The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

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

DATA PRIVACY AND DIGITAL PROTECTION IN INDIA: EMERGING LEGAL CHALLENGES IN THE MODERN ERA

Adesh kumar Srivastav

1. INTRODUCTION

Digital revolution has revolutionized the way people communicate, do business and access services to the public. India has seen a tremendous transformation from technological advancements like Digital India, internet banking, e-governance platforms, social media and use of artificial intelligence technologies. Governments, companies and online platforms have come to rely on digital services, leading to massive personal data collection and processing. Digitalization has unquestionably made information more accessible and efficient but has also given rise to serious questions of protection of personal information and the right to privacy.

With this digital age's economy, personal information is a resource. Trials constantly gather data related to an individual's identification, location, monetary deals, browsing history, and passions. Certain information can lead individuals to be vulnerable to identity theft, financial crime, cyberstalking and surveillance when used or disclosed without authorization. The frequent occurrence of data breaches, the misuse of confidential information and rising worries have made people wonder if the data protection laws in India are sufficient.

The most important milestone in this direction was when the Supreme Court in ***Justice K.S. Puttaswamy v.Union of India affirmed the right to privacy as an inherent part of Article 21***[1] of the Constitution. In response to this, the Government came out with ***the Digital Personal Data Protection Act, 2023***[2]to bring about a comprehensive regime about digital personal data and privacy protection.

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

[2] The Digital Personal Data Protection Act, No. 22 of 2023, Gazette of India (Aug. 11, 2023).

Regardless of these legislative changes, there are other issues concerning cybersecurity, government spying, AI, and misuse of private information that remain impactful to India's digital governance framework. This article looks at the existing laws relating to data privacy in India, reviews the provisions of the Digital Personal Data Protection Act, 2023, and addresses the current and potential legal issues in the digital age.

2. EVOLUTION OF DATA PRIVACY LAW IN INDIA

2.1 Constitutional Recognition of Privacy

The right to privacy is not explicitly mentioned as a fundamental right in the Indian constitution. But later, the interpretation of ***Article 21*** [3]which is a Fundamental Right guaranteed by Article 19A to the right to life and personal liberty had been broadened.

In ***Justice K.S. Puttaswamy v Union of India*** [4] the Supreme Court ruled privacy to be a fundamental right protected by Part III of the Constitution of India by a unanimous decision in a nine-judge bench and observed that privacy had three dimensions – informational privacy, bodily autonomy, and decisional freedom. The judgment also reflects the principles of lawfulness, necessity and proportionality which should be satisfied restricting privacy.

The Puttaswamy – data protection judgment was an important constitutional preceding to data protection laws in India. It also emphasized the necessity of an all-encompassing legal landscape which governs collection and processing of personal data in the digital era.

2.2 Information Technology Act, 2000

Prior to the advent of dedicated Data Protection Laws in India, the ***Information Technology Act, 2000***[5], was the main law governing the regime of cyber activities and electronic data. This was settled to legalize electronic transactions and to deal with the problems associated with cybercrime and digital communications.

The ***Information Technology Act, 2000 also, under Section 43A,***[6] imposed liability on body corporate in case of failure to maintain reasonable security practices with respect to sensitive personal data. Biosecurity was also introduced into the wide range of offline regulations under

[3] INDIA CONST. art. 21
[4] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[5] Information Technology Act, No. 21 of 2000, § 43A, India Code.
[6] Information Technology Act, No. 21 of 2000, India Code.

the ***IT Act, 2000, with Section 72A***[7] prescribing punishment for disclosure of information contravening lawful contract.

The Government had made the 'Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011' also known as the ***SPDI Rules, 2011***[8] in 2011 which provided definition of sensitive personal data and made obligations regarding consent, privacy policies and data security measures.

Despite this, existing structure was deemed having narrow scope and lack of enforcement. Given the lack of a specific data protection authority, diminished oversight and inadequate protections were necessary to increase the regulations around digital privacy and the protection of personal data.

The Digital Personal Data Protection Act, 2023 ("DPDP Act") was enacted. The Digital Personal Data Protection Act, 2023 ("DPDP Act") was passed.

2.3 Emergence of the Digital Personal Data Protection Act, 2023

With cases of privacy being considered as a fundamental right, attention was drawn to the need for extensive data protection laws in India. The Government has formed a committee chaired by ***Justice B.N. Srikrishna*** [9]to discuss the data protection issues and come up with appropriate legislation in 2017.

