Artificial intelligence, data protection and digital governance in India: a contemporary legal analysis

Om Prakash Rai

Principal and Professor of law, Bareilly College, Bareilly, Uttar Pradesh, India

Corresponding author: Om Prakash Rai

Received 8 Jan 2026; Accepted 21 Feb 2026; Published 2 March 2026

DOI: https://doi.org/10.64171/JSRD.5.1.76-81

Abstract

The blistering development of Artificial Intelligence (AI), online platforms, and data-based technologies has essentially transformed the system of governance, the economy, and interactions within the Indian society. India has made considerable legal and regulatory changes in a bid to deal with emerging issues, which concern privacy, data security, and digital responsibility. The existing legal regulations governing the use of AI and data protection in India are critically reviewed in this research paper, namely, the Digital Personal Data Protection Act, 2023 (DPDP Act), the Digital Personal Data Protection Rules, 2025, and further developments of regulations. The paper concludes that before the DPDP Act came into effect, the data governance system in India was decentralized and mostly insufficient to deal with the intricacies of the contemporary digital ecosystem. DPDP Act, 2023 has become a paradigm shift due to its introduction of consent-based model, specifying the rights of data principal, and imposing statutory duties on data fiduciaries. These provisions are implemented by the following Rules of 2025 that provide procedural protection, compliance, and enforcement frameworks. In addition, the paper examines the regulatory strategy that India has adopted in relation to AI governance. In contrast to other jurisdictions, like those of the European Union, India has never passed a separate AI law, but it regulates AI by the interaction of data protection legislation, intermediary liability regulations, and industry-specific policies. Though it is a flexible method and encourages innovation, it introduces regulatory uncertainty particularly on issues such as algorithmic accountability, algorithmic liability, and ethical governance. According to the study, even though India has made significant progress in the area of improving its digital legal environment, it continues to face numerous challenges, including the lack of enforcement strategies, the lack of clarity in AI regulation, and the emergence of threats, including deepfakes and data misuse. The article proposes the idea of a holistic, rights-based, and futuristic law system to make sure that technological development does not contradict the constitutional doctrine and social well-being.

Keywords: Artificial Intelligence, Data Protection, Digital Personal Data Protection Act, 2023, Digital Governance, Privacy Law, AI Regulation, India, Cyber Law, IT Rules, Algorithmic Accountability

1. Introduction

The modern world is marked with an unprecedented growth of digital technologies, which have changed almost all the spheres of human life. One of such instruments is Artificial Intelligence (AI), which has become a potent means of affecting decision-making in various industries in healthcare, finance, education, governance, and law enforcement. India is one of the largest digital economies in the world and its digital infrastructure, internet penetration and data creation have grown at a rapid rate in the last ten years. The transformation has not only provided new grounds to economic growth and to efficient governance, but it has also posed new legal and ethical issues. The spread of AI and data-driven technologies has led to the massive collection, processing and storing of personal data. This has increased the issue of privacy, data safety, and individualism. Algorithms bias, absence of transparency and accountability are also other problems that have been created by the growing use of algorithmic systems in decision-making. The changes require the elaboration of a powerful legal framework that will be able to respond to the complex issues of digital technologies.

In the past, the Indian law on the protection of data was small and divided. The main piece of legislation that dominated digital action was the Information Technology Act, 2000 (IT Act) that was passed to enable electronic commerce and deal with cybercrime. The IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), 2011 offered some protection to the data, but it was not sufficient to ensure the complexity of the modern digital ecosystem. These stipulations were not well defined, did not have enforceable rights or proper regulatory measure.

The establishment of privacy as a right in Justice K.S. Puttaswamy v. Union of India (2017) by the Supreme Court of India was a major turning point in developing the data protection legislation in India. The Court said that the right to privacy is inherent in the right to life and personal liberty in Article 21 of the Constitution. This historic decision formed the constitutional basis of the creation of a detailed data protection regime in India. To address the increasing demand of data protection, the Government of India formed the Justice B.N.

Srikrishna Committee that presented their report in 2018. The Committee suggested implementing a broad data protection legislature founded upon such principles as consent, limiting the purposes, minimalizing data, and accountability. Despite the multiple revisions of the initial Personal Data Protection Bill and its delays the final result was the enactment of the Digital Personal Data Protection Act, 2023.

