



## Digital Privacy, Cyber Law, and Transformation of the Indian Judicial System: Critical Analysis of the DPDP Act, 2023, and Information Technology Act, 2000

Md Jiyauddin<sup>1,\*</sup>, Sunita Banerjee<sup>2</sup>

<sup>1</sup> School of Law, Brainware University, Kolkata, West Bengal, India

<sup>2</sup> School of Law, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, India

\* Corresponding author: [imdjiyauddin@gmail.com](mailto:imdjiyauddin@gmail.com)

### ARTICLE INFO

#### Article history:

Received: 29-09-2026

Received in revised form: 08-10-2026

Accepted: 08-10-2026

Available online: 10-10-2026

#### Keywords:

Cyber Law

Digital Governance

Digital Privacy

DPDP Act, 2023

Information Technology Act, 2000

Justice System

### ABSTRACT

The advent of technological advancement and using cloud computing, artificial intelligence, and digital technology to create a digital revolution, and data governance have completely altered the legal and institutional setting in India and thus, digital privacy has become one of the core issues in cyber law and policy in the country. The Supreme Court of India's recognition of the fundamental right to privacy in the Justice K.S. Puttaswamy v. Union of India (2017) case established the constitutional foundation for the protection of personal data and required legislative changes to address the emerging digital threats. In this regard, in addition to the cyber laws under the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023 (DPDP Act) is the first law in India that governs the handling of personal digital data. However, the co-existence of both the acts has resulted in some crucial issues. Although the DPDP Act 2023 signals a paradigm shift towards a rights-based approach to data governance, there continue to be inadequacies in aligning privacy protection with cybersecurity regulation through the Information Technology Act, 2000. In its findings, the paper establishes that a privacy-oriented digital justice ecosystem in India can only be achieved through stronger enforcement mechanisms, judicial capacity-building for digital disputes, good governance, and law reform for technology.

## 1. INTRODUCTION

A modern digital technology has become central to governance and development in India. Initiatives such as Digital India, Aadhaar-based services, Unified Payments Interface (UPI), DigiLocker, online learning systems, tele-medicine and e-Courts Mission have led to an acceleration in digitization and transformation of public services delivery [1]. On the other hand, private digital platforms have started collecting huge amounts of personal data related to financial activities, health, biometric identification, communication patterns and online behavior. This way, personal data has become not only economic value but a legal issue and requires the establishment of regulatory mechanisms which would protect the rights of individuals while facilitating technological innovations [2].

The growth in digital ecosystems has increased the exposure of people to identity thefts, financial scams, illegal surveillance, data breaches, cyber harassment and algorithmic profiling among other threats [3]. Current legal instruments developed mainly for protection of electronic commerce have shown their inadequacy to cope with new challenges. The Supreme Court of India's ruling in *K.S. Puttaswamy (Retd.) v. Union of India* fundamentally altered India's legal perspective on informational privacy and served as the impetus for the country's legislative reform of personal data regulations [4]. India's first legislative framework for digital personal data was enacted in 2023 with the Digital Personal Data Protection Act. By introducing a framework based on consent, individual statutory rights, and regulatory enforcement

mechanisms, it improves the current cyber law structure rather than attempting to replace the Information Technology Act, 2000. This research will investigate how the development of the above-mentioned areas has impacted the cyber law regime in India and whether it provides sufficient protection to privacy amidst digital governance [5].

## 2. CONSTITUTIONAL FOUNDATION OF DIGITAL PRIVACY

The constitutional history of digital privacy in India attained its most crucial phase through *Justice K.S. Puttaswamy v. Union of India* (2017) was a historic ruling [4]. Prior to this ruling, privacy was protected via fragmentary judicial interpretations of the provisions of Articles 19 and 21. However, privacy had never been considered to be an independent fundamental right. A component of the basic right to life and personal liberty protected by Article 21, privacy is associated with human freedom and dignity [6].

