Digital Personal Data Protection Act, 2023 and the vision of Viksit Bharat@2047: towards sustainable digital governance and inclusive growth in India

Lokanath Patra
Assistant Professor, Ganjam Law College, Berhampur, Odisha, India
*Corresponding Author: Lokanath Patra
Received 9 March 2026; Accepted 13 Apr 2026; Published 6 May 2026
DOI: https://doi.org/10.64171/JSRD.5.S1.197-201

Abstract
The establishment of a secure, rights-respecting, and innovation-friendly digital ecosystem is inextricably linked to India's aspiration to become a developed and inclusive nation by 2047, as envisioned under Viksit Bharat@2047. The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), is a significant milestone in India's journey toward sustainable digital governance. The Act endeavors to strike a balance between the requirements of economic development, digital public infrastructure, and technological innovation, and the privacy rights of individuals. This paper critically evaluates the DPDP Act, 2023, as a legal and institutional framework for promoting India's digital transformation while simultaneously protecting the fundamental right to privacy as enshrined in Article 21 of the Indian Constitution.
The study employs a doctrinal and analytical methodology, based on constitutional jurisprudence, specifically the Supreme Court's decision in Justice K.S. Puttaswamy v. Union of India. It also includes comparative references to global data protection regulations, such as the EU's GDPR. This paper assesses the DPDP Act's main provisions on consent, data fiduciary obligations, cross-border data transfers, and enforcement mechanisms, with an emphasis on their implications for digital inclusion, trust, and accountability. It also investigates the potential of effective data stewardship to enhance India's digital public infrastructure and encourage citizen engagement in the digital economy.
The paper contends that the DPDP Act is a progressive step toward aligning privacy protection with developmental objectives; however, there remain gaps in institutional independence, proportionality, and remedies for data principals. The study concludes by underscoring the necessity of rights-centric governance, regulatory clarity, and robust implementation to ensure that data protection is a fundamental component of India's sustainable and inclusive digital future, in line with the Viksit Bharat@2047 vision.

Keywords: Digital Personal Data Protection Act 2023, Right to privacy, Digital governance, Viksit Bharat@2047, Sustainable development

1. Introduction

India's rapid digital transformation is crucial to Viksit Bharat@2047's goal of developing the nation by 2047. Aadhaar, UPI, DigiLocker, and several e-governance systems have helped India become one of the world's greatest digital societies over the past decade. These programs have improved public services, financial inclusion, and citizen participation while boosting economic growth and innovation (NITI Aayog, 2021) [10]. This data-driven governance paradigm has also led to the mass collecting, processing, and storage of personal data, creating privacy, surveillance, data misuse, and autonomy problems.

In a constitutional democracy, digital development must respect fundamental rights. In its historic Justice K.S. Puttaswamy v. Union of India (2017) [6] ruling, the Supreme Court of India declared the right to privacy an essential part of life and personal liberty under Article 21 of the Constitution. Informational privacy and data control are important to human dignity and freedom, the Court said. This judgment changed India's constitutional jurisprudence, requiring a comprehensive data protection system that meets the requirements of legality, necessity, proportionality, and procedural safeguards (Bhandari, 2018) [2].

Data protection is essential to democratic governance and sustainable development worldwide. The EU's General Data Protection Regulation (GDPR) takes a rights-based strategy to balance technological innovation with robust privacy and data controller responsibility (Kuner, Bygrave, & Docksey, 2020) [8]. India's previous legal regime primarily governed by the Information Technology Act, 2000, and its accompanying rules was widely criticized for being fragmented, antiquated, and unable to manage modern data processing ecosystems (Chander & Le, 2015) [3].

India passed the Digital Personal Data Protection Act, 2023, to comply with constitutional requirements and global regulations. India's expanding digital governance architecture includes the Act, which regulates the processing of digital personal data while promoting innovation, economic growth, and digital public infrastructure. The DPDP Act aims to balance individual rights and developmental imperatives by

protecting privacy while allowing authorized data processing for justifiable reasons (Government of India, 2023) [5].

In Viksit Bharat@2047, inclusive growth, ethical governance, technological self-reliance, and citizen-centric development make the DPDP Act particularly relevant. Sustainable digital governance requires strong technology, public trust, transparency, and accountability. Digitalization can lead to exclusion, data misuse, and a loss of civil rights, especially for vulnerable and marginalized groups, without proper data protection (Bennett & Raab, 2020) [1].