The DPDP Act, 2023 is one of the milestones of the Indian law. It presents a systematic approach to the handling of the digital personal data with the focus on the rights of the individuals (also known as the data principals) and the responsibilities of the data processing entities (also known as the data fiduciaries). The Act takes a consent-based model where organizations have to seek informed and express consent prior to processing personal data. It also gives people the right to access, correct, and delete their personal data. Besides creating substantive rights and obligations, the DPDP Act offers the formation of a Data Protection Board of India, whose mandate is to mediate disputes and enforce compliance. The Act also stipulates severe sanctions in case of non-compliance thus boosting enforcement mechanisms. The Act has however also been criticized due to some of the exemptions given to government agencies and lack of provisions in regard to non-personal data.

In order to operationalize the DPDP Act, the government presented the Digital Personal Data Protection Rules, 2025. These regulations also contain specifications on several areas of data processing such as data collection, data storage, breach notification, and redressal of grievances. The Rules also stipulate the appointment of Data Protection Officers and require organizations to establish the necessary technical and organizational measures to facilitate data security. The gradual adoption of the Act and Rules is indicative of a realistic strategy and the organization has time to get used to the new regulatory environment. Simultaneously with the progress in the area of data protection legislation, India has made efforts to control the digital platforms and intermediate services. Information Technology (Intermediary Guidelines and Digital Media Ethics Code), Rules, 2021, and subsequent amendments to 2026 have placed responsibility and disclosure on the intermediaries. Such policies include issues such as content control, redress of grievances, and the regulation of the internet platform.

India has adopted a different regulation approach in regards to AI. Unlike in other jurisdictions such as the European Union, which have incorporated specific laws on AI, India has chosen to indirectly regulate AI by citing the current laws. These include laws of data protection, IT law, and regulations in the industry. Although such a method offers flexibility and lacks overregulation, it also generates confusion over the question of liability, accountability, and ethical norms within AI systems. Increasing the application of AI to the governance and decision-making processes has serious constitutional and ethical implications. The automated systems applied in the fields of law enforcement, credit scoring, and welfare distribution can affect the basic rights, as the right to privacy, equality, and freedom of expression. These concerns are further compounded by the fact that algorithmic decision-making is not a transparent process as people cannot challenge or comprehend decisions made about them.

The next severe concern is the development of AI-harms, including deepfakes, fake news, and identity theft. Such phenomena are a great threat to the democratic processes, social stability and personal dignity. Even after the new changes in IT regulations have tried to tackle such issues by placing responsibility on the intermediaries, the success of such efforts has been doubted. The international environment is also a major determinant of the regulatory strategy in India. The General Data Protection Regulation (GDPR) and the AI Act established by the European Union have established a standard of data protection and AI regulation. The legal system in India has some similarities to these models especially in areas like principles of consent, transparency and accountability. However, the Indian approach is more flexible and gradual since it is, perhaps, predetermined by the particularities of the socio-economic context and priorities in the development of India.

Despite much development, the Indian digital legal architecture still has a few problems that are still there. They are the lack of a fully developed AI legislation, the impossibility to enforce it, and the uncertainties of the regulatory provisions. There is a need to balance between competing interests such as innovation and privacy, economic growth and individual rights and national security and data protection as well. The research paper will examine these issues further by researching the development of data protection and AI regulation in India. It will aim at examining the effectiveness of the existing laws, the loopholes in the law, and provide recommendations on the way to have a more consolidated and a thorough law framework. The study also provides a direction toward the future of legal regulation of digital governance in India by becoming part of the growing literature on the topic through its doctrinal and analytical approach.

2. Objectives of the study

The current research is being done with the following objectives:

- To analyse the development of the data protection legislation in India.
- To examine the legal system that regulates Artificial Intelligence and digital governance in India.
- To conduct a critical evaluation of Digital Personal Data Protection Act, 2023 and the Rules of 2025.
- To identify some of the relevant legal and regulatory matters in the regulation of AI and data protection.
- To establish the adequacy of the existing enforcement mechanisms.
- To propose policy and legal changes to enhance the digital governance system in India.

