The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DIGITAL AND AI GOVERNANCE IN INDIA:

CHALLENGES OF DATA PRIVACY AND ACCOUNTABILITY

~Surbhi Tripathi

ABSTRACT

Artificial Intelligence has rapidly evolved into an integral part of India's digital democracy. It has resulted in heading towards dignified digital governance. The revolutionary impact of Artificial Intelligence in governance has been clearly visible in the fields of healthcare, agriculture, finance, banking, law, etc., posing serious implications on transparency, accountability and efficiency of government machinery. This paper addresses how issues of data privacy and government accountability coexist within India's development of its digital governance framework. By analysing the law, policy reviews and case studies related to India's Digital Personal Data Protection Act 2023, we will identify gaps in the current regulatory framework and evaluate whether sufficient institutional mechanisms exist to regulate the growing area of digital technologies such as artificial intelligence (AI), algorithmic decision-making for public welfare programs and biometric surveillance systems. Globally, countries are taking significant steps to formulate ethical principles and practical guidelines to ensure citizens' digital rights and effective public administration. This paper suggests a systemic approach to an efficient regulatory framework for digital governance by encompassing technical experts, policymakers, and legal professionals, all responsible for the better implementation of artificial intelligence in civil society. Our research suggests that effective digital governance in India requires not only legislative reform but also the creation of a truly independent and empowered Data Protection Authority, the enforcement of algorithmic transparency, and the provision of appropriate remedies for citizens harmed by poor governance decisions. Finally, we provide recommendations for developing a rights-based accountability framework for India's socio-legal context.

Keywords: *Artificial Intelligence; AI Regulation in India; Data Privacy; AI Governance; Digital Personal Data Protection Act; Algorithmic Accountability; Surveillance and Digital Rights; Global comparative frameworks*

1. INTRODUCTION

In the contemporary world, marked by the growth of digital technologies, almost all spheres of human life have transformed. One such instrument is Artificial Intelligence (AI), which has become a potent means of influencing decision-making in various industries such as healthcare, finance, education, governance, and law enforcement. The transformation has not only provided new grounds for economic growth and 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. The enactment of the Digital Personal Data Protection (DPDP) Act, 2023, is an umbrella legislation that has empowered data protection and digital autonomy. The Hon'ble Supreme Court recognised the right to privacy as a fundamental right in the case of Justice K.S. Puttaswamy v. Union of India[1], which marked a notable turning point in India's digital governance journey. However, the actual effective enforcement of digital governance with emerging technologies like Artificial Intelligence (AI) is still ongoing. India's digital landscape has evolved significantly with the advent of artificial intelligence, posing serious challenges to the digital autonomy and legal accountability of government machinery.

This paper critically examines the interrelationship between data privacy, autonomy, and effective digital governance. To bridge the gap between innovation and data privacy, there is a need for a robust legislative and institutional framework to ensure compliance with cross-border AI enforcement mechanisms. In addition to this, it analyses the legislative framework regarding digital governance and government accountability in comparison to other countries.

2. RESEARCH QUESTIONS

The central questions in this research are:

- Does India's current legal and institutional framework adequately protect citizens' digital rights?

[1] *Justice K.S. Puttaswamy v. Union of India,* (2017) 10 SCC 1 (India).

- What reforms are necessary to build a governance model that is both constitutionally grounded and practically effective?

To answer these questions, this paper undertakes a qualitative, doctrinal, and comparative analysis.

3. LITERATURE REVIEW

3.1 GLOBAL FRAMEWORKS FOR DATA PRIVACY AND AI GOVERNANCE

Due to the number of high-profile data breaches and the increasing ability of both state and non-state actors to watch citizens, researchers have worked much harder at establishing the rules that govern data privacy than they have in the past. According to Westin[2], the right to privacy is an integral right of an individual to control their personal information; this definition laid the foundational stone for statutes such as the EU's General Data Protection Regulation (GDPR)[3]. There was a heated argument about calling personal data a commodity with the rise of surveillance capitalism by Zuboff [4]. Henceforth, considering this imbalance of power between data principals and data fiduciaries, the authenticity of data governance was largely questioned. These international frameworks for privacy are now used as a standard by which regulators in developing countries have established their responses to emerging regulations.

