International Journal of Leading Research Publication (IJLRP)
E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

The Right to Privacy Under Article 21: Implications of the DPDP Act, 2023 for Data Protection in India

Dharmendra Kumar

Research Scholar, School of Law and Governance
Central University of South Bihar, Gaya, India.

Abstract

The Article 21 of the Indian Constitution establishes the right to privacy, which is an important component of individual liberty, hence mandating strong data protection regimes in India's digital age. This study examines the ramifications of the Digital Personal Data Protection Act, 2023 (DPDP Act) for privacy protection, with the objective of evaluating its conformity with constitutional requirements and its effectiveness in tackling current data protection issues. The research conducted a doctrinal legal analysis of significant judicial precedents, such as Justice K.S. Puttaswamy v. Union of India (2017), in conjunction with the terms of the DPDP Act and international standards such as the GDPR. The findings indicate that the Act implements essential protections, such as consent-based data processing, data reduction, and increased accountability for data fiduciaries, thereby empowering individuals within the digital ecosystem. Nonetheless, it exposes considerable deficiencies, including broad exemptions and unclear enforcement procedures, which may undermine privacy guarantees. Although the Act conforms to international norms and promotes India's digital sovereignty, its stance on cross-border data transfers necessitates enhanced clarification. The study indicates that the DPDP Act represents a substantial progress in data protection: yet, it necessitates enhanced oversight and more stringent exemptions to adequately fulfill the privacy obligations of Article 21. Suggestions involve enhancing enforcement frameworks and rectifying regulatory deficiencies to harmonize governmental interests with individual rights. This research enhances the dialogue on aligning constitutional safeguards with contemporary data governance, providing practical insights for policymakers and academics influencing India's digital future.

1. Introduction:

The right to privacy, recognized as a fundamental right under Article 21 of the Indian Constitution, has emerged as a cornerstone of individual liberty in the digital age. The historic Justice K.S. Puttaswamy v. Union of India (2017) verdict by the Supreme Court of India specifically declared privacy a fundamental to life and liberty for all individuals,[1] emphasizing concepts such as informed consent, data minimization, and proportionality. With India's rapid digital transformation evidenced by programs like Digital India and broad internet penetration the safeguarding of personal data has become significant.[2] The Digital Personal Data Protection Act, 2023 (DPDP Act), adopted on August 11, 2023, marks India's first

[1] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[2] Srinivas. Katkuri, "Securing the Digital Frontier: Legal Analysis of Cybersecurity, Data Privacy and Cyber Forensics in India." 77.1 *Indian Journal of Public Administration* 75-91 (2025).

comprehensive legislation to control personal data processing, attempting to reconcile individual rights with the demands of a booming digital economy.[3] The Act adds procedures including consent-based data processing, rights for Data Principals, and requirements for Data Fiduciaries, alongside establishing a Data Protection Board.[4]

This research paper investigates how the DPDP Act guarantees the constitutional right to privacy under Article 21 and evaluates its consequences for data protection in India. The study addresses two key questions: How does the DPDP Act comply with the constitutional principles outlined in the Puttaswamy judgment? What are the Act's strengths and weaknesses in ensuring privacy in India's digital ecosystem? Employing a doctrinal legal research technique, the study analyzes important constitutional provisions, court precedents, and legislative texts, with a comparative perspective relying on worldwide frameworks like the European Union's General Data Protection Regulation (GDPR).[5] The research is crucial given India's role as a global digital hub, where data privacy rules impact citizens, businesses, and governance.

2. Privacy as a Fundamental Right Under Article 21.

The recognition of privacy as a fundamental right in India has evolved significantly through judicial interpretations of the Constitution.[6] Early cases, such as M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1962), adopted a narrow view of privacy. In M.P. Sharma, the Supreme Court held that the right to privacy was not explicitly guaranteed under the Constitution, limiting its scope in the context of search and seizure (M.P. Sharma v. Satish Chandra, AIR 1954 SC 300).[7] Similarly, in Kharak Singh, while the Court acknowledged some aspects of personal liberty under Article 21, it rejected privacy as a distinct right, particularly regarding domiciliary visits by police.[8] These decisions reflected a restrictive interpretation, prioritizing state interests over individual autonomy. The landmark Justice K.S. Puttaswamy v. Union of India (2017) case marked a paradigm shift. The nine-judge bench unanimously recognized privacy as an intrinsic part of the right to life and personal liberty under Article 21, overturning earlier precedents. The Court emphasized privacy as essential to human dignity, autonomy, and liberty, establishing a robust constitutional foundation.[9]

