ARTIFICIAL INTELLIGENCE AND PERSONAL DATA: REASSESSING THE DIGITAL PERSONAL DATA PROTECTION FRAMEWORK IN INDIA

Preeti, LLM, Amity University, Gurugram

ABSTRACT

However, Artificial Intelligence (AI) is changing the way personal data is collected, inferred, aggregated and reused, which is threatening fundamental data protection and privacy principles and calls for a re-thinking of the Indian Digital Personal Data Protection (DPDP) regime. The objective of this study was to understand the correlation between AI and personal data processing in India, delineate privacy risks and challenges of data protection with respect to AI, analyze the effectiveness of the DPDP Act, 2023 and DPDP Rules, 2025, and investigate the transparency, accountability, and governance measures with respect to processing and using personal data in India through AI technologies, and to draft qualitative metrics for assessment of compliance and adequacy with respect to data protection laws and regulations in India. Employing a qualitative, theoretical method based on secondary sources, the study analyzed the possibility of a largely consent-based regime to cope with the lifecycle-based processing of AI through privacy-as-control, contextual integrity, privacy-as-dignity and autonomy (including the constitutional framing in Justice K.S. Puttaswamy v. Union of India), surveillance-capitalism, critical privacy, and algorithmic accountability theories. The results show that there is a mismatch between the discrete, purpose-specific processing logic of the DPDP Act and the continuous processing logic, inferences, and repurposing of AI systems throughout the model lifecycle, confirming concerns raised in the context of the DPDP Act for improper information flow after secondary use. The three salient risks were identified as re-identification, function creep and algorithmic bias, with UNESCO's point of viewpoint driven by a lifecycle approach being more analytically appropriate than the Act's point of collection approach under Section 6. In the Rules' substantive section, there was a relatively small number of AI-specific obligations, such as no algorithmic fairness principles, no protections against automated decision-making, and operationalising the right to erasure proved challenging for generative AI due to the lack of machine unlearning at scale. The study also noted that the framework is about disclosure-based transparency, and not relational accountability that is enough to ensure meaningful algorithmic answerability. While the DPDP framework is an important piece of general-

purpose legislation, its failure to adequately protect informational autonomy from profiling and inference by AI does have implications for dignity, equality, public trust, the necessity of AI-specific subordinate legislation and sectoral codes for certain high-risk sectors and fields, and the fact that there is a lack of specific qualitative indicators.

Keywords: Artificial Intelligence, Digital Personal Data Protection, privacy-as-control, contextual integrity, informational privacy, surveillance-capitalism, automated decision-making.

INTRODUCTION

AI is changing everything about the collection, processing, inference, and application of personal data, impacting the existing paradigm on data protection and individual privacy. In this techno-dynamic environment, India's Digital Personal Data Protection (DPDP) has to be critically evaluated to see if its legal safeguards, accountability measures, and rights-based protection are still appropriate in the face of the unprecedented risks posed by AI-based data processing. The research had been informed by several interrelated theoretical perspectives that provided a normative and analytical foundation for reassessing the Digital Personal Data Protection Framework in India. First, the privacy-as-control theory had conceptualised privacy as an individual's capacity to determine when, how, and to what extent personal information was disclosed, thereby providing an important basis for examining whether consent and individual control under the Digital Personal Data Protection Act, 2023 ("DPDP Act") had remained meaningful in AI-driven environments where data had been continuously collected, inferred, aggregated, and repurposed. Alan F. Westin had similarly conceptualised privacy in terms of an individual's ability to determine when personal information was communicated to others, a conception that had become increasingly difficult to sustain where AI systems had operated through large-scale and opaque data processing.[1] Second, contextual integrity theory, developed by Helen Nissenbaum, had provided a more suitable framework for assessing AI-related data processing because it had treated privacy not merely as secrecy or individual control, but as the appropriate flow of information within particular social contexts according to context-specific norms governing the subject, sender, recipient, information type, and transmission principle.[2] This theory had been particularly relevant to AI because personal data collected for one purpose could subsequently have been used for algorithmic profiling, model

[1] Alan F. Westin, Privacy and Freedom, 25 WASH. & LEE L. REV. 166, 166 (1968).
[2] Helen Nissenbaum, Privacy as Contextual Integrity, 79 WASH. L. REV. 119, 119 (2004).