This article critically evaluates the Digital Personal Data Protection Act, 2023, as a tool for sustainable digital governance and inclusive progress in India. It examines whether the Act implements constitutional privacy principles, adheres to global best practices, and supports India's long-term development. The paper evaluates the DPDP Act within constitutional jurisprudence and Viksit Bharat@2047 to identify gaps, assess its performance, and emphasize the significance of rights-centric data governance in defining India's digital future.

2. Objectives of the study

In the context of India's evolving digital culture, the Digital Personal Data Protection Act (DPDP Act) of 2023 is scrutinized to align with the long-term vision of Viksit Bharat@2047. The study aims to explore:

a) The constitutional basis of data protection in India, particularly the right to privacy and relevant Supreme Court cases;
b) Key aspects of the DPDP Act, including consent and data principal rights;
c) The Act's role in fostering sustainable digital governance, emphasizing privacy and data security;
d) Implications for inclusive growth and protection for marginalized groups;
e) Gaps and implementation challenges such as state exemptions and grievance mechanisms; and
f) Recommendations for legal reforms to strengthen data protection as a core element of ethical digital governance in India.

3. Research methodology

The research methodology examines the Digital Personal Data Protection Act (DPDP Act, 2023) in relation to constitutional rights and regulatory policy, utilizing a doctrinal and analytical framework for qualitative legal analysis. It is descriptive, analytical, and evaluative, focusing on the Act's constitutional validity and its implications for sustainable digital governance and inclusive development. The analysis involves comparing Supreme Court concepts, drawing on primary data from the Constitution of India and key judgments, as well as secondary sources such as books and peer-reviewed articles. The method incorporates doctrinal analysis and a comparative framework, assessing India's data protection against global standards and identifying normative gaps. The DPDP Act's impact on informational privacy and its alignment with governance frameworks, including the Viksit Bharat@2047 initiative, are considered, while limitations include the absence of empirical evaluation of implementation outcomes.

4. Indian data protection constitutional foundations

The foundational aspect of Indian data protection lies within Article 21 of the Constitution, which guarantees the right to life and personal liberty. Although privacy and data protection are not explicitly mentioned, judicial interpretations have extended Article 21 to encompass personal autonomy and dignity, particularly in the context of digitalization and government data use, thereby providing a normative basis for laws such as the Digital Personal Data Protection Act (DPDP Act), 2023.

The evolution of privacy rights in Indian law showcases a shift from earlier rulings, such as M.P. Sharma v. Satish Chandra (1954) [9] and Kharak Singh v. State of Uttar Pradesh (1963) [7], where privacy was not confirmed as a constitutional right, to the more favorable interpretations in Gobind v. State of Madhya Pradesh (1975) and R. Rajagopal v. State of Tamil Nadu (1994), which began recognizing privacy as implicit. The watershed moment was the Justice K.S. Puttaswamy v. Union of India (2017) [6] ruling, in which the Supreme Court unanimously recognized privacy as a fundamental right under Articles 14 and 19, mandating robust data protection laws.

Post the Puttaswamy ruling, privacy and data governance underwent further clarification. For instance, the Supreme Court upheld Aadhaar's validity while imposing stringent limitations on data management and stressing the necessity of proportionality in data-handling practices. Additionally, the Anuradha Bhasin v. Union of India (2020) [6] decision reinforced internet access as integral to constitutional rights, highlighting the need for a cohesive approach to digital governance grounded in accountability.

The principles of constitutional data protection legislation emphasize legality, proper purpose, proportionality, and the prevention of abuses. While the DPDP Act, 2023, outlines consent-based processing and obligations for data fiduciaries, concerns persist regarding state exemptions, the independence of the Data Protection Board, and efficacy in implementing remedies. Evaluating these features against the Puttaswamy ruling is crucial for assessing the adequacy of rights protection. Furthermore, establishing a robust data protection framework is essential to India's vision of Viksit Bharat@2047, signaling a commitment to maintaining democracy by protecting privacy, combating surveillance and data exploitation, and fostering public trust in governance amid rapid technological change. Ultimately, the DPDP Act is envisioned as a constitutional mechanism that aligns privacy rights with the evolving digital landscape.