In 2018, the Committee shared their report A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians and a draft Personal Data Protection Bill. The proposed framework brought in certain concepts like Data Fiduciaries, Data Principals, Consent-based Processing, and Data Localisation Requirements etc.

The Digital Personal Data Protection Act, 2023, was enacted by the Government and received Presidential assent on 11.08.2023. It is the first comprehensive personal data law of India dedicated to protection of digital personal data and personal privacy.

The Act aims to strike a balance between the right to privacy and the need for lawful processing of personal data with a primary focus on digital personal data within India or extending to

[7] Information Technology Act, No. 21 of 2000, § 72A, India Code.
[8] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[9] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).

activities outside of India involving the processing of digital personal data of individuals in India.

3. DIGITAL PERSONAL DATA PROTECTION ACT, 2023: AN OVERVIEW

Digital Personal Data Protection Act, 2023 lays down a framework of law for the collection, storage, processing and transfer of digital personal data in the country of India. The act aims to make organisations holding personal data accountable, and to give protection to the privacy rights of individuals.

3.1 Scope and Applicability

The Digital Personal Data Protection Act, 2023 (Within Section 2(t) [10] Digital personal data means data relating to an identifiable person, in digital form. applies to both private and public bodies that process digital personal data.

Data that is processed is owned by Data Principals and the person who decides on the purpose and means of the processing are known as Data Fiduciaries. A central feature of the Act is the focus on consent as the basis for processing as well as on specific and unambiguous consent where individuals may wish for their personal data to be processed.

3.2 Rights of Data Principals

This Act provides that people have certain rights with respect to their personal information. According to Section 11 to 14, Data Principals have the right to access information about how their personal data are processed and can request its rectification or its deletion if it is inaccurate.

In addition the Act allows for cancellation of consent already given for processing of personal data. Moreover, grievance redressal processes have been established to enable any facing grievances due to misuse of personal information or use of the same without rights and privileges have been included.

The purpose of these provisions is to increase the transparency, accountability and individual control of personal data in the digital space.

3.3 Obligations of Data Fiduciaries

[10] The Digital Personal Data Protection Act, No. 22 of 2023, § 2(t), Gazette of India (Aug. 11, 2023).

Data Fiduciaries must also ensure that it applies reasonable security measures to protect personal data from disclosure, including data breaches.

The Act also highly stresses that personal information shall not be stored for any illegal reason and should be destroyed when the purpose of processing is fulfilled. There may be further compliance requirements to which SDFs are subject, such as Designation of Data Protection Officers and regular audits.

These are the measures aimed at enhancing the accountability of institutions and setting high digital governance standards within India.

4. EMERGING LEGAL CHALLENGES IN THE DIGITAL ERA

With the growing penetration of digital technologies in India, there has been rising apprehensions about privacy, cyber security and abuse of personal data. The Digital Personal Data Protection Act, 2023 (DPDP) laid a foundation legal framework for protecting data; however, there are a number of practical and legal hurdles to its implementation.

4.1 Cybersecurity and Data Breaches

Data breaches and cybersecurity are a combined concern. Data breach combined with cyber security concerns.

Cybersecurity threats are a growing worry of the digital world. Sensitive personal information is also commonplace in financial and healthcare institutions, e-commerce sites, databases, and the government, where it's frequently collected and processed, making it vulnerable to hacking, phishing, ransomware attacks, and identity theft.

Information leaks frequently reveal unpublicized information like banking information, passwords, Aadhaar data, medical information, among others. These situations impact on the dignity and privacy of the individual as well as causing financial loss. Although laws and guidelines mandate reasonable security safeguards, many organizations still have ineffective cyber security infrastructure and security compliance protocols.

The lack of detailed technical standards and the inadequacy of enforcement capacity is one of the concerns the DPPDA, 2023 mentions in Section 8 with respect to Data Fiduciaries' obligations to implement reasonable security measures to prevent personal data breaches.

4.2 Government Surveillance and Privacy Concerns

Another big concern in today's India digital ecosystem is government surveillance. The adoption of surveillance technologies like communications interception, Internet surveillance, and facial recognition systems has sparked debate on the rights and liberties civilians enjoy versus the security of the state.

A fundamental right to privacy was recognized by the Supreme Court in Justice K.S. Puttaswamy v. Union of India, but issues persist around usage of excessive surveillance and absence of timely and effective oversight mechanisms.