training, automated decision-making, or prediction in a substantially different context, thereby raising questions concerning purpose limitation and legitimate processing. Third, privacy-as-dignity and autonomy theory had influenced the constitutional understanding of informational privacy in India, particularly through *Justice K.S. Puttaswamy (Retd.) v. Union of India*, in which the Supreme Court had recognised privacy as an intrinsic component of life, personal liberty, dignity, and autonomy under the Constitution.[3]. This constitutional theory had been significant because AI-enabled profiling and prediction could have affected individual autonomy even without conventional forms of physical intrusion. Fourth, surveillance-capitalism theory had illuminated the structural dimension of AI-driven data exploitation by demonstrating how personal information had been transformed into an economic resource through continuous extraction, behavioural prediction, personalisation, and commodification.[4] This perspective had exposed the limitations of a purely consent-based regulatory model because individuals had often lacked meaningful bargaining power against entities possessing extensive technological, informational, and economic advantages. Fifth, critical privacy theory had further demonstrated that data protection had involved questions of power rather than merely individual secrecy, particularly where corporations and state institutions had possessed substantially greater capacities to collect, analyse, predict, and influence behaviour through data-intensive technologies.[5] Finally, algorithmic accountability theory had provided a governance-oriented framework for examining whether AI systems had remained transparent, explainable, auditable, and subject to meaningful institutional oversight; Kroll and his co-authors had argued that accountability mechanisms had been necessary because algorithmic systems could produce consequential decisions without conventional forms of human transparency.[6] Collectively, these theories had demonstrated that the regulation of AI and personal data could not have been evaluated solely through the traditional paradigm of individual consent; rather, the Indian framework had needed to be assessed through the combined lenses of individual autonomy, contextual appropriateness, dignity, structural power, surveillance, and algorithmic accountability, particularly in light of the DPDP Act's stated objective of balancing the protection of personal data with the lawful processing of digital personal data.[7]

[3] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India)
[4] Shoshana Zuboff, Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, 30 J. INFO. TECH. 75, 75 (2015).
[5] Julie E. Cohen, What Privacy Is For, 126 HARV. L. REV. 1904, 1904 (2013).
[6] Joshua Alexander Kroll, Accountable Algorithms (Sept. 2015) (Ph.D. dissertation, Princeton University).
[7] Digital Personal Data Protection Act, No. 22, Acts of Parliament, 2023, pmbl. (India).

The research on "Artificial Intelligence and Personal Data: Reassessing the Digital Personal Data Protection Framework in India" had been situated within a rapidly changing technological and regulatory environment in which artificial intelligence ("AI") had increasingly depended upon the collection, processing, inference, and reuse of large volumes of personal and non-personal data. A major trend had been the transition from conventional data-processing systems towards AI systems capable of profiling individuals, generating behavioural predictions, automating decisions, and deriving new information from existing datasets. The OECD had observed that recent developments, particularly generative AI, had intensified questions concerning data governance and privacy because AI and privacy regulation had often evolved in separate regulatory silos (OECD, 2024). In India, this trend had acquired particular significance following the enactment of the Digital Personal Data Protection Act, 2023 ("DPDP Act"), which had established obligations for data fiduciaries, rights for data principals, consent requirements, legitimate-use provisions, security obligations, and penalties for breaches[8]. The regulatory landscape had subsequently developed further through the Digital Personal Data Protection Rules, 2025, notified on November 13, 2025, together with an enforcement timeline and the establishment of the Data Protection Board of India. (Ministry of Electronics & Information Technology, 2025). A second important trend had been the movement from a conventional consent-centric model of privacy towards risk-based, accountability-oriented, and human-rights-based AI governance. NITI Aayog had identified privacy and security, transparency, accountability, equality, inclusivity and non-discrimination, safety and reliability, and protection of human values as core principles for responsible AI in India[9]. Similarly, UNESCO had emphasised that privacy and data protection should be protected throughout the entire AI lifecycle and had recommended privacy-by-design, impact assessments, transparency, accountability, and meaningful data-subject rights (UNESCO, 2021). A third trend had been the increasing difficulty of maintaining individual control over personal information because AI systems could transform apparently innocuous datasets into highly revealing profiles through inference and correlation. This development had challenged traditional conceptions of privacy based primarily on secrecy or individual control and had supported Helen Nissenbaum's contextual-integrity approach, under which privacy had depended upon whether information had flowed appropriately within a particular social context

[8] Digital Personal Data Protection Act, No. 22, Acts of Parliament, 2023, §§ 4–17, 33 (India).
[9] NITI AAYOG, APPROACH DOCUMENT FOR INDIA: PART I—PRINCIPLES FOR RESPONSIBLE AI (2021).

rather than merely upon whether an individual had technically consented to its disclosure[10]. A related trend had been the commercialisation and commodification of personal data, in which data had become an economic resource for behavioural prediction, targeted advertising, personalisation, and automated decision-making. Shoshana Zuboff had characterised this transformation as part of "surveillance capitalism," in which human experience had increasingly been appropriated as raw material for prediction and commercialisation[11].