5. Overview of Digital Personal Data Protection Act, 2023

The 2023 Digital Personal Data Protection (DPDP) Act marks India’s inaugural comprehensive regulation for digital personal data processing, responding to the Supreme Court's Justice K.S. Puttaswamy decision and addressing the needs of a data-centric economy. This Act seeks to balance privacy rights with

developmental and governance objectives, establishing a more cohesive legal framework compared to the fragmented protections under the Information Technology Act, 2000.

The DPDP Act applies both domestically and internationally to transactions involving Indian individuals, in line with a globally relevant context informed by legislation such as the General Data Protection Regulation (GDPR). It notably excludes non-digital personal data and information publicly disclosed by individuals, as well as legally mandated disclosures, potentially leaving significant data categories unprotected.

Some components of the Act include defined roles for data principals, fiduciaries, and processors, reflecting the risk levels associated with different types of data. The establishment of the Data Protection Board of India is intended to oversee compliance and enforcement. However, concerns persist about its potential lack of independence from government influence, which may compromise impartial regulation.

Consent is the cornerstone of lawful data processing under the DPDP Act, requiring it to be free, informed, and explicit. However, the Act also provides pathways for data processing without consent in specific scenarios, such as state functions and emergencies, raising questions about constitutional proportionality under the Puttaswamy framework.

Data principals are granted rights that enhance their control and transparency regarding their personal data, allowing them to obtain information, make corrections, and lodge grievances. Nevertheless, the Act imposes responsibilities on data principals, arguably complicating individuals' rights, especially those from more vulnerable sectors of society.

Responsibilities of data fiduciaries include maintaining data security, ensuring accuracy, and properly managing data retention and breaches. While the Act emphasizes accountability, it lacks explicit provisions on data minimization and purpose limitation, which are critical under the GDPR.

Regarding international data transfers, the DPDP Act permits the transfer of personal data to countries identified by the Central Government, signaling India's integration into the global digital economy. However, the absence of concrete criteria for assessing the adequacy of these foreign jurisdictions raises concerns about the protection of data principals' rights once their data is transferred abroad.

The Act also outlines exceptions for national security and public safety that warrant scrutiny to ensure their proportional application. Despite imposing hefty penalties for non-compliance, the lack of a precise compensation mechanism for affected data principals poses challenges to the enforcement of individual privacy rights.

In alignment with India's digital development vision, articulated in Viksit Bharat@2047, the DPDP Act aims to foster trust in digital systems, thereby promoting sustainable economic growth and civic engagement. Nonetheless, issues surrounding independence, proportionality, and available remedies indicate that further legal reforms may be necessary.

6. Sustainable digital governance and DPDP act

Sustainable digital governance involves the responsible and ethical deployment of digital technologies to uphold democratic values and support inclusive economic development, as articulated in India's Viksit Bharat@2047 initiative. Central to this governance model is the Digital Personal Data Protection Act, 2023 (DPDP Act), which institutionalizes privacy, trust, and data protection within India's evolving digital landscape.

The DPDP Act establishes that public trust is foundational to sustainable digital governance, mandating that both state and private entities handle personal data transparently and securely. This is achieved through a consent-based data processing framework, stringent data fiduciary standards, and explicit personal data rights (Bennett & Raab, 2020) [1]. The Act transitions digital governance from arbitrary methods to a robust legal framework, anchoring it in constitutional principles that require governance to respect individual rights and promote autonomy.

The legislation also addresses accountability within India's Digital Public Infrastructure (DPI), where massive government systems such as Aadhaar have raised concerns about profiling and exclusion. The establishment of the Data Protection Board of India under the Act is intended to enhance enforcement. However, its independence from executive power raises questions about long-term accountability and effectiveness (Bhandari, 2018) [2].

Equity and inclusion are critical components of sustainable digital governance. The DPDP Act seeks to protect marginalized communities, acknowledging the heightened risks they face from surveillance and data misuse. Nonetheless, the Act's reliance on individual consent presupposes a level of digital literacy and awareness that may be lacking among significant portions of India's population. Consequently, there is an urgent need for educational initiatives and accessible grievance mechanisms to empower citizen participation in the digital economy.