3. Literature review

Academic literature and policy-focused literature, based on books, journal articles, and online legal materials, can be useful in understanding the advantages and disadvantages of the regulatory practice of India.

3.1 Pre-DPDP phase: fragmentation and legal inadequacy

Much of the scholarly discussion during this early period was on the ineffectiveness of current legal provisions in the Information Technology Act, 2000. Some authors like Bhatia (2021) believed that the IT Act did not aim to offer an overall data protection framework but focused on cybercrime and electronic commerce. On the same note, Greenleaf (2021) pointed out that India did not have a single law on data protection equivalent to international regulations like the General Data Protection Regulation (GDPR) of the European Union. The weaknesses of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 were also noted in academic studies. These rules have been criticized as being narrow in scope, lack of enforcement mechanism and imprecision in data subject rights. As Kuner (2022) notes, lack of enforcement of rights and institutional control were major factors which compromised the efficiency of the data protection regime in India. The effect of the Justice B.N. Srikrishna Committee Report (2018) persisted in the literature during this period. Scholars have widely acknowledged the report to be a pivotal document that outlined the need to have a rights-based data protection framework. It highlighted concepts like consent, limitation of purpose, minimization of data, and accountability concepts which were subsequently used to guide the DPDP Act, 2023.

3.2 Emergence of comprehensive framework: DPDP act analysis

With the implementation of the Digital Personal Data Protection Act, 2023, a lot of scholarly and policy-driven literature has been created. Researchers have described the Act as an important development in the Indian law. The Act is designed to guarantee the equilibrium between the rights of the individuals and the legitimate interests of the state and the businesses to provide a protective and facilitative framework (Ministry of Electronics and Information Technology, 2023). According to Chander and Sun (2023), the DPDP Act can be discussed as the application of the consent-centric model, in accordance with which, the processing of personal information must be performed with informed and explicit consent of the individuals. This model is consistent with the principles of data protection in the world, but has also been criticized as over-relying on user consent, which is not always significant in the complicated digital world. In addition, academics, including Narayanan (2024), have discussed the definition of such a concept as data fiduciaries that the Act proposes. The concept introduces a responsibility of care on organisations that handle personal information, thus making them more responsible. But there have been apprehensions about the sweeping exceptions that have been given to government agencies and this could compromise the right to privacy. The enforcement mechanisms provided in the Act have also been brought into the limelight of policy analyses and online legal commentaries. The creation of Data Protection Board of India is regarded as the right move in terms of compliance. Yet, there are still inquiries about the autonomy and the ability of the Board to efficiently control a fast-changing digital ecosystem.

3.3 Operationalization phase: DPDP rules and compliance challenges

Operationalization of the DPDP Act was a decisive step that came with the coming up with the Digital Personal Data Protection Rules, 2025. The literature during this period is founded on the fact of the implication of the regulatory framework and the challenges that organizations face in achieving compliance. Such consulting firms as EY (2025) and KPMG (2025) provide certain details of the compliance requirements including data mapping, consent management, information about breaches and the appointment of Data Protection Officer. These studies point out that despite the fact that the Rules are a relief in providing visibility; they are accompanied with significant compliance costs on business entities, particularly small and medium-sized organisations.

Accountability and transparency are also the values which are underlined in the scholarly debates at this stage. Procedural protections are also included in the Rules as they enhance data governance and reduce the risk of data breaches (Singh, 2025). Nevertheless, these protective measures are limited by the presence of institutional capacity and enforcement. Law blogs and policy platforms have served as important tools in distributing real-time information in regard to regulatory developments. The sources will offer a realistic understanding of the challenges in the implementation of the DPDP framework, including the challenges in obtaining a meaningful consent, addressing cross-border data flows, and providing cybersecurity.

3.4 AI regulation and Legal gaps

The next aspect that scholars have come to appreciate is that AI systems are dependent on massive datasets, hence the importance of data protection laws in AI regulation. Nevertheless, the lack of a specific AI legislation in India has been a recurrent pattern in the scholarly literature. Jain and Yadav (2026) assert that the use of the current legal frameworks to govern AI in India brings about ambiguity and uncertainty, especially in liability and accountability. According to the authors, these gaps require an all-encompassing AI-specific legislation.