The principal issues arising from these trends had concerned the adequacy of the DPDP framework when applied to AI systems whose data practices had been substantially more complex than ordinary digital processing. The first issue had been the meaningfulness of consent. Although the DPDP Act had recognised consent as a principal ground for processing personal data, AI applications had frequently involved complex processing operations, secondary uses, model training, inference, and unpredictable future applications that could make genuinely informed consent difficult to obtain. The second issue had been purpose limitation and also function creep: data that was initially gathered for a single legitimate function could have been utilized by AI in a vastly various way, such as for the training of AI, profiling, recommendation systems, or predictive analytics. This problem had been the first to highlight how machine-learning systems, which gained value from the combination and re-use of large sets of data, clashed with traditional data-protection principles. Algorithmic transparency and explainability were the third challenge. The information created by AI systems might produce decisions or predictions in complex computational processes that are hard to comprehend by data principals and regulators, which might lead to questions about whether transparency requirements provide a sufficient basis for meaningful accountability. Transparency and accountability, therefore, were identified by NITI Aayog as key considerations for responsible AI governance in India (NITI Aayog, 2021). The fourth issue was privacy, dignity and informational autonomy. The Supreme Court of India had also declared privacy to be a constitutionally protected fundamental right and had equated privacy with dignity, liberty, autonomy and individual choice in Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. As such, AI-based profiling, biometric identification, predictive behaviour and automatic classification had questioned the constitutionality of such practices beyond the traditional notions of data security. The study had also found key difficulties in balancing the innovation of AI with effective personal data protection. A big

[10] Nissenbaum, supra note 2, at 125.
[11] Zuboff, supra note 4, at 75.

problem had been the size and complexity of data processing by AI, as large AI models might need vast amounts of data and could process information in ways that were not predictable at the time of collection. A second challenge had been data minimisation, since the effectiveness of some AI systems had been associated with access to increasingly large and diverse datasets, creating a structural tension between technological optimisation and the principle of collecting only data necessary for a legitimate purpose. A third challenge had been re-identification and inferential privacy risks, whereby anonymised or apparently non-sensitive information could potentially be combined with other datasets to reveal information about identifiable individuals. A fourth challenge had been bias and discrimination, because AI systems trained on historically biased or unrepresentative datasets could reproduce or amplify existing social inequalities; UNESCO had specifically recognised that AI could embed and amplify bias and thereby threaten human rights. A fifth challenge had been cross-border data flows and fragmented regulatory regimes, particularly because AI development had frequently involved multinational corporations, cloud infrastructure, distributed datasets, and international model-development processes. The OECD had therefore emphasised the need for greater coordination between privacy and AI governance frameworks [12]. A sixth challenge had been regulatory adaptability. AI technologies had evolved substantially faster than conventional legislative processes, creating the risk that highly prescriptive rules could become technologically obsolete while broad principles could prove insufficiently enforceable. UNESCO had accordingly advocated adaptive, multi-stakeholder governance and lifecycle-based oversight rather than static regulation[13]. Finally, the Indian framework had faced the challenge of balancing privacy protection with innovation, economic development, public interest, and legitimate governmental and commercial uses of data. The DPDP Act itself had sought to recognise both individual data-protection interests and the need for lawful processing, demonstrating that Indian data governance had not been constructed as an absolute prohibition on data use but as an attempt to establish a regulatory balance. Accordingly, the central question that the research aimed to address was whether the DPDP framework, even after being updated by the Rules 2025, is able to offer adequate protection against the specific risks that AI poses, such as inference, profiling, automated decision-making, opacity, bias, function creep and large-scale data exploitation, without having to unnecessarily limit the social and economic

[12] OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (May 22, 2019), amended May 3, 2024.
[13] UNESCO, Recommendation on the Ethics of Artificial Intelligence, UNESCO (May 16, 2023), https://www.unesco.org/en/artificial-intelligence/recommendation-ethics.