In fostering innovation and economic growth, the DPDP Act allows specific data uses without consent and enables cross-border data transfers, thereby bolstering India's digital marketplace. However, this flexibility requires caution; expansive state exemptions could compromise constitutional rights, underscoring the need for careful regulation that balances innovation with compliance with established legal standards.

Additionally, the ethical implications of sustainable digital governance must include considerations for data minimization, systemic risk reduction, and responsible data management in the face of rapid technological advancement. Although the Act does not prescribe specific environmental or algorithmic accountability standards, its emphasis on data security and purpose limitation encourages responsible handling of information.

Ultimately, the Viksit Bharat@2047 vision calls for a benign, technologically advanced society where digital transformation reinforces democratic integrity and public confidence. For the DPDP Act to fulfill its potential as an effective governance mechanism, it necessitates ongoing evaluations and revisions to enhance institutional independence, curtail exemptions, and integrate mechanisms that uphold citizens' rights, thereby

aligning data protection laws with India's overarching developmental goals.

7. Findings/Results

The paper draws the following conclusions from doctrinal and analytical analysis of constitutional law, DPDP Act provisions, and comparative global frameworks. These findings show how the DPDP Act supports sustainable digital governance and equitable development in Viksit Bharat@2047.

7.1. Privacy rights and constitutionality

The Supreme Court's recognition of the right to privacy in Justice K.S. Puttaswamy v. Union of India (2017) [6] informs the DPDP Act, establishing privacy as a fundamental right under Article 21. However, the conversion of constitutional rights into statutory provisions remains incomplete, particularly with respect to proportionality and legal remedies.

7.2. Complete data protection framework

The DPDP Act is noted as India's first comprehensive data protection law, replacing the inadequate Information Technology Act, 2000. It formalizes definitions and obligations, enhancing predictability and sustainability in digital governance.

7.3. Digital governance accountability improvement

The Act mandates data fiduciaries to ensure data security and provides mechanisms for breach reporting and grievance redressal. This strengthens accountability and builds trust in the digital infrastructure necessary for sustainable governance.

7.4. Institutional oversight and independence limitations

The Data Protection Board of India's lack of independence raises concerns about regulatory neutrality, particularly as the executive influences it. Independent enforcement is crucial for adequate privacy protection.

7.5. Broad state exemptions and proportionality

The DPDP Act allows state exemptions for national security and public order, which are constitutionally acceptable but might dilute privacy protections and regulatory oversight if not limited rigorously under the Puttaswamy proportionality doctrine.

7.6. Few personal remedies and rights enforcement

The Act emphasizes penalties over individual remedies, lacking provisions for compensation for data principals. This contrasts with the rights-based approach of regulations like GDPR, potentially sidelining marginalized groups.

7.7. Digital economy and innovation facilitation

By liberalizing cross-border data flows and defining the lawful use of personal information, the DPDP Act encourages economic growth and integration into the global digital economy, aiding the realization of Viksit Bharat@2047 goals.

7.8. Digital awareness and inclusion challenges

Implementation of the DPDP Act hinges on digital literacy and institutional competency. The complexity of India's socio-economic landscape may hinder informed consent, limiting the Act's potential for inclusivity without proactive awareness initiatives.

7.9. Law and policy must evolve

The Act establishes a legal foundation for data protection but necessitates continuous evaluation to adapt to challenges posed by emerging technologies like AI and big data analytics, ensuring long-term relevance and effectiveness of governance frameworks.

8. Discussion

The document provides a comprehensive analysis of the Digital Personal Data Protection (DPDP) Act, highlighting its implications for digital governance in India within the Viksit Bharat@2047 vision. Key findings include:

8.1. Privacy rights and constitutionality

The Supreme Court's recognition of the right to privacy in Justice K.S. Puttaswamy v. Union of India (2017) [6] informs the DPDP Act, establishing privacy as a fundamental right under Article 21. However, the conversion of constitutional rights into statutory provisions remains incomplete, particularly with respect to proportionality and legal remedies.

8.2. Complete data protection framework

The DPDP Act is noted as India's first comprehensive data protection law, replacing the inadequate Information Technology Act, 2000. It formalizes definitions and obligations, enhancing predictability and sustainability in digital governance.