The comparative studies have also become prominent where researchers have been studying the approach of India in comparison to global structures. The AI Act of the European Union is commonly referred to as a template of risk-based regulation. Bradford (2025) asserts that the approach adopted by the EU is more predictable and clear, unlike the incremental approach adopted by India, which is flexible and has no coherency. The other new field of literature is that of the ethical implications of AI. As scholars of the field, like Floridi (2024), note, ethical guidelines are required to tackle the problem of algorithmic bias, discrimination, and transparency. These issues are especially important in the Indian context, where the socio-economic environment is rather diverse, and AI systems can contribute to the enhancement of the existing disparities.

3.5 Emerging issues: deepfakes, misinformation, and digital harm

In recent literature, there has been also interest in the emergence of AI-generated content, such as deepfakes and fake news. Legal regulation is posed a major challenge by these developments, which may compromise democratic procedures and rights of individuals. The studies have shown that despite the amendments that have been made to IT Rules to introduce such provisions as labeling the content and takedown requirements, the implementation is a significant problem. As Kumar (2026) notes, the pace of AI technological evolution exceeds regulatory action, which leads to the constant gap between the law and practice.

All in all, the literature is rather indicative of an agreement that India has gone a long way in establishing a legal framework on data protection and digital governance. However, it also indicates several issues that remained open, including:

- Absence of overall AI legislation.
- Misunderstanding of responsibility and accountability.
- Constraints of enforcement and institutional capacity.
- AI and its ethical and societal implications.

The literature highlights the necessity of the comprehensive and progressive treatment of digital governance, combining legal, technological, and ethical aspects.

4. Research methodology

The current research will take the form of a doctrinal and analytical research methodology, where the study will utilize only the secondary sources of data. This methodology fits the research as it is legal and policy-based, which means that the study is based on the analysis and interpretation of the existing laws, regulations, and academic literature.

4.1 Nature of research

The study is qualitative because it will critically analyze legal frameworks and policy developments concerning artificial intelligence and data protection in India. It includes no empirical data gathering but, on the contrary, it is based on textual analysis of the legal documents and academic literature.

4.2 Sources of data

The research is founded on a total of secondary data, and this entails:

Statutory Sources

Digital Personal Data Protection Act, 2023.
Information Technology Act, 2000.
IT Rules, 2021 and future amendments (until 2026)
Digital Personal Data Protection Rules, 2025.

Judicial Sources

Such landmark cases include Justice K.S. Puttaswamy v. Union of India (2017).

Books and Academic Literature.

Research literature regarding data protection, cyber law, and AI governance.
Articles in peer-reviewed journals (2021-2026).

Government Publications and Policy Reports.

Ministry of Electronics and Information Technology (MeitY) Reports.
Reports of committees (e.g., Srikrishna Committee).

Online Sources

Legal commentaries and blogs.
Consulting firms (EY, KPMG, etc.) reports.
Policy analysis forums and research organizations.

5. Description and Analysis

The history of the digital legal regulation in India also indicates progressive, but still important change of a system of fragmented regulation to a more organized and holistic system. The growing value of data as a strategic asset and the accelerated adoption of Artificial Intelligence (AI) technologies in industries have contributed to this change. The current section gives a specific understanding of the legal processes, institutional dynamics and the new issues in the regulation of data protection and AI in India.

5.1 Evolution of data protection framework in India

The process of India moving towards the creation of a comprehensive data protection regime has been gradual and policy-based. Key milestones are demonstrated in the table below:

Year	Legal/Policy Development	Significance
2000	Information Technology Act	Foundation of cyber law in India
2011	IT Rules on Sensitive Personal Data	Limited data protection framework
2017	Puttaswamy Judgment	Privacy recognized as a fundamental right
2018	Srikrishna Committee Report	Proposed comprehensive data protection law
2023	DPDP Act enacted	First full-fledged data protection law
2025	DPDP Rules notified	Operationalization of the Act
2025–2027	Phased implementation	Gradual compliance mechanism

This development can be described as the shift towards proactive rules as opposed to reactive rules. The establishment of privacy as a basic right, coupled with the constitutional basis of the law on the necessity of change, is the initial step in the law, and the DPDP Act is the final step in the policy-making process over the years.