Three constitutional principles which were developed in this ruling play a crucial part in the current regulation of digital governance. These principles include the following: there should be a legal basis for the infringement on privacy as stipulated by legislation; any restriction on the exercise of the right should serve the achievement of a legitimate government interest; any restriction should meet the requirement of proportionality meaning that it is not excessively restrictive to achieve the goal pursued by the government. Notably, In the digital era, the Court recognized informational privacy as a crucial component of constitutional rights. There is an increased tendency among individuals to share personal information via digital means without knowing the possible exploitation of such information. In this way, the Court laid down the fact that constitutional rights must adapt to technology. As such, the ruling served as the intellectual and constitutional foundation on which India's data protection regime was developed [7].

## 3. DEVELOPMENT OF CYBER LAW IN INDIA

### 3.1 The Act of 2000 on Information Technology

India's first effort at comprehensive cyber rules was the Information Technology Act, 2000 [8]. It was formulated mainly to promote electronic transactions and to provide legal recognition to the electronic record and digital signature. Thus, this Act allowed development of digital economy in India. The Amendment to the Information Technology Act, 2008 significantly broadened its scope by incorporating such Identity theft, phishing, cyberterrorism, and privacy invasion are examples of cybercrimes and liability of intermediaries [9]. The Act also contained significant obligations in the sphere of cybersecurity. For instance, section 43A provided civil liability to body corporates that failed to ensure reasonable security of sensitive personal data or information. Sections 69 and 69A allowed interception of communication and blocking of internet content by government agencies in accordance with statutory provisions [2].

### 3.2 Limitations of the IT Act

The IT Act is important from a historical point of view, it is designed to deal with technology from the early years of the new millennium and not the present-day digital economy. The IT Act came at a time when there were no smartphones, cloud computing, artificial intelligence, blockchain technology, and platforms that operated on a large scale [10]. Most importantly, the IT Act was not meant to act as a full-fledged personal data protection law in the first place.

## 4. THE PROTECTION OF DIGITAL PERSONAL DATA ACT OF 2023

An important development in India's field of digital governance is the Digital Personal Data Protection Act, 2023, as personal data protection is made the centerpiece of legislation [5]. While the IT Act focuses on regulating cyber activities and electronic transactions, the DPDP Act is based on the principles of right-based regulation of processing of digital personal data [11]. The Digital Personal Data Protection Rules' progressive adoption through compliance processes began with its notification [12].

### 4.1 Consent-Based Governance

The DPDP Act follows informed consent as its primary principle of regulation. Generally, processing personal data requires the Data Principal's voluntary, explicit, informed, and unequivocal consent. This increases the power of people through the necessity to notify organizations of the purposes of collecting and processing personal data [13].

## 4.2 Rights of Data Principals

This act provides individuals with statutory rights such as receiving information about processing of data, rectification of erroneous personal data and removal of personal data for certain reasons, grievances redressal, and nomination rights [14].

## 4.3 Data Fiduciary Obligations

When businesses handle personal data, they have to comply with certain obligations. Specifically, the law requires Data Fiduciaries to protect personal data in a proper way, report personal data breaches, use personal data only for legitimate purposes, and exercise accountability over the entire data life-cycle. Another interesting provision of the law is that of Significant Data Fiduciaries, whose obligations are strengthened depending on several criteria [15].

## 4.4 Board of Data Protection

Data Protection Board of India is the new organization, which can be considered a judicial body that adjudicates in cases of non-compliance and levies fines. However, there are some ongoing debates concerning whether it has sufficient regulatory autonomy.