Scholars have critically examined the regulatory challenges of machine learning systems and the competing demands for both innovation and protection for rights regarding those systems in terms of AI governance.[5] The OECD Principles on Artificial Intelligence and the European Union's AI Act[6] are the foundations of key multilateral norms of fairness, accountability and transparency. However, Jobin et al.[7] find in their comparative analysis of AI ethics guidelines that many of the principles are still aspirational and that there is a gap between normative

[2] Alan F. Westin, *Privacy and Freedom* (1967).
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of Natural Persons with regard to the processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.
[4] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019).
[5] Allan Dafoe, *AI Governance: A Research Agenda, Future of Humanity Inst.,* Univ. of Oxford (2018); Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap,* 51 U.C. Davis L. Rev. 399 (2017).
[6] OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (May 21, 2019), https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449; Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 1689) 1, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.
[7] Anna Jobin, Marcello Ienca & Effy Vayena, *The Global Landscape of AI Ethics Guidelines,* 1 Nature Mach. Intelligence 389 (2019).

aspirations and actual capacity to implement those principles - a pattern evident in the developing world.

3.2 DATA PRIVACY GOVERNANCE IN INDIA: LEGISLATIVE EVOLUTION

Many scholars have examined how data protection laws have evolved over time in this digital era in India. Interestingly, Indian research-based scholar Prasad[8] has outlined the key developments of the Justice B.N. Srikrishna Committee Report on "A Free and Fair Digital Economy: Protecting Privacy, Empowering Citizens" and the Joint Parliamentary Committee (JPC)[9], which have played a decisive role in highlighting the journey from the Information Technology Act, 2000[10], towards the enactment of the Digital Data Protection Act, 2023[11]. Each of these pathways acted as the guiding light in creating balance between individual privacy and state interests in distinctive ways. Further, Bhatia and Bhatt[12] critically argued that individual privacy concerns have been gradually diluted, and the resultant legislation favoured the government authorities and large establishments, raising concerns about arbitrary regulations.

In the context of India's digital governance constraints, scholars have examined a case-based study on the Aadhaar biometric identification system.[13] Although the Supreme Court upheld the constitutionality of the Aadhaar scheme in the Justice K.S. Puttaswamy II case[14], dissenting opinions and subsequent academic commentary point to substantial risks of exclusion, mission creep and lack of meaningful consent for disenfranchised groups who have enrolled into the Aadhaar system as part of social welfare schemes. These contributions highlight the socially uneven nature of decisions related to data governance.

3.3 INSTITUTIONAL AND ACCOUNTABILITY MECHANISMS

[8] S. Prasad*, India's Evolving Data Protection Framework,* 11 NUJS L. Rev. 1 (2018).
[9] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians,* Ministry of Electronics & Information Technology, Government of India (2018); Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, Report, Lok Sabha, Government of India (2021).
[10] Information Technology Act, No. 21 of 2000, India Code.
[11] Digital Personal Data Protection Act, No. 22 of 2023, India Code.
[12] G. Bhatia & S. Bhatt, *The Dilution of Data Rights: A Critique of India's Personal Data Protection Bill*, 57 Econ. & Pol. Wkly. 22 (2022).
[13] Usha Ramanathan, Aadhaar, the State and Surveillance: Reflections on a Decade of Biometric Governance*,* 13 S. Asian Hist. & Culture 299 (2022*)*; Smriti Parsheera, *The Aadhaar Ecosystem: Data Governance Challenges* (National Institute of Public Finance & Policy, Working Paper No. 345, 2021).
[14] *Justice K.S. Puttaswamy (Aadhaar-5 J.) v. Union of India,* (2019) 1 SCC 1 (India).

Researchers have investigated the future structure of Data Protection Authorities in India. As per the study of Kohli and Singh[15], the genesis of India's proposed Data Protection Board has been inspired by the similar regulatory bodies of the UK Information Commissioner and the German Federal Commissioner for Data Protection. There were some structural issues found in the study, primarily the executive functions of the appointment of board members and having limited adjudicatory functions.

Furthermore, it has been contended that an effective overview of AI cannot be achieved through internal coordination in the executive branch. Instead, it demands the active involvement of a diversified group of stakeholders, inclusive of civil society members, technical experts and communities that are directly affected by AI mechanisms.[16]

Conclusively, this area of literature has grown rapidly and is highly debated. In particular, the Indian scholars have made notable contributions by critically examining the structuring of the legislative framework based on digital governance and scrutiny and how effective these are in implementation. However, apart from its effective applicability, certain gaps highlight the risk of digital privacy that this paper aims to address.