benefits of AI usage. With the rapid adoption of Artificial Intelligence ("AI") in India, the way in which personal data was being collected, processed, analysed, inferred, and being commercially and/or institutionally utilised had completely changed, giving rise to regulatory issues that were not sufficiently covered under the traditional data-protection principles. AI systems increasingly used large and diverse datasets for profiling and prediction, recommendation, biometric identification, automated decision-making and generative functions, raising concerns about undue data collection and secondary use, re-identification, surveillance, algorithmic discrimination, opacity and loss of individual control over personal information. These developments have gained constitutional weight after Justice K.S. Puttaswamy (Retd.) v. Union of India, where the Supreme Court of India had held that privacy is a fundamental right, and had specifically identified informational privacy and the control of personal information as significant aspects of privacy, and had affirmed the need for a strong data-protection regime (Supreme Court of India, 2017). The enactment of the Digital Personal Data Protection Act, 2023 ("DPDP Act") had been a substantial legislative measure aimed at providing a framework for the processing of digital personal data and a recognition of the balancing of individual data-protection rights with the lawful processing of personal data . *Digital Personal Data Protection Act*, No. 22 of 2023, pmbl. (India 2023). However, the increasing sophistication of AI had raised questions regarding whether a framework substantially structured around consent, notice, purpose limitation, data-fiduciary obligations, and individual rights had been sufficiently equipped to address AI-specific risks, particularly where individuals had been unable to foresee how their data would subsequently be combined, inferred from, or used for machine-learning purposes. The problem had therefore extended beyond the protection of data at the point of collection and had concerned the entire AI lifecycle, including dataset development, model training, deployment, inference, automated decision-making, and subsequent reuse of personal information. This regulatory challenge had also been recognised in India's broader AI-governance policy discussions, which had identified privacy, transparency, accountability, bias, security, and fairness as significant risks requiring regulatory attention. (NITI Aayog, 2021). The justification for the research had consequently arisen from the gap between the rapidly evolving capabilities of AI and the capacity of the existing Indian data-protection framework to provide sufficiently specific and effective safeguards against AI-mediated processing of personal data. The research had been particularly relevant because India had simultaneously pursued large-scale digitalisation and AI innovation while seeking to protect constitutional values of privacy, dignity, autonomy, and equality.The study was thus needed to clarify whether the DPDP framework had adequately accommodated

the risks emerging in the context of AI or if its principles, institutional structures and enforcement mechanisms needed to be reinterpreted, supplemented or reformed. Its significance was growing for all stakeholders from legislators and regulators to courts, tech firms and data custodians and to the general public as the balance between innovation and personal data protection in India would take an important turn on how AI is developed and used. The study thus aimed to reexamine the Indian framework from AI specific point of view and to explore gaps and potential changes in the regulatory structure that could help sustain a proper balance between technological advancement and the robust safeguarding of individual informational autonomy.

OBJECTIVE

- To explore the relationship between AI and personal data processing in India.
- To identify AI-related privacy risks and data protection challenges.
- To examine the adequacy of the DPDP Act, 2023 and Rules, 2025.
- To analyse AI transparency, accountability, and governance mechanisms.
- To develop qualitative metrics for assessing DPDP compliance and regulatory adequacy.

The study has identified the research problem, research objectives and the challenges that have come in the way of the convergence of AI and personal data protection in India, it then reviews the available scholarly/legal literature. The literature review examines the current state of thinking regarding governance of AI, privacy, data protection, algorithmic accountability, and the Digital Personal Data Protection framework, and identifies the gaps that warrant the present study. It also sets the conceptual and academic framework to review the need for a robust data protection regime in India, in light of the fast development of AI technologies.

METHODOLOGY

This article uses a qualitative research methodology; it is a theoretical research study in which secondary information from various writers and researchers was used to gather the necessary data. Books, journals, newspapers, and various reports on the subject as well as related

publications, were examined by the researcher, whose name is mentioned. The format of the Bluebook 19th or 20th Edition is adhered to by the article.