# 5. INTERPLAY OF THE DPDP ACT WITH THE INFORMATION TECHNOLOGY ACT

## 5.1 Complementary Legislation: Privacy and Cyber Security

The Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023 form a complementary legislative framework in India's digital legal system rather than supplanting each other [5, 8]. The Information Technology Act deals mainly with electronic commerce, cyber offences, intermediary liability, and cyber security, whereas a framework for the lawful processing of digital personal data is provided by the DPDP Act. While identity theft, hacking, and cheating by using computer resources are all illegal under the IT Act, the DPDP Act is concerned with consent-based processing of data, individual rights, and organizational responsibilities. These statutes provide a dual layered regulatory system wherein cyber security ensures the safety of digital systems while data protection ensures individual privacy. The complementary nature of these laws demonstrates how India is moving from a technology-centric digital legal framework to a digital right oriented regulatory structure. However, the proper working of this system requires proper coordination among agencies that enforce cyber security and data protection respectively to prevent issues of jurisdiction [12].

## 5.2 Overlapping Regulations and Enforcement Difficulties

Despite their similar purpose, there are some overlapping regulations between the two pieces of legislation which pose difficulties of an enforcement nature. A single cybersecurity incident, including a personal data breach, can result in duties arising from both regulations at the same time. While the responsibility of organizations in terms of maintaining reasonable security practices can be considered in light of the IT Act, the DPDP Act makes it a duty of Data Fiduciaries to establish security measures and report on data breaches to the authority in charge of regulation [5]. Moreover, intermediaries that come under the scope of the IT Act continue to operate under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, while having to follow data protection standards in case of handling personal data. It is clear that the overlap in compliance can be confusing in terms of reporting processes, investigations and regulatory responsibilities [16].

## 5.3 Future Harmonization for Digital Governance

The dynamic relationship between the DPDP Act and the IT Act makes it clear that harmonization is necessary in the future in order to respond to technological change and digital governance issues. The IT Act was made in an era where the issue of electronic commerce was the main issue. However, the current digital environment involves artificial intelligence, cloud computing, biometric recognition and cross border data transfer. Although the DPDP Act updates the Indian privacy law regime, the legislation does not provide for all aspects of AI driven profiling, automated decision making and algorithmic accountability [17]. In the future, such reforms must bring clarity on the relationship between cybersecurity under the IT Act and privacy under the DPDP regime. This will include technology-specific

regulations. Harmonization through institutional coordination between the Data Protection Board of India and other cyberspace law enforcement agencies will increase efficiency of regulation and build trust among the citizens. Such harmonization will lead to a better legal architecture which will protect the constitutional right of privacy while enabling innovation and digital commerce [13].

## 6. EMERGING CHALLENGES IN DIGITAL PRIVACY

### 6.1 Artificial Intelligence

Artificial Intelligence has opened up new dimensions in terms of privacy regulation. AI is now increasingly being used to work on large amounts of data which can produce behavioral analysis, facial recognition, predictive analysis, automated decision-making about employment, healthcare, finances, and law enforcement [15]. Whereas the DPDP framework regulates general personal data processing, there is a lack of regulation of algorithmic transparency, explainability, automated decision-making protections, and AI accountability. Automated decision-making also raises overt and covert challenges to justice that privacy law alone does not resolve [18].

### 6.2 Exemptions for the Government

The DPDP framework allows for exemptions to be made for specific governmental operations in particular statutory situations. Proponents claim that such exemptions aid national security, public order, and good governance. Opponents believe that such discretionary powers by the executive can undermine the privacy rights provided for in Puttaswamy. Future court judgments would clarify whether these exemptions meet the constitutional requirements of legality, necessity, and proportionality.

### 6.3 Cross-Border Data Transfer

Today, most digital businesses involve transfer of personal data beyond borders. In lieu of any localization of data transfer requirement, the DPDP framework allows for international data transfer except to those jurisdictions barred by the Central Government. This flexible model facilitates digital trade while also requiring international cooperation for Indian citizens' personal information.

### 6.4 Integration of Cybersecurity

The increasing number of cyberattacks on banks, hospitals, universities, and governmental bodies illustrates that there is no point in making a distinction between privacy protection and cybersecurity resistance. Encryption, reporting, organizational liability, and regulatory response have become essential parts of privacy governance nowadays [19]. IoT-based smart applications are similarly being designed with security enhancement as a core requirement [20].

