BALANCING PRIVACY AND PROGRESS: LEGAL AND ETHICAL CHALLENGES IN THE AGE OF ARTIFICIAL INTELLIGENCE IN INDIA

Dr. B. Jaipal Reddy
Principal, K.V. Ranga Reddy Law College,
Gaganmahal, Hyderabad, India,
drjrbattu@gmail.com

Abstract:
Artificial intelligence is spreading at a high pace within the Indian public and private sectors and this has been backed by national interest in policy formulation of using AI in governance, healthcare, education, agriculture, and economic development. Meanwhile, AI systems deeply depend on the pool of data gathering, profiling, and automated decision-making which casts serious doubts on privacy, consent, surveillance, prejudice, transparency, and accountability. These issues are particularly acute in India, as the Supreme Court has already identified privacy as one of the essential guarantees, and the Digital Personal Data Protection Act, 2023 aims at the balance of data protection and legal processing of data. This paper takes a doctrinal and analytical position to evaluate whether the existing legal framework in India is sufficient to govern harms that are caused by AI. It states that India should have a balanced rights based system that guarantees privacy and human dignity without hindering technological advances.
Keywords: *Artificial Intelligence; Privacy; Data Protection; AI Ethics; India.*

Introduction

Artificial intelligence has played a huge role in digital transformation in India, whose influence is felt in the spheres of governance, finance, healthcare, education, policing, and commercial decision-making. The policy discourse of India is becoming more and more focused on considering AI as a means of economic development, government efficiency, and high-scale service delivery but recent literature is also demonstrating how AI may further expose social and legal weaknesses when governance systems are poorly developed (Bhalla, Brooks, & Leach, 2024). The core problem is that the modern AI technologies rely on large amounts of data gathering, continual processing, and predictive analytics, which exacerbate the threats to informational privacy, autonomy, and control over personal information (Martin & Zimmermann, 2024). These dangers are not limited to the abuse of data only. Recent studies about AI governance highlight that the harms of privacy, in many cases, intersect with that of opacity, bias, limited explainability, and responsibility ambiguity in situations where automated systems have an impact on rights and opportunities (Papagiannidis, Mikalef, & Conboy, 2025). Extended comparative analysis of AI ethics also reveals that privacy, fairness, accountability, and transparency are consistent principles in regulating AI worldwide, indicating that these issues are now at the center of the policy, and not marginal to it (Corrêa et al., 2023). The legal importance of such concerns in India is further enhanced by the fact that privacy is declared as one of the fundamental rights by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), that associated privacy with dignity, liberty and constitutional autonomy. The Digital Personal Data Protection Act, 2023 is also reflective of an effort to balance personal data protection with

legitimate data processing, though in its general structure does not in itself address the entire scope of AI-specific issues, especially the issues of automated decision-making and accountability of the institution. This paper seeks to discuss how India may both promote the technological innovation and protection of constitutional privacy, with the case that privacy and progress must be promoted jointly in a regulatory practice that is rights-based and ethically grounded.

Literature Review

Artificial intelligence as a technical instrument, but rather as a socio-legal regime that influences the administration, economies, and decision-making of the masses, by processing data in large quantities, predicting, and automating it. The studies on related governance demonstrate that AI is gradually becoming part of data-driven administration and is employed to categorise people, assist in making choices on a population level, and optimise organisational workflows (Charles et al., 2022). Meanwhile, this literature underlines that these qualities of AI are also what make the technology desirable to governance, such as speed, scale, and predictive capacity; meanwhile, these aspects also make systems dangerous when there are insufficient legal and procedural controls in place (Wirtz et al., 2022). Regulation through AI governance research is thus increasingly being considered as a matter of institutional design and not necessarily of technological performance.

The privacy literature has ceased to have a narrow concept of secrecy and rather it has considered privacy as directly connected to autonomy, dignity, liberty, and informational self-determination. The recent research on AI and data privacy claims that AI systems produce unique harms since they allow inference to be made continuously, predict behaviour and turn previously disclosed personal data into new uses (Martin & Zimmermann, 2024). Recurring threats mentioned by scholars include mass surveillance, profiling, creep of functionality, misuse of data, and destruction of meaningful consent, particularly in the situation when no one can plausibly comprehend or challenge algorithmic processing (Wirtz et al., 2022). This literature is important in that it demonstrates that the loss of privacy in AI ecosystems tends to be compound and systemic as opposed to a solitary illegal leakage.

