveness in ensuring compliance is limited by their non-binding nature.

H. The Necessity of Reform and Policy Developments

The DPDP Rules, 2025, and other recent policy developments are significant contributions to enhancing India's data protection regime by establishing more explicit compliance requirements, including consent management, data minimization, and breach notification mechanisms. Nevertheless, these measures are insufficient to address the broader challenges posed by AI technologies, particularly regarding algorithmic accountability and systemic risks. The study therefore emphasizes the pressing need for a comprehensive, integrated regulatory framework that combines AI-specific governance mechanisms with data protection. Institutional mechanisms for oversight and enforcement, as well as provisions for algorithmic audits, impact assessments, and clear liability standards, should be included in such a framework.

In conclusion, the study's findings suggest that, despite India's substantial progress in establishing a data protection framework through the DPDP Act, the rapid advancement of AI technologies has surpassed the capacity of existing legal frameworks. The regulatory gap that urgently needs to be addressed results from the scope of data-driven governance and economic activity, as well as the absence of explicit provisions addressing AI-specific risks. A



coordinated strategy that includes adopting global best practices, strengthening institutions, and reforming legislation will be necessary to bridge this divide, ensuring that technological innovation aligns with constitutional values and fundamental rights.

V. CONCLUSION

The present study illustrates that the rapid proliferation of Artificial Intelligence (AI) within India's digital ecosystem has profoundly altered the nature of data governance, while simultaneously revealing critical gaps in existing legal frameworks. The empirical findings underscore that India is one of the world's foremost adopters of AI technologies, with a significant projected contribution to economic development and widespread integration across sectors. The unprecedented levels of data generation resulting from the expansion of digital infrastructure, including large-scale platforms such as UPI and widespread internet penetration, have positioned data as a central pillar of economic development and governance. Nevertheless, this data-intensive environment has also exacerbated apprehensions regarding the ethical use of technology, surveillance, and privacy.

The recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017) and subsequent judicial developments such as *Anuradha Bhasin v. Union of India* (2020) establish a strong normative foundation for data protection and digital rights in India from a constitutional perspective. These decisions underscore the importance of principles such as legality, necessity, proportionality, and transparency, which must serve as the foundation for any regulatory framework that regulates data and AI systems. Nevertheless, the growing deployment of AI-driven technologies, particularly in public administration, surveillance, and decision-making processes, raises substantial concerns about the practical effectiveness of these safeguards.

The research indicates that the Digital Personal Data Protection Act, 2023, is a significant legislative milestone; however, it primarily regulates personal data processing and falls short of adequately addressing the complexities introduced by AI systems. The lack of explainability, algorithmic bias, and the diffusion of accountability are still largely unregulated. The Act's ability to effectively address AI-related harms is restricted by the absence of explicit provisions regarding automated decision-making and liability frameworks, which creates uncertainty. Biased AI systems may exacerbate existing inequalities and disproportionately affect vulnerable populations in a socio-economically diverse country such as India, which is why this regulatory disparity is of particular concern.

The necessity of a more comprehensive and integrated regulatory approach is underscored by a comparative analysis with global frameworks, particularly the GDPR of the European Union and the proposed AI Act. These frameworks adhere to a risk-based model, which prioritizes accountability, transparency, and human oversight. Consequently, they offer valuable insights for India. In contrast, India's current strategy is fragmented, as it is predicated on general data protection principles and non-binding policy guidelines, such as those proposed by NITI Aayog. Although these initiatives demonstrate an understanding of the potential hazards associated with artificial intelligence, their practical application is restricted by their lack of enforceability.

The results further emphasize the growing difficulties associated with data concentration and state surveillance. The potential misuse of personal data and mass surveillance are concerns that are raised by the expansion of centralized data systems and AI-enabled monitoring technologies. In this context, the constitutional principles established by the Supreme Court must be operationalized through robust legal and institutional mechanisms to prevent technological advancements from undermining fundamental rights.

The study recommends establishing a comprehensive, integrated AI governance framework in India to address these obstacles. By incorporating AI-specific regulatory provisions, such as mandatory algorithmic audits, impact



assessments, and explicit liability mechanisms, such a framework should complement the DPDP Act. Additionally, it should establish autonomous regulatory bodies that are authorized to supervise the deployment of AI and enforce compliance. Furthermore, to ensure accountability and public confidence, it is imperative to advance ethical standards, transparency, and explainability in AI systems.

Additionally, there is an urgent need to allocate resources to initiatives that promote digital literacy and capacity-building to facilitate the effective exercise and understanding of data rights by individuals. To mitigate algorithmic bias and ensure impartiality in AI systems, policymakers must also promote the creation of inclusive, representative datasets. To achieve a balanced approach that promotes innovation while protecting individual rights, collaboration among government, industry, and academia will be essential.

In summary, India has made substantial strides toward establishing a data protection regime through the DPDP Act. However, the accelerated advancement of AI technologies requires a paradigm shift in regulatory thinking. To address the challenges of AI governance, it is imperative to establish a legal framework that is technology-sensitive, rights-based, and forward-thinking. India can ensure its digital transformation is both sustainable and inclusive by aligning technological innovation with constitutional values and global best practices. This will reinforce the principles of democratic governance, accountability, and justice in the digital age.

ACKNOWLEDGEMENT

The author expresses sincere gratitude to all those who directly or indirectly contributed to the successful completion of this research work. Special thanks are extended to colleagues, reviewers, and academic mentors for their valuable guidance, constructive suggestions, and continuous encouragement throughout the study.

REFERENCES

1. Bhandari, V., & Bansal, S. (2022). Data protection and privacy laws in India: A critical analysis. *Indian Journal of Law and Technology*, 18(1), 45–67.
2. Floridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28(4), 689–707.
3. Kuner, C., Bygrave, L. A., & Docksey, C. (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.
4. O’Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing.
5. Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.
6. Zuboff, S. (2019). *The age of surveillance capitalism*. PublicAffairs.
7. Digital Personal Data Protection Act, 2023 (India).
8. Digital Personal Data Protection Rules, 2025 (India).
9. Information Technology Act, 2000 (India).
10. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
11. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
12. K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1.
13. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
14. Ministry of Electronics and Information Technology (MeitY). (2024). *IndiaAI Mission Document*. Government of India.
15. NITI Aayog. (2024). *Responsible AI for All: Strategy for India*. Government of India.
16. NITI Aayog. (2025). *AI for Viksit Bharat: Economic Growth Report*. Government of India.
17. Press Information Bureau. (2025). *AI adoption trends in India*. Government of India.



18. IndiaAI. (2024). *AI adoption among knowledge workers in India*. Government of India.
19. IAMAI & Kantar. (2024). *Internet in India Report 2024*.
20. NASSCOM. (2025). *AI Adoption Index Report*.
21. National Payments Corporation of India (NPCI). (2024). *UPI transaction statistics*.
22. EY India. (2025). *Navigating the data protection landscape in India*.
23. European Union. (2016). *General Data Protection Regulation (GDPR)*.
24. European Commission. (2021). *Proposal for Artificial Intelligence Act*.
25. OECD. (2019). *OECD Principles on Artificial Intelligence*.
26. Barat, S. (2025). Data protection and AI under the DPDP Act: Challenges and opportunities. *Journal of Indian Legal Studies*, 12(2), 115–134.
27. Khurana & Khurana. (2025). AI training data under India's DPDP regime: Compliance challenges and strategies.
28. ArXiv. (2025). Algorithmic accountability and AI governance in emerging economies