5.2 Key Features of the digital personal data protection act, 2023

The DPDP Act presents a number of significant aspects that change the concept of data governance in India. These are summarized below:

Feature	Description	Implications
Consent-based processing	Data processing requires informed consent	Enhances individual autonomy
Data Principal Rights	Access, correction, erasure	Strengthens user control
Data Fiduciary Obligations	Duty of care, security safeguards	Promotes accountability
Significant Data Fiduciaries	Additional compliance requirements	Risk-based regulation
Data Protection Board	Adjudicatory authority	Institutional enforcement
Penalties	Up to ₹250 crore	Strong deterrence

The Act indicates a change in terms of a rights-based approach in line with global data protection requirements. Nevertheless, critics believe that its effectiveness can be watered down by broad exemptions of state agencies.

5.3 Institutional mechanisms and enforcement

The enforcement mechanism is a very vital aspect of any given legal framework. The act of DPDP creates the Data Protection Board of India which competes to resolve disputes, impose penalties and compliance.

Nevertheless, there are a number of difficulties that occur in this respect:

- **Institutional capacity:** The performance of the Board is based on its technical skills and resources.
- **Independence:** Concerns have been expressed regarding potential executive influence.
- **Enforcement efficiency:** Due to the size of the data processing in India, enforcement might experience practical constraints.

The effectiveness of the DPDP framework will highly rely on the capacity of the institutions to enforce the law.

5.4 AI regulation in India: An indirect approach

In contrast to other countries like the European Union, India does not have a single law which directly governs AI. Rather, AI is regulated by a mixture of:

- Data protection laws (DPDP Act, 2023)
- IT Rules and intermediary guidelines.
- Sector-specific regulations

This method can be described as the indirect regulation, with the emphasis on the results of AI systems, as opposed to technology.

Aspect	India's approach	Implication
AI-specific law	Absent	Regulatory ambiguity
Focus	Output-based regulation	Flexible but unclear
Liability	Not clearly defined	Legal uncertainty
Ethical standards	Emerging but non-binding	Weak enforcement

Although, this model is flexible and promotes innovation, it also introduces loopholes including accountability, transparency, and liability.

5.5 Emerging legal challenges

The combination of AI and data technologies has created a number of difficult legal issues:

5.5.1 Privacy vs Innovation

The training and operation of AI systems consume huge volumes of data. The high consent requirements by the DPDP Act can inhibit access to data, hence, innovation. The problem of privacy and technological progress is one of the most important issues.

5.5.2 Algorithmic Bias and Discrimination

Artificial intelligence systems are prone to biases in the training data. This may cause discriminatory results especially in sensitive fields like employment, credit rating and law enforcement. There is a gap in the lack of explicit legal provisions on algorithmic bias.

5.5.3 Deepfakes and Misinformation

The emergence of generative AI has made possible the production of deepfakes and synthetic media, which is highly dangerous to:

- Democratic processes
- Public trust
- Individual reputation

Though the recent changes in the IT Rules obligate labeling and takedown of such content, it is difficult to enforce them.

5.5.4 Data Breaches and Cybersecurity

Even with regulatory protection, data breaches are still being experienced, which underscores the importance of more robust cybersecurity. Companies usually struggle to adopt effective data security measures.

5.6 Comparative analysis: India and global frameworks

Criteria	European Union	India
Data Protection	GDPR (comprehensive)	DPDP Act (emerging)
AI Regulation	AI Act (risk-based)	No dedicated law
Enforcement	Strong institutional framework	Developing institutions
Approach	Strict and rights-focused	Flexible and incremental

This strategy of India represents its developmental priorities and socio-economic background. Although it is flexible, it is not as clear and comprehensive as the EU model.

5.7 Need for a comprehensive AI framework

The discussion shows that there is an urgent necessity of an exclusive AI regulatory framework in India. Such a framework must cover:

- Responsibility of AI-related damage.
- Transparency and explainability
- Social responsibility and morality.
- Risk based classification of AI systems.