It is notable that ethical scholarship also tends to come to a fixed set of concerns, such as fairness, accountability, transparency, explainability, and anti-discriminative protection (Schiff et al., 2024). Recent reviews observe that AI system transparency undermines the capacity of the affected individuals to interpret negative consequences, and that fragmented accountability among their developers, deployers, and institutions makes it challenging to apportion accountability (Novelli et al., 2024). The development of AI ethics auditing has also been identified as a feature in research work, which means that governance discussion is moving away not only from abstract principle-setting, but also verification, oversight, and answerability (Cheong, 2024). Notably, this literature cautions numerous times that vulnerable communities experience disproportionate negative impacts whenever automated systems are implemented in the welfare, policing, financial, job or health settings without effective protections (Wang et al., 2025).

Scholarship in the Indian context is starting to be influenced progressively by the constitutional privacy doctrine following Justice K.S. Puttaswamy (Retd.) v. Union of India, in which case the Supreme Court considered privacy as a civil right that is correlated to dignity, liberty, and personal autonomy. This verdict lies at the center of modern Indian literature since it gives the constitutional language of evaluating AI-enabled surveillance, data mining, and automated decisions of the state. A shift in statutory landscape is also manifested by the Digital Personal Data Protection Act, 2023, which clearly aims to acknowledge the right of an individual to ensure the safeguard of personal data and the state interest in the legal processing. However, the recent India-oriented research proposes that this framework, though significant, fails to address AI-specific issues, like explainability, algorithmic responsibility, industry regulation, and solutions to harms created by the automated systems (Biju and Gayathri, 2024); (Bhalla et al., 2024).

It is quite obvious, then, that the literature has a tendency to analyse innovation and digital growth and has rather a number of studies addressing privacy and civil-liberties risks, yet has fewer works that create an Indian-specific framework which can combine both aims of the study (Bhalla et al., 2024). According to the recent scholarship in AI on India, the country needs context-sensitive governance, which is responsive to constitutional values, social inequality, institutional capacity, and developmental priorities instead of just mimicking foreign regulatory forms (Mohanty and Sahu, 2024). The literature thereby justifies the need to adopt a balanced and hence Indian specific approach where privacy protection, ethical accountability and innovation are seen as complementary and not competing objectives (Biju & Gayathri, 2024).

Results

In this paper, a doctrinal legal research approach is used based on analytical and narrow comparative arguments. The main aim of this approach is to analyze the reaction of the Indian law in place to the privacy and ethical issues that artificial intelligence has brought instead of testing a technical model or generating any statistical results. Doctrinal research in legal studies is applied to interpret authoritative legal sources and discover principles together with assessing the soundness, sufficiency, and normative justifiability of the present framework (Papagiannidis et al., 2025). In the given discussion, it is the right strategy since the core issues are constitutional safeguard, statutory design, regulatory loopholes, and accountability standards in AI regulation as opposed to laboratory research or system engineering. This type of normative and institutional inquiry is also supported in recent scholarship of AI governance as regulation is discussed as a concern of legal framework, procedural protection, and shape of governance (Batool et al., 2025).

The main sources are the Constitution of India, in particular, the jurisprudential interpretation of the concept of privacy in Article 21, the Supreme Court of India decisions, legislative acts, and other policy or governmental documents. Particularly, Justice K.S. Puttaswamy (Retd.) v. Union of India is the constitutional basis since it acknowledged privacy to be a basic right in relation to dignity, liberty and autonomy. As the key statutory guideline on the processing

of digital personal information in India, the Digital Personal Data Protection Act, 2023 is analyzed, and how it addresses the issue of lawful processing, the provision of a notice, and the consent of the data processing are discussed (Bhalla et al., 2024). The secondary sources will be peer-reviewed journal articles, books, policy reports, and expert commentary addressing the issue of AI governance, data protection, responsible AI, ethics, and comparative regulatory development.

The paper takes place in an analytical framework that goes through three dimensions. The initial one is the legal aspect, which evaluates privacy, data security, constitutional guarantees, and potential regulatory loopholes in the current framework in India (Bhalla et al., 2024). The second is the ethical aspect that assesses fairness, transparency, explainability, accountability, consent, and meaningful human supervision of AI systems is required (Papagiannidis et al., 2025). The third is the governance aspect, which takes into account what India might do to facilitate innovation and digital development and maintain the degree of public trust and protect basic rights. It implies that the paper will not experiment with algorithms or perform technical experimentation; rather, it will analyse and evaluate law, policy, and the recent scholarship to determine whether the current approach by India is adequate to the AI-enabled decision making in a developing and highly digitised society. This particular approach is particularly appropriate to India since the recent responsible-AI literature highlights that governance should be adapted to the constitutional values, local institutional conditions, and social environment instead of being mechanically replicated according to the foreign examples (Batool et al., 2025).