The process of collection of biometric data through Aadhaar has also raised issues about data security and risks of misuse of data. Rather, the Supreme Court observed that there should be safeguards to prevent misuse of personal data in the name of Aadhaar while affirming the constitutional validity of Aadhaar in the case of K.S. Puttaswamy v. Union of India (Aadhaar Judgment).

Besides, personal data, and information about social welfare, is exempt from processing if it is related to sovereignty, public order and security of the State as per the DPPDA, 2023. This is a right that is necessary but in excess will make the constitutional protection of privacy weaker.

4.3 Artificial Intelligence and Social Media Risks

Any new development in AI and automated technology has raised new legal and ethical worries. AI systems are hugely dependent on large masses of personal information for predictive analysis, facial recognition, targeted marketing, behavioural profiling, and more. Some of these technologies, however, can create algorithmic bias, discrimination and sneaky surveillance.

India does not have a legislation that explicitly specifies regulations in the field of artificial intelligence and automated decision-making systems. While the Digital Personal Data Protection Act, 2023 lays general safeguards on the use of personal data, it is not a comprehensive framework of algorithmic transparency and responsibility of AI.

Social media websites, likewise, accumulate a great deal of info about the energy of the individuals who visit. Personal data and manipulation, misinformation and online exploitation are concerns brought to the forefront by controversies about WhatsApp's privacy policy concerning its commercialization of personal data.

Thinking about cross-border data transfer and enforcement issues

4.4 Cross-Border Data Transfer and Enforcement Issues

Cross-Border Data Transfer has emerged as a key topic on digital governance. Multinational corporations tend to be spread out across different jurisdictions, which poses challenges for identifying the legal accountability and regulatory control.

Yet, ambiguity surrounding foreign laws and data protection principles persist and result in legal hurdles.

Weak enforcement is another big worry. Good institutions, public knowledge and technical skills, are necessary for privacy law implementation. Even if section 18 of the Act introduces the data protection board of India, there are concerns about the independence of the Board and the powers it has for enforcement of privacy laws. But if the regulation is not effective either privacy law will not offer individuals any substantive protections.

5. COMPARATIVE ANALYSIS WITH GLOBAL DATA PROTECTION REGIMES

EU's General Data Protection Regulation (GDPR) is considered one of the strictest privacy laws around the world. It puts great importance on informed consent, transparency, accountability and rich individual rights concerning personal data. The GDPR also has robust sanctions for non-compliance, making for higher standards of enforcement.

The United States has gone for a sector specific approach to data protection instead. California Consumer Privacy Act (CCPA) is an example of privacy laws in specific areas or states, not one overarching law.

The Digital Personal Data Protection Act, 2023 (DPDP Act) strikes a balance between regulation and flexibility, showcasing India's commitment to safeguarding personal data while fostering economic growth and innovation. But still, India may draw lessons from the models in the world, such as further enforcement of the measures, transparency, and better safeguards on AI and automated decision making systems.

6. SUGGESTIONS AND RECOMMENDATIONS

India needs to further enhance the cybersecurity infrastructure and create in-depth compliance protocols for entities that process personal data. Regular audits and mandated reporting of data breaches would enhance accountability and digital security.

There is also a need for more transparency and judicial oversight in relation to the monitoring and interception of communications by the government. Surveillance measures must be within the constitution and subject to proportionality.

Additionally, India should create a specific Artificial Intelligence and technology of facial recognition regulation. Transparent rules, algorithms and ethical AI practices are necessary to safeguard individual privacy.

Educational campaigns and promoting digital literacy should also be encouraged to raise public awareness on digital privacy rights. Lastly, the institution independence and efficiency of Data Protection Board of India should be increased to execute privacy laws adequately.

7. CONCLUSION

Digital technologies have changed the way the Indian economy functions, the way people communicate, and raised concerns about privacy, cyber security, and the use of personal information. The modern concept of data protection in India began with Justice K.S. Puttaswamy's decision in the case of Puttaswamy v. Union of India, which established privacy rights as a fundamental right in the Constitution.

The passage of the Digital Personal Data Protection Act, 2023 is a significant move towards enhancing digital accountability and safeguarding personal data. But issues regarding cybersecurity attacks, government surveillance, AI and cross border data transfers remain to be a hurdle in the working of India's privacy regime.

In India's journey towards becoming a big digital economy, it is essential to strike a balance between innovation and protection of constitutional privacy. To protect digital rights in the modern era, there is a need for strong enforcement, institutional accountability and public awareness.