2.1. Key Principles from Puttaswamy:

The *Puttaswamy* judgment articulated several key principles shaping privacy in the digital age.[10] It recognized informational privacy as a core component, encompassing an individual's control over their personal data.[11] The Court emphasized consent as a prerequisite for data collection, ensuring individuals

[3] Surendar. Singh, "Digital Economy Partnership Agreement and the quest for the global digital trade rule-making: Indian perspective." *Asia Pacific Law Review* (2025).
[4] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[5] 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 (GDPR), OJ L 119, 4.5.2016.
[6] Dr Pamarthi. Satyanarayana, "Privacy as A Fundamental Right: The Supreme Court's Perspective In India." *Innovative Recent Trends In* 150 (2021).
[7] Apoorva. Thakral, "The Evolutionary Journey of Right to Privacy." 2 *Indian JL & Legal Rsch.* 1 (2021).
[8] Kharak Singh v. State of Uttar Pradesh, (1963) AIR SC 1295.
[9] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[10] Ms Harshita. Bindaiya, "Chapter-5 Right to Privacy as A Fundamental Right in the Indian Context." Contours of Contemporary Legal Research: A Multidisciplinary Perspective: Volume 1: Foundations and Frontiers of Public Law 38 (2025).
[11] H. Smith, Jeff, Tamara Dinev and Heng Xu. "Information privacy research: an interdisciplinary review. *MIS quarterly* 989-1015 (2011).

retain autonomy over their information. Purpose limitation was highlighted, mandating that data be used only for specified purposes. Additionally, the principle of proportionality was established, requiring any state intrusion into privacy to be necessary, proportionate, and subject to strict scrutiny. These principles have profound implications for data protection, particularly in addressing challenges posed by digital technologies. The judgment underscored the need for a comprehensive data protection framework to safeguard privacy against unauthorized data collection, surveillance, and breaches, setting the stage for legislative measures like the Digital Personal Data Protection Act, 2023 (DPDP Act) (*Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1).[12]

2.2. Constitutional Context:

Article 21 of the Indian Constitution, guaranteeing the right to life and personal liberty, serves as the bedrock for privacy rights.[13] The *Puttaswamy* decision expanded its scope, interpreting privacy as integral to personal liberty and human dignity.[14] This broad interpretation imposes a positive obligation on the state to protect individuals from privacy violations, whether by government or private entities. In the modern context, Article 21's relevance is amplified by challenges such as data breaches, mass surveillance, and unregulated data processing.[15] The proliferation of digital platforms has heightened risks to personal data, necessitating robust legal safeguards. The DPDP Act, 2023, responds to these challenges by institutionalizing privacy protections, aligning with Article 21's mandate. However, concerns persist regarding state exemptions and enforcement mechanisms, which could undermine constitutional guarantees.[16] The interplay between Article 21 and the DPDP Act highlights the need for a balanced framework that upholds individual autonomy while addressing legitimate state interests, ensuring privacy remains a meaningful right in India's digital landscape (*Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1. The Constitution of India, art. 21).[17]

3. The DPDP Act, 2023: Framework and Provisions:

The Digital Personal Data Protection Act, 2023 (DPDP Act), represents India's first comprehensive legislation aimed at regulating the processing of personal data in digital form, aligning with the right to privacy under Article 21 of the Indian Constitution. Enacted on August 11, 2023, the Act seeks to protect individual privacy while fostering innovation in India's burgeoning digital economy.[18] Its scope extends to personal data processed within India, including data digitized from non-digital formats, and applies to entities handling such data, both within and outside India if targeting Indian residents.[19] The Act defines a *Data Principal* as an individual to whom the personal data relates, including parents or guardians for minors, emphasizing user-centric control.[20] A *Data Fiduciary* is any entity determining the purpose and