Conclusions

Artificial intelligence will be of significant potential to the development of India since it could enhance the provision of people, enhance the economic productivity, and facilitate other types of innovations. Simultaneously, the legal and ethical discussion in this paper demonstrates that AI poses severe threats to privacy, autonomy, dignity, and equality in the situation of personal data collection, processing, and repurposing at scale. In India, these issues have a constitutional value since in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India was an acknowledged fundamental right that was related to liberty and dignity. The Digital Personal Data Protection Act, 2023 offers a valuable statutory framework to the regulation of digital personal data and acknowledges the right of an individual to safeguard personal data and the necessity of a legal processing. Nevertheless, the current framework does not include all the complexity of AI-led harms, particularly, when it comes to the issues of opacities, algorithmic responsibility, elucidation, and adequate solutions. India must thus be provided with a better integrated and contextual governance model based on the constitutional values, transparency, proportionality, accountability and human dignity, in order that the technological advancements can be socially valuable besides being legally justifiable.

References

1. *Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: A systematic literature review. AI Ethics, 5, 3265–3279. https://doi.org/10.1007/s43681-024-00653-w.*
2. *Bhalla, N., Brooks, L., & Leach, T. (2024). Ensuring a "responsible" AI future in India: RRI as an approach for identifying the ethical challenges from an Indian perspective. AI Ethics, 4, 1409–1422. https://doi.org/10.1007/s43681-023-00370-w.*
3. *Biju, P. R., & Gayathri, O. (2024). The Indian approach to artificial intelligence: An analysis of policy discussions, constitutional values, and regulation. AI & Society, 39, 2321–2335. https://doi.org/10.1007/s00146-023-01685-2.*
4. *Charles, V., Rand, N. P., & Carter, L. (2022). Artificial intelligence for data-driven decision-making and governance in public affairs. Government Information Quarterly, 39(4), 101742. https://doi.org/10.1016/j.giq.2022.101742.*
5. *Cheong, B. C. (2024). Transparency and accountability in AI systems: Safeguarding wellbeing in the age of algorithmic decision-making. Frontiers in Human Dynamics, 6, 1421273. https://doi.org/10.3389/fhumd.2024.1421273.*
6. *Dadhich, A., & Bansal, Y. (2025). Implementing responsible and ethical artificial intelligence in India: Balancing innovation and regulation for sustainable AI development. In C. Hoffmann & D. Bansal (Eds.), AI ethics in practice. Springer. https://doi.org/10.1007/978-3-031-87023-1_3.*
7. *Martin, K. D., & Zimmermann, J. (2024). Artificial intelligence and its implications for data privacy. Current Opinion in Psychology, 58, 101829. https://doi.org/10.1016/j.copsyc.2024.101829.*
8. *Mohanty, A., & Sahu, S. (2024, November 21). India's advance on AI regulation. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation.*
9. *Novelli, C., Taddeo, M., & Floridi, L. (2024). Accountability in artificial intelligence: What it is and how it works. AI & Society, 39, 1871–1882. https://doi.org/10.1007/s00146-023-01635-y.*
10. *Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. The Journal of Strategic Information Systems, 34(2), 101885. https://doi.org/10.1016/j.jsis.2024.101885.*
11. *Schiff, D. S., Kelley, S., & Camacho Ibáñez, J. (2024). The emergence of artificial intelligence ethics auditing. Big Data & Society, 11(2). https://doi.org/10.1177/20539517241299712.*
12. *Wang, S., Zhang, Y., Xiao, Y., & Liang, Z. (2025). When artificial intelligence meets accountability: Who holds legitimacy as account givers and holders? Big Data & Society, 12(1–2). https://doi.org/10.1177/20539517251339120.*
13. *Wirtz, B. W., Weyer-er, J. C., & Kehl, I. (2022). Governance of artificial intelligence: A risk and guideline-based integrative framework. Government Information Quarterly, 39(4), 101685. https://doi.org/10.1016/j.giq.2022.101685.*