LITERATURE REVIEW

AI-Driven Personal Data Processing, Privacy, and Data Protection in India

Since the Digital Personal Data Protection Act, 2023 ("DPDP Act") came into effect, scholars have been struggling with the difficulties arising due to the role of AI in the consent-based framework of the Act. While the DPDP Act includes principles like shared consent, data minimization, and lawful processing, commentators observe that AI's reliance on vast amounts of personal information, often gathered from sensitive sources, and its opaque decision-making processes have thrown into question fundamental concepts of consent, data security, and individual autonomy. A similar conflict between innovation and rights protection is echoed throughout the literature, as scholars have pointed to a need for ongoing, flexible, and comprehensive policy-making by governments, industry, civil society, and individuals to help India reach a sustainable balance between the transformative promise of AI and the protection of privacy [14]. Another related line of research looks at the exception to public data protection under Section 3(c)(ii) of the DPDP Act. The exemption of publicly available data from the scope of the Act's protections is concerning as it could lead to a diminishing of privacy and loss of trust in India's digital economy, given the lack of a clear definition of “necessary” data Processingg by intermediaries and the absence of a robust mechanism of oversight. The analyses typically recommend a stronger ethical standard for the use of AI systems that make use of such exemptions [15]. Constitutional framing is also prevalent. While the right to privacy is constitutionally guaranteed in India, the laws surrounding data protection and AI remain in their infancy, and AI systems, owing to their capacity to gather and process large quantities of personal information using machine learning and deep learning algorithms, can identify patterns that could impact individual's privacy rights [16]. TheDPDP Act is also placed in the context of the current global regulatory landscape in policy oriented literature. In an assessment of the Act's effect on Indian "digital nagriks" (digital citizens), the authors place the increased

[14] Neha Bhuwania & Kishore Kumar D., Right to Privacy and Artificial Intelligence: A Critical Analysis of the Digital Personal Data Protection Act, 2023, 8 INDIAN J.L. & LEGAL RSCH. 8566 (2026).
[15] Ishnay Prakash, Dhruv, & Sanjeev Purkar, “Navigating the Regulatory Landscape for AI and Publicly Available Data in India.” The article was published/uploaded in May 2024, and the PDF itself identifies the journal as *Indian Journal of Law and Legal Research*, Volume VI, Issue II, ISSN 2582-8878.
[16] Advocate Apoorva Thakur et al., Right to Privacy vis-à-vis Artificial Intelligence: Indian Scenario, 7 INT'L J. L. MGMT. & HUMAN. 3370 (2024).

use of AI applications and the extensive collection, storage, and analysis of personal data by service providers as the impetus behind growing concerns about privacy that led to the enactment of the 2023 legislation [17]. The literature after 2023 generally arrives at a similar conclusion that India's legislation, although essential, was not crafted with AI-specific risks on its radar, posing questions on the extent of exemptions, oversight and enforcement to the scholars.

DPDP Act, 2023, DPDP Rules, 2025, and AI-Related Privacy Governance in India

The scholarship consensus tends to be that the DPDP Act is a good starting point but didn't consider the risks posed by AI, and that the Rules from 2025 at least partially fill that gap. One of the constant complaints is that the legislation is applicable to data processing in general, but doesn't account for specific technical risks posed by AI systems. The DPDP Act does not contain regulatory obligations for AI systems, including algorithmic fairness requirements or protections for automated decision making, which is important as traditional data protection laws do not necessarily fully reflect the accountability of AI systems .[18]

scholars point out a second thread delves into the question of whether the fundamental tenets of the Act (consent, purpose limitation, and erasure) can make sense in the context of the technical infrastructure of AI . Analysts highlight that the statutory right to erasure sits uneasily with generative AI, since machine unlearning and algorithmic destruction techniques remain costly, unreliable, and difficult to verify at scale, while differential privacy can reduce model accuracy, and modern AI systems transform and regenerate data rather than merely storing it, making full application of erasure rights to AI systems extremely difficult if not impossible. Nonetheless, the same literature credits the Rules with creating enforcement pathways, observing that the DPDP framework's prohibition on non-consensual processing, safeguards against misuse of sensitive data, and empowerment of the Data Protection Board to investigate AI-driven profiling harms establish accountability mechanisms tied to AI model training and deployment.[19]

[17] Chandana Malhotra & Usha Malhotra, Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India, 70 INDIAN J. PUB. ADMIN. 516, 516 (2024).
[18] Anurati Dasgupta & Ruchika Sharma, Artificial Intelligence and Data Protection: Legal Challenges and the Need for a Robust Framework in India, 13 INT'L J. CREATIVE RSCH. THOUGHTS, Nov. 2025, at c778.
[19] Vikrant Rana, Anuradha Gandhi & Prateek Chandgothia, Effect of Digital Personal Data Protection Rules, 2025 on AI Regulation, S.S. RANA & CO. (Nov. 24, 2025), https://ssrana.in/articles/effect-of-digital-personal-data-protection-rules-2025-on-ai-regulation/