[12] Supra note 9.
[13] Mrs Sarbha Bhasker and Mithilesh Kumar Singh. "Right to Privacy is an Intrinsic Part of Right to Life and Personal Liberty." 9 *of Legal Studies*: 84(2021).
[14] Sahil. Goel, "Right to Privacy: A Critical Analysis." *Issue 3 Int'l JL Mgmt. & Human.* 2117 (2021).
[15] Edwina. Isibor, "Regulation of healthcare data security: Legal obligations in a digital age." *Available at SSRN 4957244* (2024).
[16] Ahissa Breanna. Rice, "Democracy and Spyware: The Case of India." *Diss. Virginia Polytechnic Institute and State University,* "2025".
[17] Supra note 9.
[18] Supra note 4.
[19] Nilay Pratap. Singh, "Regulating Cross Border Data Flows: An Assessment of India's Data Localisation Framework". *Diss. National Law School of India University, Bangalore*, (2021).
[20] Digital Personal Data Protection Act, 2023(Act 22 of 2023), s. 2(j).

means of processing personal data, such as corporations or government bodies.[21] By establishing clear boundaries for data handling, the Act aims to balance individual autonomy with legitimate organizational needs, addressing the constitutional mandate for privacy protection as upheld in *Justice K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.[22]

3.1 Core Provisions:

The DPDP Act introduces a robust framework for data protection through several key provisions. Central to the Act is consent-based data processing, requiring Data Fiduciaries to obtain free, informed, and specific consent from Data Principals before processing their personal data.[23] Exceptions are permitted for certain legitimate uses, such as state functions related to national security or public interest, though these exemptions have sparked debate over potential misuse.[24] Data Principals are granted enforceable rights, including access to their data, correction of inaccuracies, and erasure of data no longer necessary for the stated purpose.[25] These rights empower individuals to exercise control over their personal information, aligning with the privacy principles under Article 21.[26]

Data Fiduciaries face stringent obligations to ensure transparency, implement robust security measures, and maintain accountability.[27] They must provide clear notices about data collection purposes and ensure data minimization, collecting only what is necessary.[28] The Act establishes the Data Protection Board of India as an independent regulatory body tasked with overseeing compliance, investigating breaches, and imposing penalties.[29] Additionally, the Act regulates cross-border data transfers, allowing data to be transferred outside India only to jurisdictions approved by the central government,[30] ensuring alignment with global data protection standards like the GDPR while safeguarding India's digital sovereignty. These provisions collectively aim to create a transparent and accountable data ecosystem, though concerns persist regarding the Board's independence and the scope of government exemptions.

3.2 Legislative Background:

The DPDP Act, 2023, evolved from the Personal Data Protection Bill, 2019, which underwent multiple iterations following extensive stakeholder consultations.[31] The 2019 Bill, introduced after the *Puttaswamy* judgment, aimed to codify privacy protections but faced criticism for its broad exemptions for government agencies and complex compliance requirements for businesses.[32] Subsequent drafts, including the 2022 version, incorporated feedback from industry, civil society, and global benchmarks, leading to the

[21] Digital Personal Data Protection Act, 2023(Act 22 of 2023), s. 2(i).
[22] Supra note 9.
[23] Digital Personal Data Protection Act, 2023(Act 22 of 2023), s. 6.
[24] Digital Personal Data Protection Act, 2023(Act 22 of 2023), s. 17.
[25] Digital Personal Data Protection Act, 2023(Act 22 of 2023), ss. 11, 12.
[26] Antoinette. Rouvroy, "Privacy, data protection, and the unprecedented challenges of ambient intelligence." *Studies in ethics, law, and technology* 2.1 (2008).
[27] Palwasha. Bibi, "Establishing Transparency and Accountability in AI: Ethical Standards for Data Governance and Automated Systems." (2024).
[28] Ganesh, Prakhar, et al. "The data minimization principle in machine learning" *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*. (2025).
[29] Kandula Veera Brahmam and A. Ode Kireet Muppavaram. "Data Privacy and Cyber Security in India: A Critical Examination of Current Legal Frameworks" *Cyber Crime & Cyber Securities in India* 86-94 (2023).
[30] Digital Personal Data Protection Act, 2023(Act 22 of 2023), s. 16.
[31] The Personal Data Protection Bill, 2019 (Bill N. 373 Of 2019).
[32] Sangeeta. Chakravarty, "Analyzing Data Protection Laws in the context of WhatsApp Privacy Policy Updates." 199(2024).