## 7. RECENT CASE LAWS ON DIGITAL PRIVACY, CYBER LAW, AND JUSTICE SYSTEM TRANSFORMATION IN INDIA

The case of *Karthick Theodore v. Registrar General*, High Court of Madras (2024) is one of the earliest decisions interpreting the Digital Personal Data Protection Act, 2023 in the judicial context [21]. The High Court ruled that even though the DPDP Act affords increased privacy protection to individuals, before restricting access to court records, courts must perform a proportionality test in order to achieve a balance between privacy and the idea of open justice. The Indian Supreme Court ruled in *Re: Right to Privacy of Adolescents* (2025) reiterated the importance of ensuring greater privacy of children in the digital space in judicial processes, ordering that the technological means used for managing the data of adolescents ensure dignity and confidentiality in the digital court [22]. In *Prashant Kumar Tripathi v. Indian Bank* (2025), the Central Information Commission held that the DPDP Act is to be construed in harmony with the Right to Information Act, 2005, such that the requirement of privacy protection is not presumed to always override the need for transparency in the context of implementation of the new regime [23]. Lastly, the Supreme Court's pending hearing in the case of *Venkatesh Nayak v. Union of India* (2026) represents the latest constitutional challenge to the DPDP Act and its Rules. The petition raises issues relating to the government exemptions, the amendments made to the RTI Act, and the autonomy of the Data Protection Board, under Articles 14, 19, and 21 of the Constitution [24].

## 8. COMPARATIVE PERSPECTIVE AND POLICY RECOMMENDATIONS

The developing framework in India can be seen as having similarities with other privacy policies around the world, especially the GDPR of the EU, with respect to the elements of consent-driven processing, accountability and data subject rights [7]. However, the framework in India intentionally maintains flexibility in regulation in light of its national interests.

Some recommendations for improvement in India's digital privacy law include:

- i. Increased independence of the Data Protection Board through transparent appointments and technical expertise;
- ii. More clear coordination between the IT Act and the DPDP framework to eliminate the ambiguity in regulation;
- iii. India needs to develop its own standard of AI governance, which includes issues related to automation, algorithmic transparency and behavioral profiling;
- iv. Capacity building programs in judicial courts on digital evidence and cybersecurity; and
- v. Nationwide digital literacy programs informing the citizens about consent, privacy rights, and cybersecurity.

## 9. CONCLUSION

There is no doubt that the Indian legislation on cyber laws has transformed from merely regulating e-commerce to providing constitutional-level digital privacy protections. In particular, While the Digital Personal Data Protection Act of 2023 signaled a significant change in India's approach to digital governance, the Information Technology Act of 2000 established the first foundation for cybersecurity and electronic governance, which has been rights-based rather than regulatory. However, for successful implementation of privacy protection laws, additional measures have to be taken. It means that institutional independence, collaboration on enforcement, AI regulation, incorporation of cybersecurity measures, judicial readiness, and constitutionality of control and oversight mechanisms are required to realize the visionary goals set forth by Justice K.S. Puttaswamy. With continuous expansion of India's digital governance initiatives, fintech solutions, smart city initiatives and use of artificial intelligence for public sector projects, it is important to see privacy as a value that supports, rather than hinders, the development.