3.4 CONSTITUTIONAL DIMENSION OF DIGITAL GOVERNANCE

This paper significantly highlights the importance of doctrinal research in the constitutional dimension of digital governance. In particular, the role of fundamental rights is unprecedented in shaping the discourse of data protection. Studies carried out by notable scholars have firmly inclined towards the disproportionate impact laid down upon the marginalised communities due to the biometric surveillance bias. Precisely, their research pointed to the systemic bias of algorithmic machineries that often led to social inequalities.[17] These studies are responsible for efficiently highlighting the need for the right to privacy under Article 21 to be read with the right to equality under Article 14[18], thereby ensuring that the State abides by fairness, accountability, and transparency in AI-driven governance systems. Henceforth, strengthening

[15] A. Kohli & P. Singh, *Independence and Design of India's Data Protection Authority: A Comparative Assessment,* 33 Nat'l L. Sch. India Rev. 1 (2021).
[16] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, supra note 9; A. Verma, *Multi-Stakeholder Governance for AI in India: Lessons from Emerging Regulatory Practice,* 5 J. Sci. & Tech. Pol'y 18 (2023).
[17] S. Narayan, *Predictive Policing and the Criminalisation of Marginalised Communities in India,* 58 Econ. & Pol. Wkly. 34 (2023); S. Chakraborty, *Biometric Surveillance and the Erosion of Public Privacy in India*, 14 J. Human Rights Practice 45 (2022).
[18] India Const. art. 21; id. art. 14.

the contention that digital governance is fundamentally rooted in constitutional morality rather than mere technological advancements.

4. RESEARCH GAP

There is already a great deal of research that enhances our knowledge of the legal framework surrounding the usage of data in India with respect to data privacy and emerging challenges related to artificial intelligence governance. Artificial Intelligence has been the paradigm shift towards digital governance, making the implementation of digital literacy prompt and efficient. Primarily, most of the research that has examined this topic has either employed a legislative lens or focused on the technological aspect of computer technology without connecting data privacy regulations with AI technologies as being interrelated parts thereof. Secondly, most of the existing literature does not investigate a considerable number of marginalised groups (e.g., rural Indians, disabled individuals, etc.) and their intersections with respect to the pervasive nature of surveillance.

Thirdly, there is a lack of literature comparing India's data privacy and artificial intelligence governance challenges with those faced by other Asian countries (Singapore, Japan and South Korea). This limited cross-country comparison reduces our ability to learn from their similar legal systems. Lastly, no substantive analysis has been done on how the Digital Personal Data Protection (DPDP) Act of 2023 will function after it has been implemented. The intended purpose of this paper is to fill these gaps by utilising doctrinal and comparative mechanisms and positioning the findings within the constitutional framework.

5. METHODOLOGY

This research is a qualitative, doctrinal, and interpretive study that is appropriate for the primarily legal and policy-oriented nature of this question. The study does not produce original empirical data through surveys or fieldwork; instead, it relies upon a systematic approach to using primary and secondary sources to develop an analytical representation of the current digital governance environment in India.

5.1 PRIMARY SOURCES

Constitutional provisions (i.e., Articles 19 and 21 of the Constitution of India)[19], Acts (e.g., the Information Technology Act of 2000, the Aadhaar Act of 2016, and the Digital Personal Data

[19] India Const. arts. 19, 21.

Protection Act of 2023)[20], subordinate legislation, and policy documents constitute the primary sources. The Supreme Court and High Court of India's rulings, especially those in the Justice K.S Puttaswamy v. Union of India[21] case, as well as parliamentary committee reports and regulatory decrees, are being treated as the primary sources of law. The primary sources will be evaluated doctrinally to evaluate their reach, internal arrangement and compliance with the Constitution.

5.2 SECONDARY SOURCES

The secondary sources used are peer-reviewed academic publications, working papers, publications from civil society like Access Now, the Internet Freedom Foundation and the Centre for Internet and Society[22], investigations from independent journalists, and international regulatory regimes such as GDPR, OECD A.I. Principles and UNESCO Ethical recommendations regarding A.I. Systems[23]. The systematic literature review process is conducted through searches conducted through the databases of Google Scholar, HeinOnline, and JSTOR using search terms such as "data privacy in India," "India AI governance," "DPDP Act", and "algorithmic accountability."

5.3 ANALYTICAL FRAMEWORK

The analysis will use three normative dimensions of democratic governance: rights-based approach, institutional accountability and participatory legitimacy. Each of these dimensions will be used to assess business processes, legislation, institutions, and technology. Some comparative examples from other jurisdictions, particularly with regard to the European Union, will also be consulted as appropriate in order to help identify potential regulatory frameworks.