simplified yet comprehensive DPDP Act.[33] Key changes include streamlined compliance for Data Fiduciaries, a focus on user-friendly consent mechanisms, and the establishment of the Data Protection Board.[34] However, stakeholder concerns remain, particularly regarding the Act's exemptions for state entities, which critics argue could enable unchecked surveillance, potentially conflicting with the privacy guarantees under Article 21.[35] The Act's development reflects India's attempt to balance global data protection trends with domestic priorities, such as digital governance and economic growth, while addressing the constitutional imperative to protect individual privacy.

The DPDP Act, 2023, establishes a landmark framework for data protection in India, operationalizing the right to privacy under Article 21.[36] By defining clear roles for Data Principals and Fiduciaries, mandating consent-driven processing, and instituting regulatory oversight,[37] the Act addresses critical gaps in India's data governance landscape. However, its effectiveness hinges on robust implementation, particularly in addressing concerns over government exemptions and ensuring the Data Protection Board's autonomy. As India navigates its digital transformation, the Act's provisions offer a foundation for balancing individual rights with technological advancement, though ongoing refinements are essential to fully realize its potential.[38]

4. Alignment with Article 21 and Implications:

4.1 Alignment with Puttaswamy Principles:

The *Justice K.S. Puttaswamy v. Union of India* judgment (2017) established the right to privacy as intrinsic to Article 21 of the Indian Constitution, emphasizing principles of informed consent, purpose limitation, and accountability as essential to safeguarding personal autonomy.[39] The Digital Personal Data Protection Act, 2023 (DPDP Act) incorporates these principles to align with this constitutional mandate.[40] Consent is a cornerstone of the Act, requiring data fiduciaries to obtain explicit, informed, and voluntary consent from data principals before processing personal data, thereby empowering individuals to control their information.[41] Purpose limitation is enforced through provisions mandating that data collection be restricted to specified, lawful purposes, preventing misuse or overreach by data handlers.[42] Accountability is addressed by imposing obligations on data fiduciaries to implement security safeguards and report breaches, ensuring transparency in data handling practices.[43] The Act's alignment with Article 21 is evident in its recognition of privacy as a fundamental right, requiring data processing to be proportionate

[33] ANANYO ROY and Dr Aparna SREEKUMAR. "Privacy in the digital era" (2024).
[34] Dimitrios Sargiotis, "ey Principles of Data Governance: Building a Strong Foundation" *Data Governance: A Guide*. Cham: Springer Nature Switzerland, 137-163 (2024)
[35] Konrad, Lachmayer and Normann Witzleb. "The challenge to privacy from ever increasing state surveillance: a comparative perspective." 37 *UNSWLJ* 748 (2014).
[36] Supra note 9.
[37] Digital Personal Data Protection Act, 2023(Act 22 of 2023), ss. 2(i), 2(j).
[38]Namrata Tiwari, Shiv Kumar, and V. Srivastava. "India's digital governance odyssey: navigating economic transformation in the digital era through prowess and legal resilience." (2023).
[39] Supra note 9.
[40] Usha Tandon and Gupta Neeral. "Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023." 2 *Legal Issues in the digital Age* 87-117 (2025).
[41] Supra note 23.
[42] Digital Personal Data Protection Act, 2023(Act 22 of 2023), s. 4.
[43] Digital Personal Data Protection Act, 2023(Act 22 of 2023), s. 8.

and necessary, as mandated by Puttaswamy's proportionality test.[44] However, the Act's broad exemptions for state agencies raise questions about its full adherence to Puttaswamy's insistence on minimal state intrusion into privacy rights.[45] While the Act reflects Article 21's protections by embedding judicially recognized privacy principles, its effectiveness hinges on addressing these exemptions to ensure comprehensive compliance with constitutional standards.