## REFERENCES

- [1] Nandan Nilekani Committee. (2009). Creating a unique identity number for every resident in India. Government of India.
- [2] Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.
- [3] Srivastava, A. (2021). Cyber laws and IT protection (7th ed.). Taxmann Publications.
- [4] Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. Supreme Court of India. <https://main.sci.gov.in>
- [5] Ministry of Electronics and Information Technology. (2023). Digital Personal Data Protection Act, 2023. Government of India.
- [6] Bennett, C. J. (2018). The governance of privacy: Policy instruments in global perspective (2nd ed.). MIT Press.
- [7] European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [8] Parliament of India. (2000). Information Technology Act, 2000. Government of India. <https://legislative.gov.in/sites/default/files/A2000-21.pdf>
- [9] Richards, N. M. (2015). Intellectual privacy: Rethinking civil liberties in the digital age. Oxford University Press.
- [10] International Association of Privacy Professionals. (2025). Top operational impacts of India's DPDP. <https://iapp.org>
- [11] Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220. <https://www.jstor.org/stable/1321160>
- [12] Ministry of Electronics and Information Technology. (2025). Digital Personal Data Protection Rules, 2025. Government of India.
- [13] Kuner, C. (2020). Transborder data flows and data privacy law. Oxford University Press.

- [14] OECD. (2013). OECD guidelines on the protection of privacy and transborder flows of personal data. Organisation for Economic Co-operation and Development. [https://www.oecd.org/sti/ieconomy/oecd\\_privacy\\_framework.pdf](https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf)
- [15] Richards, N. M., & King, J. H. (2014). Big data ethics. *Wake Forest Law Review*, 49(2), 393–432.
- [16] Lakra, R., Kolanu, P., & Shrivastava, A. (2025). Data, control, and power: Decoding India's Digital Personal Data Protection Act, 2023. *Global Privacy Law Review*.
- [17] Parliament of India. (2008). Information Technology (Amendment) Act, 2008. Government of India. <https://legislative.gov.in/sites/default/files/A2009-10.pdf>
- [18] Pandey, J. K., & Kumar, R. (2025). Governing the algorithmic agent: Confronting overt and covert challenges to justice and the future of work. *International Journal of Law Management & Humanities*, 8(4), 1974–1984. <https://doi.org/10.1000/IJLMH.1110648>
- [19] Sundara, K., & Narendran, N. (2023). The Digital Personal Data Protection Act, 2023: Analysing India's dynamic approach to data protection. *Computer Law Review International*, 24(5), 129–141. <https://doi.org/10.9785/crl-2023-240502>
- [20] Pandey, J. K., Jain, R., Dilip, R., Kumbhkar, M., Jaiswal, S., Pandey, B. K., & Gupta, A., et al. (2023). Investigating role of IoT in the development of smart application for security enhancement. In N. Sindhwani, R. Anand, M. Niranjnamurthy, D. C. Verma, & E. B. Valentina (Eds.), *IoT-based smart applications* (pp. 219–243). Springer. [https://doi.org/10.1007/978-3-031-04524-0\\_13](https://doi.org/10.1007/978-3-031-04524-0_13)
- [21] Karthick Theodore v. Registrar General, High Court of Madras (2024).
- [22] In Re: Right to Privacy of Adolescents, Suo Motu Writ Petition (C) No. 3 of 2023 (Supreme Court of India, 2025).
- [23] Prashant Kumar Tripathi v. Indian Bank (Central Information Commission, 2025).
- [24] Venkatesh Nayak v. Union of India, W.P. (C) No. 177 of 2026 (Supreme Court of India).
- [25] Cate, F. H. (2010). The limits of notice and choice. *IEEE Security & Privacy*, 8(2), 59–62. <https://doi.org/10.1109/MSP.2010.63>
- [26] Greenleaf, G. (2022). Global data privacy laws 2022: Despite COVID delays, 157 laws show GDPR dominance. *Privacy Laws & Business International Report*.
- [27] Ministry of Electronics and Information Technology. (2023). Salient features of the Digital Personal Data Protection Bill, 2023. Press Information Bureau.
- [28] Sethi, M. I., Manjunatha, N., Channaveerachari, N. K., Chakraborty, T., Math, S. B., & Andrade, C. (2025). The Digital Personal Data Protection Act 2023: Implications for mental healthcare practice in India. *Indian Journal of Psychiatry*. <https://doi.org/10.1177/02537176251370651>