6. ANALYSIS AND FINDINGS

6.1 LEGISLATIVE FRAMEWORK: STRENGTHS AND WEAKNESSES OF THE DPDP ACT, 2023

The Digital Personal Data Protection Act, 2023, is the first extensive data protection law in India and a significant normative achievement. The Act creates a consent-driven processing

[20] Information Technology Act, *supra* note 10; Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, India Code; Digital Personal Data Protection Act, *supra* note 11.
[21] *Justice K.S. Puttaswamy (Aadhaar-5 J.) v. Union of India*, *supra* note 14.
[22] Internet Freedom Found., *Project Panoptic: Facial Recognition Tracker* (2023), https://panoptic.in.
[23] Regulation 2016/679, *supra* note 3; OECD, *supra* note 6; UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (Nov. 23, 2021), https://unesdoc.unesco.org/ark:/48223/pf0000380455.

model, enumerates data principal rights such as the right of access, correction and erasure, and requires data fiduciaries to provide security protections. The establishment of a quasi-judicial adjudicative body in the form of the Data Protection Board is a favourable institutional change.

However, there are some clauses in the Act that go a long way in sabotaging its protective mandate. Section 17 gives blanket immunities to both the central and state governments to use in matters such as national security, public order, and sovereignty, without defining immunities or any independent check of the immunities.[24] This structure reflects the criticism that the state exempts itself from the norms that it applies to others. Although the consent framework is formally sound, there is no meaningful operationalisation of the coerced or asymmetric consent scenarios, especially when it comes to welfare access via Aadhaar. Moreover, the Act does not set any explicit transparency or impact evaluation criteria related to algorithms, which means that AI-based decisions remain mostly unregulated.

6.2 INSTITUTIONAL ACCOUNTABILITY: DATA PROTECTION BOARD

The Data Protection Board, as formed by the DPDP Act, poses significant independence issues. The central government appoints the board members via a process that considers parliament, civil society and the judiciary. This method of appointing officers does not align well with the GDPR framework, where the supervisory bodies are formally independent of both government and industry. Some restrictions are also imposed on enforcement powers: the Board can impose financial penalties but has no investigative powers at the level of regulators like the Information Commissioner's Office in the UK. Another limitation to proactive enforcement is the lack of powers of a suo motu inquiry.

7. DISCUSSION

This study highlights the dynamic governance machinery. It is changing from being a regulatory vacuum (as it was before 2023) to one that is not fully committed to protecting people’s rights through an accountable framework, based on the requirements of the Indian Constitution and the country’s size (including over a billion people).

When we examine these issues holistically, we find three overarching tensions.

The first of these tensions is between security and privacy. Within the DPDP Act, there exist vast and flexible exemptions available to government agencies for cases where the need for

[24] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023), § 17.

security trumps any obligation to protect an individual's right to privacy. It is widely accepted that some level of national security exemption from privacy laws is necessary globally; whereas the Indian system is unusual in that it has such broad exemptions as well as no independent agencies or courts to oversee or provide checks on these types of exemptions, thereby making it difficult to balance individual privacy with state security.

The second aspect of AI deployment is the normalisation of technologies such as mass facial recognition systems, predictive scoring, and automated welfare decision-making processes, without legal authority, impact assessments and mechanisms for redress, indicates a governance approach that values operational efficiency more than compliance with rights. By way of international best practice, examples include the EU's prohibition on certain high-risk AI applications as part of the EU AI Act, which should be considered by Indian policymakers.[25] Civil society and the judiciary also provide an important countervailing force to the lack of strong statutory protection through litigation by groups like the Internet Freedom Foundation[26] and investigative journalism on deployments of surveillance technologies, thus creating pressure for accountability where formal institutions do not. Accordingly, independent journalism, adequate access to RTIs, and a well-funded legal aid system must be supported as part of an effective ecosystem of digital governance.

In comparison, India's path differs from both the EU's heavily regulated model and the US's sector-specific approach, making an Indian-style governance necessary that balances innovation, constitutional rights, and development priorities within a middle-income democratic society. This new governance paradigm must be developed using stakeholder engagement over time and through independent regulatory design as well as commitment to measuring the outcomes of technologies deployed against measurable rights.

8. CONCLUSION

The development of digital governance in India has made significant advances towards creating a robust system that ensures digital independence and transparency. The advent of India's digital transformation has marked one of the ambitious achievements of the 21st Century. The Digital Personal Data Protection Act of 2023 is the primary legislative framework that recognises citizens' digital rights with respect to personal data.