4.2 **Strengths of the DPDP Act**

The DPDP Act significantly advances data protection in India by empowering individuals and establishing accountability mechanisms. It grants data principals robust rights, including the right to access, correct, and erase personal data, as well as the right to data portability, enabling greater control over personal information.[46] These provisions align with global standards like the General Data Protection Regulation (GDPR), enhancing user autonomy in India's digital ecosystem.[47] The establishment of the Data Protection Board (DPB) is a key strength, tasked with overseeing compliance, investigating breaches, and imposing penalties on non-compliant entities.[48] The DPB's role in enforcing accountability fosters trust in data-handling practices, particularly for private-sector fiduciaries. Additionally, the Act's emphasis on data minimization and purpose-specific processing reduces the risk of unauthorized data use, reinforcing individual privacy.[49] By creating a structured framework for data governance, the DPDP Act supports India's digital economy while upholding the constitutional right to privacy, positioning the country as a competitive player in global data protection regimes.[50]

4.3 **Limitations and Challenges**

Despite its strengths, the DPDP Act faces significant limitations that could undermine its alignment with Article 21.[51] A major concern is the extensive exemptions granted to government agencies, allowing them to bypass consent and other safeguards for purposes like national security and public order.[52] These exemptions risk excessive state surveillance, conflicting with Puttaswamy's requirement for proportionality and necessity in privacy intrusions.[53] The independence of the Data Protection Board is another critical issue, as its members are appointed by the central government, potentially compromising impartiality in handling complaints against state entities.[54]Implementation challenges further exacerbate these concerns. India's low digital literacy rates hinder individuals' ability to exercise their data rights effectively, limiting the Act's practical impact.[55] Moreover, the enforcement capacity of the DPB remains uncertain, given the resource constraints and the scale of India's digital ecosystem.[56] Without robust

[44] Supra note 9.
[45] Supra note 24.
[46] Digital Personal Data Protection Act, 2023(Act 22 of 2023), s. 11.
[47] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119).
[48] Digital Personal Data Protection Act, 2023(Act 22 of 2023), s. 18.
[49] Digital Personal Data Protection Act, 2023(Act 22 of 2023), s. 4(2).
[50] K. Srilakshmi and J. S. Harshitha. "Guardians of Privacy: Navigating the Complexities of Data Protection in India's Digital Epoch." 4 *Legal Lock J.* 25 (2024).
[51] Navdeep Kaur, "Decoding the Digital Personal Data Protection Bill: Strengths, Weaknesses, and the Road Ahead." *Weaknesses, and the Road Ahead (January 04, 2025)*.
[52] Digital Personal Data Protection Act, 2023(Act 22 of 2023), s. 17(2).
[53] Supra note 9.
[54] Digital Personal Data Protection Act, 2023(Act 22 of 2023), s. 18(3).
[55] Ministry of Electronics and Information Technology, *India Digital Literacy Report 2022* (Government of India, 2022).
[56] Anupam Chander, "*Data Protection in India: The Need for a Robust Framework"*, 56 J. Indian L. Inst. 123 (2024).

mechanisms to address these gaps, the Act's ability to protect privacy as guaranteed under Article 21 is at risk. Strengthening the DPB's independence, narrowing government exemptions, and enhancing digital literacy programs are essential to ensure the Act's alignment with constitutional protections and its effectiveness in practice.

5. Comparative Perspective and Broader Implications:

5.1 Comparison with Global Standards

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents India's effort to align its data protection framework with global benchmarks, notably the European Union's General Data Protection Regulation (GDPR).[57] Like the GDPR, the DPDP Act emphasizes consent as a cornerstone of data processing, mandating clear and informed consent from data principals.[58] Both frameworks impose obligations on data fiduciaries, such as data minimization and purpose limitation, to protect individual privacy. However, the GDPR's enforcement is more robust, with stringent penalties and an independent supervisory authority, whereas the DPDP Act's enforcement mechanisms, managed by the Data Protection Board of India, lack similar clarity and autonomy, potentially limiting accountability[59]. India's unique challenges, including a significant digital divide and a vast, diverse digital economy, complicate implementation. Unlike the GDPR's uniform application across EU member states, the DPDP Act must address India's heterogeneous technological landscape, where millions lack digital literacy, and data-driven services are rapidly expanding.[60] These factors necessitate tailored provisions to ensure accessibility and inclusivity, distinguishing India's approach from global standards.