Comparative work situates India's approach alongside the GDPR to assess adequacy. Research examining AI-powered expert systems in healthcare, finance, and public administration questions whether the DPDP Act and comparable GDPR provisions are robust enough to govern opaque automated decision-making, and proposes a dedicated framework to promote responsible AI development while preserving privacy rights and accountability.[20]A third body of scholarship reviews the Rules' procedural contribution more directly. Critical review of the DPDP Act and Rules concludes that pre-2023 Indian data governance was decentralized and largely inadequate for a complex digital ecosystem, and that the Rules of 2025 operationalize the Act's consent-based model by supplying procedural protections, compliance mechanisms, and enforcement frameworks, including with respect to India's broader AI governance strategy.[21]

Collectively, this literature suggests the DPDP framework has advanced procedural and enforcement infrastructure but has not resolved deeper doctrinal tensions between AI's data-intensive, opaque operations and rights such as consent and erasure.

DISCUSSION AND RESULTS

The research had produced findings that directly addressed each of the study's five objectives while confirming the theoretical concerns raised at the outset. With respect to the relationship between AI and personal data processing in India, the study had found that AI systems operated on a data logic fundamentally at odds with the DPDP Act's structure: whereas the statute had been organized around discrete, purpose-specific processing events, AI systems had continuously aggregated, inferred, and repurposed data across the model lifecycle, confirming Nissenbaum's contextual-integrity concern that information flows appropriate to one context could become inappropriate once repurposed for algorithmic training. On AI-related privacy risks, the research had identified re-identification, function creep, and algorithmic bias as the most significant threats, with UNESCO's lifecycle-based framing proving more analytically useful than the DPDP Act's point-of-collection orientation, since the Act's consent and notice obligations under Section 6 had addressed only the moment of collection rather than downstream inference. As for the adequacy of the DPDP Act and 2025 Rules, the findings reflected a split picture: the Rules had clarified the procedural aspects of the DPDP Act –

[20] S. Srivastava et al., Privacy in the Age of AI: Regulatory Challenges and Risk Governance in Expert Systems, in EXPERT APPLICATIONS AND SECURITY 33 (V.S. Rathore, B. Raman & S. Kashuba eds., Springer 2026).

[21] Om Prakash Rai, Artificial Intelligence, Data Protection and Digital Governance in India: A Contemporary Legal Analysis, 5 J. SOC. REV. & DEV. 76, 79 (2026).

including timelines for notifications of breaches and registration of consent-managers and the pathways for claims to be brought before the Data Protection Board – but had failed to comprehensively address AI-sphere specific obligations, supporting literature evidence that found no algorithmic fairness obligations or no AI-specific safeguards for automated-decision making within the DPDP Act. The right-to-erasure provisions were especially problematic in the context of generative AI, as machine-unlearning methods were unreliable at large scale. The study has found that India had focussed on disclosure-based transparency and not the relational accountability architecture as proposed by Novelli, Taddeo and Floridi which involved recognition, interrogation and limitation of authority during the process.Lastly, when creating qualitative metrics to measure regulatory adequacy, the research had suggested indicators that ranged from the meaningfulness of consent, resilience against secondary uses of AI, erasure feasibility, and institutional capacity to audit algorithms.Despite the 2025 Rules, that the DPDP framework was still a general-purpose data-While it is a protection statute and not an AI specific instrument of governance, Lacking some of the constitutional protections against profiling and inference by AI.

CONCLUSION

This study has been an effort to reappraise the Digital Personal Data Protection regime in India in light of the unprecedented threats of personal data processing by AI. The study had discovered that while the DPDP Act 2023 and the Rules 2025 had implemented some important procedural and institutional mechanisms, the overall framework still lacked the necessary transparency, accountability, and enforceability of erasure rights for the data practices that AI systems typically involve, which were continuous, inferential, and not necessarily linked to a specific processing event. The study had brought to light that the gaps in the framework of India had direct implications for constitutional values such as dignity, autonomy and equality as recognised in Puttaswamy. Puttaswamy, supra. The lack of adequate algorithmic accountability frameworks put in place would compromise public confidence in India's growing digitalization process at a time when it was vital to inclusive digitalization, while unregulated AI-driven profiling and inference could exacerbate biases against historically marginalized communities. Future directions. Further studies and policy change were necessary to emphasize the need to develop AI-specific subordinate legislation, sectoral codes for high-risk areas like healthcare and biometric identification, as well as efforts to establish standards for machine unlearning and algorithmic explainability.