Without such a structure, there may be regulatory loopholes, and this may undermine the confidence of the people and the rule of law.

6. Conclusion

The introduction of Digital Personal Data Protection Act, 2023, and the subsequent declaration of the Digital Personal Data Protection Rules, 2025 are the significant milestones in the development of an efficient and properly structured system of data protection. These legal instruments indicate that the Indian state is consciously trying to adjust its regulatory environment to the global standards and is addressing the issues peculiar to its socio-economic environment. The performance appraisal performed in this research article demonstrates that India has come a long distance in order to improve its data governance architecture. The shift towards a rights-based and responsible framework is reflected in the introduction of a consent-based model, the consideration of the individual rights, and the creation of institutional instruments, such as the Data Protection Board. In the meantime, the strategy of phased implementation may be regarded as a realistic reaction that will aim at balancing regulatory compliance and simple compliance.

Nevertheless, the paper also identifies a number of essential issues that are still not addressed. Lack of a specific legal framework on Artificial Intelligence also brings ambiguity in terms of liability, accountability and ethical governance. Indirect regulation, however flexible, may be inadequate to deal with the multifaceted risks of AI systems, such as algorithmic bias, deepfakes, and automated decision-making. Moreover, the issues of enforcement capacity, institutional independence as well as exemptions provided to state agencies cast doubt on the efficiency of the current structure. The pace of technological change is only adding to these barriers and this necessitates legal and policy responses that are continually changing. Considering these results, it is crucial that India will become more integrated and progressive in terms of digital governance. This involves the introduction of an overall AI legislation, reinforcement of regulatory standards, and integration of ethics in regulatory frameworks. Such actions would not only increase the legal certainty, but would also guarantee that technological innovation is consistent with the constitution and the best interests of the society. To sum up, although the digital legal system is being developed in India in the correct direction, the continuous work is necessary to close the gaps and establish a strong, inclusive, and rights-based system of governance in the digital era.

References

1. Beck U. *Risk society: towards a new modernity*. London: Sage, 1992.
2. Beck U. *The metamorphosis of the world: how climate change is transforming our concept of the world*. Cambridge: Polity Press, 2016.
3. Brooks N, Grist N, Brown K. Development futures in the context of climate change: challenging the present and learning from the past. Dev Policy Rev. 2009;27(6):741–65.
4. Chakrabarty D. The climate of history: four theses. Crit Inq. 2009;35(2):197–222.
5. Denter P. Motivated reasoning and the political economy of climate change inaction. arXiv, 2011.
6. Foucault M. *Discipline and punish: the birth of the prison*. New York: Pantheon Books, 1977.
7. Foucault M. *Power/knowledge: selected interviews and other writings*. New York: Pantheon Books, 1980.
8. Hossain MN. The ethics of climate change: a philosophical analysis of the moral obligations of individuals and nations. Res Rev Int J Multidiscip. 2006;10(8):1–5.
9. Klein N. *This changes everything: capitalism vs. the climate*. New York: Simon & Schuster, 2014.
10. Kivle B, Espedal G. Values in climate discourse. Front Commun. 2019;7:1.
11. Knight FH. *Risk, uncertainty and profit*. Boston: Houghton Mifflin, 1925.
12. Lucarini V. Towards a definition of climate science. arXiv, 2004.
13. Polanyi K. *The great transformation: the political and economic origins of our time*. Boston: Beacon Press, 1944.
14. Porritt J. *Breaking new ground: mining, minerals and sustainable development*. London: Earthscan, 2002.
15. O'Brien K, et al. Social transformation in response to global environmental change. Ambio. 2014;43(4):376–90.
16. Rodríguez-Madariaga M. *Ethics and sustainability: human dignity and solidarity*. Vatican City: Pontifical Academy of Sciences, 2018.
17. Srivastav S, Rafaty R. Political strategies to overcome climate policy obstructionism. arXiv, 2009.
18. Sunstein CR. *Climate justice: what rich nations owe the world—and the future*. Cambridge (MA): Harvard University Press, 2009.
19. World Commission on Environment and Development. *Our common future*. Oxford: Oxford University Press, 1987.