8.3. Digital governance accountability improvement

The Act mandates data fiduciaries to ensure data security and provides mechanisms for breach reporting and grievance redressal. This strengthens accountability and builds trust in the digital infrastructure necessary for sustainable governance.

8.4. Institutional oversight and independence limitations

The Data Protection Board of India's lack of independence raises concerns about regulatory neutrality, particularly as the executive influences it. Independent enforcement is crucial for adequate privacy protection.

8.5. Broad state exemptions and proportionality

The DPDP Act allows state exemptions for national security and public order, which are constitutionally acceptable but might dilute privacy protections and regulatory oversight if not limited rigorously under the Puttaswamy proportionality doctrine.

8.6. Few personal remedies and rights enforcement

The Act emphasizes penalties over individual remedies, lacking provisions for compensation for data principals. This

contrasts with the rights-based approach of regulations like GDPR, potentially sidelining marginalized groups.

8.7. Digital economy and innovation facilitation

By liberalizing cross-border data flows and defining the lawful use of personal information, the DPDP Act encourages economic growth and integration into the global digital economy, aiding the realization of Viksit Bharat@2047 goals.

8.8. Digital awareness and inclusion challenges

Implementation of the DPDP Act hinges on digital literacy and institutional competency. The complexity of India's socio-economic landscape may hinder informed consent, limiting the Act's potential for inclusivity without proactive awareness initiatives.

8.9. Law and policy must evolve

The Act establishes a legal foundation for data protection but necessitates continuous evaluation to adapt to challenges posed by emerging technologies like AI and big data analytics, ensuring long-term relevance and effectiveness of governance frameworks.

9. Conclusion

India's ambition to become a sophisticated and resilient society by 2047 is underpinned by the Digital Personal Data Protection Act (DPDP Act), 2023. This legislation aims to establish a comprehensive framework for digital personal data processing, emphasizing consent and fiduciary responsibilities, and aligns with global regulatory trends. Despite its advancements, the Act faces challenges, including broad State exclusions, limited institutional independence of the Data Protection Board, and inadequate individual remedies, which hinder the protection of constitutional privacy rights.

The DPDP Act's pragmatic regulatory approach supports innovation and economic competitiveness through data and cross-border transfer flexibility. However, effective governance requires transparency and robust oversight. Success in digital governance also hinges on inclusivity, necessitating enhanced digital literacy and grievance mechanisms to ensure equitable data protection across socioeconomic divides.

Ultimately, while the DPDP Act marks a significant step in India's data protection journey, its long-term effectiveness will depend on ongoing legal refinement, a rights-centric approach to implementation, and robust institutional frameworks, making data protection essential to India's democratic future in the digital age.

References

1. Bennett CJ, Raab CD. *The governance of privacy: policy instruments in global perspective*. 2nd ed. Cambridge (MA): MIT Press, 2020.
2. Bhandari S. The Supreme Court of India and the right to privacy: a landmark judgment. *Indian Law Rev*. 2018;2(2):149-65. doi:10.1080/24730580.2018.1514647.
3. Chander A, Le UP. Data nationalism. Emory Law J. 2015;64(3):677-739.
4. Government of India. *Information Technology Act, 2000*. New Delhi: Ministry of Law and Justice, 2000.
5. Government of India. *Digital Personal Data Protection Act, 2023*. New Delhi: Ministry of Law and Justice, 2023.
6. *Justice K.S. Puttaswamy (Retd.) v. Union of India*. (2017) 10 SCC 1 (Supreme Court of India).
7. *Kharak Singh v. State of Uttar Pradesh*. AIR 1963 SC 1295.
8. Kuner C, Bygrave LA, Docksey C, editors. *The EU General Data Protection Regulation (GDPR): a commentary*. Oxford: Oxford University Press, 2020.
9. *M.P. Sharma v. Satish Chandra*. AIR 1954 SC 300.
10. NITI Aayog. *India's digital transformation: building a resilient digital public infrastructure*. New Delhi: Government of India, 2021.
11. *R. Rajagopal v. State of Tamil Nadu*. (1994) 6 SCC 632.
12. European Parliament, Council of the European Union. 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). Off J Eur Union. 2016;L119:1-88.