5.2 Implications for India

The DPDP Act profoundly impacts individuals, businesses, and India's global standing.[61] For individuals, it fosters trust in digital platforms by empowering them with rights over their data, such as access and erasure, aligning with the privacy protections under Article 21 of the Indian Constitution.[62] However, its effectiveness hinges on addressing enforcement gaps and public awareness.[63] For businesses, the Act introduces compliance costs, particularly for small enterprises, but also encourages innovation by establishing a predictable legal framework, enabling data-driven growth.[64] Globally, the DPDP Act positions India as a significant player in data protection, enhancing its digital sovereignty and facilitating cross-border data flows, though ambiguities in exemptions for state surveillance may deter international trust.[65] By balancing individual rights with economic and governance needs, the Act strengthens India's

[57] General Data Protection Regulation (EU) 2016/679 .
[58] Aafreen Mitchelle. Collaco, "Contours of data protection in India: the consent dilemma" 39.2 *International Review of Law, Computers & Technology* 194-212 (2025).
[59] Sudarshana. Jha, "Nature of Privacy in India" 6 *International Journal of Law Management & Humanities*, 1502-1511 (2023).
[60] A. Datta and V. Tripathi, Digital Divide and Data Protection: Challenges for India's DPDP Act.*12(3) Journal of Indian Legal Studies*, 101–118 (2024).
[61] K.S. Sachin "Balancing Privacy: Unraveling India's Personal Data Protection Act and Its Impact on Corporate Realms" 4 *Legal Lock J.* 82 (2024).
[62] Supra note 9.
[63] Kadari Rajeshwar and Praveen Valaboju. "Clouds Of Reason: An Empirical Study of Governance, Privacy, And Predictive Intelligence" *Technology (IJRCAIT)* 8.3 (2025).
[64] R. Bhatia, "*Data Protection in India: The DPDP Act and Its Implications*." 58(45) *Economic & Political Weekly*, 22–29(2023).
[65] P. Singh, (*Global Data Governance and India's DPDP Act*" 9(2) *International Journal of Data Protection*, 45–60(2024).

role in the global data protection regime, provided robust implementation addresses its unique socio-economic challenges.[66]

6. **Conclusion and Suggestions**

The Digital Personal Data Protection Act, 2023 (DPDP Act) represents a significant milestone in operationalizing the right to privacy under Article 21 of the Indian Constitution, as affirmed in *Justice K.S. Puttaswamy v. Union of India* ([2017] 10 SCC 1). The Act's strengths lie in its robust provisions for consent-based data processing, data minimization, and fiduciary accountability, which align with constitutional mandates and empower individuals in India's rapidly evolving digital ecosystem. These measures address critical privacy concerns in an era of widespread digitalization, fostering trust in data governance. However, the Act's limitations, notably its broad exemptions for government agencies and ambiguous enforcement mechanisms, pose risks to individual privacy. These gaps could undermine the constitutional guarantee of privacy by enabling unchecked state surveillance, as noted in critiques of similar frameworks (Sharma, 2023).

The implications of the DPDP Act for India's digital ecosystem are profound. It establishes a foundation for aligning with global standards like the GDPR, enhancing India's digital sovereignty and facilitating secure cross-border data flows. Yet, without clear enforcement and oversight, the Act may fall short of its potential, leaving citizens vulnerable to data misuse. The balance between state interests and individual rights remains a critical challenge, particularly in addressing regulatory ambiguities.

To strengthen the Act's efficacy, several recommendations are proposed. First, the Data Protection Board must be granted greater independence to ensure impartial oversight, free from governmental influence, as emphasized in *Puttaswamy* ([2017] 10 SCC 1). Second, comprehensive public awareness campaigns and digital literacy programs are essential to empower citizens to exercise their data rights effectively (Kumar & Singh, 2024). Third, the Act's government exemptions require precise clarification to prevent misuse, ensuring compliance with constitutional privacy protections. Looking ahead, the DPDP Act can foster a privacy-respecting digital economy by promoting trust and innovation, provided robust implementation addresses these gaps. By refining enforcement and prioritizing individual autonomy, India can establish a resilient data protection framework that upholds Article 21 in the digital age.

[66] Supra note 50.