[25] Regulation (EU) 2024/1689, *supra* note 6, art. 5.
[26] Internet Freedom Found., *supra* note 22.

This research paper provides a milestone in accomplishing significant development in lieu of digital data governance. Moving towards the rights and responsibility paradigm is illustrated by such measures as introducing a consent mechanism, taking into account individual rights, and setting up institutional mechanisms, including the Data Protection Board. Meanwhile, phased implementation can be viewed as a reasonable response to achieving the balance between regulatory and simple compliance.

However, the research paper shows that the lack of legislation on Artificial Intelligence creates ambiguity in liability, accountability, and ethical aspects of governance. In addition to the legislative and institutional reforms, there is an urgent need to build a digital constitutionalism in India. This primarily includes the enshrinement of fundamental rights such as privacy, equality and dignity into the very cornerstone of digital technologies. Strengthening public awareness and citizens' participation regarding digital literacy allows them to become not merely passive data providers, but active stakeholders in the government machinery. Furthermore, India needs to invest in robust capacity-building within regulatory frameworks and encourage the inter-disciplinary accountability between legal scholars, policy makers and technocrats. Only then India can move towards the path of trustworthy digital governance with efficiency and innovation. Artificial Intelligence has emerged as a potent weapon of good governance while promoting efficiency and ethical advancement of technology.

To conclude, the future of digital governance in India largely depends on the proper implementation of laws and the critical examination of their rules along with institutions regulating them. The accountable digital governance framework is duly required for an enriching recognition of citizens' rights, at first by keeping intact democratic values and constitutional responsiveness.

9. REFERENCES

Bhatia, G. & Bhatt, S., *The Dilution of Data Rights: A Critique of India's Personal Data Protection Bill,* 57 Econ. & Pol. Wkly. 22 (2022).

Calo, R., *Artificial Intelligence Policy: A Primer and Roadmap,* 51 U.C. Davis L. Rev. 399 (2017).

Chakraborty, S., *Biometric Surveillance and the Erosion of Public Privacy in India,* 14 J. Human Rights Practice 45 (2022).

Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians,* Ministry of Electronics & Information Technology, Government of India (2018).

Dafoe, A., *AI Governance: A Research Agenda, Future of Humanity Inst.,* Univ. of Oxford (2018).

Internet Freedom Foundation, *Project Panoptic: Facial Recognition Tracker* (2023), available at https://panoptic.in.

Jobin, A., Ienca, M. & Vayena, E., *The Global Landscape of AI Ethics Guidelines,* 1 Nature Mach. Intelligence 389 (2019).

Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, Report, Lok Sabha, Government of India (2021).

Kohli, A. & Singh, P., *Independence and Design of India's Data Protection Authority: A Comparative Assessment,* 33 Nat'l L. Sch. India Rev. 1 (2021).

Narayan, S., *Predictive Policing and the Criminalisation of Marginalised Communities in India,* 58 Econ. & Pol. Wkly. 34 (2023).

OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (May 21, 2019), available at https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449.

Parsheera, S., *The Aadhaar Ecosystem: Data Governance Challenges,* National Institute of Public Finance & Policy, Working Paper No. 345 (2021).

Prasad, S., *India's Evolving Data Protection Framework,* 11 NUJS L. Rev. 1 (2018).

Ramanathan, U., *Aadhaar, the State and Surveillance: Reflections on a Decade of Biometric Governance,* 13 S. Asian Hist. & Culture 299 (2022).

UNESCO, Recommendation on the Ethics of Artificial Intelligence (Nov. 23, 2021), available at https://unesdoc.unesco.org/ark:/48223/pf0000380455.

Verma, A., *Multi-Stakeholder Governance for AI in India: Lessons from Emerging Regulatory Practice,* 5 J. Sci. & Tech. Pol'y 18 (2023).

Westin, *A.F., Privacy and Freedom* (1967).

Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019).

Statutes, Constitutional Provisions, and International Instruments

India Const. arts. 14, 19, 21.

Information Technology Act, No. 21 of 2000, India Code.

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, India Code.

Digital Personal Data Protection Act, No. 22 of 2023, India Code.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1, available at https://eurlex.europa.eu/eli/reg/2016/679/oj/eng.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 1689) 1, available at https://eurlex.europa.eu/eli/reg/2024/1689/oj/eng.

Cases

Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

Justice K.S. Puttaswamy (Aadhaar-5 J.) v. Union of India, (2019) 1 SCC 1 (India).