
DIGITAL PERSONAL DATA PROTECTION IN INDIA: A CRITICAL ANALYSIS OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023 IN AGE OF ARTIFICIAL INTELLIGENCE AND DIGITAL GOVERNANCE

Dr. Surinder Kalyan¹ & Ram Deep Singh²

ABSTRACT

The rapid development of digital economy in India has made personal data one of most important resources. With implementation of digital governance, digital commerce, artificial intelligence, cloud computing, digital health and fintech, amount of personal data being collected, stored and processed by various governmental bodies and businesses has been growing significantly. While mentioned technologies have contributed to innovations and economic prosperity, they have also led to increased risks of attacks, surveillance, identity theft, personal data breaches and misuse. The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's first law that regulates digital personal data and maintains a balance between individual privacy and interests of state and businesses. This paper discusses evolution of right to privacy in India from a constitutional perspective, development of DPDP Act and its main provisions and rights of Data Principals and duties of Data Fiduciaries as established by law. In its conclusion, study maintains that while DPDP Act represents an important milestone in India's digital governance architecture, there is a need for effective implementation, institutional independence and continued legislative reforms in order to overcome technological challenges, especially those posed by developments in artificial intelligence and cross-border data flows.

Keywords: Digital Personal Data Protection Act, Privacy, Data Principal, Data Fiduciary, Artificial Intelligence, GDPR, Digital Governance, Data Protection.

¹ Author is an Associate Professor, School of Legal Studies, NIILM University, Kaithal (Haryana)

² Co-Author is a LL.M. Student, School of Legal Studies, NIILM University, Kaithal (Haryana)

I. Introduction

The explosion in use of technologies has resulted in significant changes in ways governments, organizations and citizens create, use and share information. Personal data has become an invaluable economic resource for innovation, digital business transactions, digital government, health care, education and finance. The fast pace of digitalization of India through Digital India program, digital payments system, e-governance systems, cloud computing, artificial intelligence and greater access to Internet has led to increased collection and processing of personal data.³ Although digitalization has brought many benefits, it has also raised many issues in terms of privacy violation, identity theft, cyber-fraud, unauthorized surveillance, personal information exploitation and even data breach on a large scale. It became evident that increased sophistication of cyber threats requires effective protection of people's personal data with help of legislative measures.⁴

Prior to introduction of Digital Personal Data Protection Act, 2023, legal structure of country in regard to regulation of personal information was fragmentary and incomplete to regulate complexities of modern digital economy.⁵ While Information Technology Act, 2000 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 have mainly placed an obligation on body corporates in respect of sensitive personal data, there was no proper legal regime based on rights governing matter of digital privacy in place.⁶ The lack of statutory provisions with regard to right to consent, right to correction, right to erasure, redressal mechanism and regulatory supervision became all too apparent in face of fast-evolving digital technologies and platforms. It is precisely due to above-stated factors that scholars always emphasized need for comprehensive legislation.⁷

It is thus clear that Digital Personal Data Protection Act, 2023 constitutes a significant achievement with respect to constitutional and technological governance in India.⁸ The statute creates a legal structure which regulates processing of digital personal data through creation of

³ Manindra Singh Hanspal, *The Digital Personal Data Protection Act, 2023: Key Provisions, Issues and Future Directions*, 6 DME J. L. 12 (2025).

⁴ Gauri Goyal, *Privacy and Data Protection in India: A Critical Analysis of Legal Framework* (UPES Research Paper, 2025).

⁵ Manindra Singh Hanspal, *supra* note 1

⁶ Information Technology Act, No. 21 of 2000 (India)

⁷ Hiral Kapadiya & Nilesh Kumar Kapadiya, *User Privacy in Digital Libraries: Challenges, Implications and Strategies for Safeguarding Information*, 1 Indian J. Libr. Sci. Res. & Info. Tech. 37 (2024).

⁸ Digital Personal Data Protection Act, No. 22 of 2023 (India)

specific rights of individuals, duties of persons handling personal data, regulatory body in form of Data Protection Board of India and severe consequences for failure to comply.⁹ At same time, law seeks to achieve a balance between protection of informational privacy under Constitution of India and needs of governance, business innovations and economic development in digital environment. Despite evident similarities with laws of other nations including General Data Protection Regulation of European Union, Act takes an Indian approach to regulation of matter which takes into account local constitutional values and developmental priorities.¹⁰

II. Evolution of Privacy Jurisprudence in India

The gradual evolution of constitutionally protected privacy has been achieved through judicial interpretations rather than an express mention in constitutional document itself. While Indian society in its earlier form recognized notion of individual dignity, confidentiality and autonomy via its social and cultural traditions, early constitutional jurisprudence took a narrower view in recognizing privacy as a fundamental right. *M.P. Sharma v. Satish Chandra*¹¹ and *Kharak Singh v. State of Uttar Pradesh*¹² were cases wherein courts refused to recognize privacy as an independent fundamental right owing to fact that there was no express mention of it in Constitution. But emergence of advanced technologies, electronic surveillance measures, biometric identity schemes, digital governance measures and collection of personal information by government and private institutions have changed dynamics of privacy as a right. It was becoming clear that right to live with dignity and respect under Article 21 was meaningless without a constitutional protection for informational privacy.¹³

The critical change in constitution came with nine-judge bench case of Justice K.S. Puttaswamy (Retd.) v. Union of India¹⁴, where court pronounced with unanimous verdicts that privacy is an inherent part of Right to Life and Personal Liberty protected under Article 21 of constitution. It held that informational privacy, bodily integrity, autonomy and personal dignity form essential parts of constitutional liberty in a democracy. In addition to this, it overruled previous decisions holding that privacy lacks any recognition under constitution and any state

⁹ Manindra Singh Hanspal, *supra* note 1.

¹⁰ Gauri Goyal, *supra* note 2.

¹¹ *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

¹² *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295

¹³ Gauri Goyal, *supra* note 2.

¹⁴ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

intervention on personal information must have legal justification, necessity, proportionality and procedural safeguard. Thus, it was a groundbreaking case in India's constitutional history in that it imposed an obligation on state to provide for laws for regulating gathering, storage, processing and dissemination of personal information. Every contemporary scholarship agrees to say that Puttaswamy judgment provided constitutional ground from which Digital Personal Data Protection Act, 2023 emerged.¹⁵

The constitutional endorsement of right to privacy was also part of wider international trends on data protection laws.¹⁶ International instruments such as Universal Declaration of Human Rights and regulatory mechanisms like General Data Protection Regulation of European Union have had a great impact on development of India's privacy discourse through their emphasis on informed consent, accountability, limited use and exercise of control over one's data. In response to these trends, Government of India undertook an exhaustive legislative process by forming expert committees like Justice B.N. Srikrishna Committee that have had a major bearing on draft of India's personal data protection act.¹⁷ While previous attempts at formulating data protection legislation led to many debates around government exemptions, data localization, independence of regulatory institutions and cross-border transfer of data, all of these discussions were eventually instrumental in bringing into force Digital Personal Data Protection Act, 2023. Thus, DPDP Act is result of constitutional jurisprudence, international experiences and domestic regulation.¹⁸

III. Legislative Evolution of Digital Personal Data Protection Act, 2023

The evolution of a data protection framework in India has not been immediate and straightforward. Prior to DPDP Act¹⁹, data protection laws in India consisted of IT Act, 2000 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. While these statutes have placed certain duties on body corporates with respect to their handling of sensitive personal data, they did not establish a full rights-based framework that could adequately tackle emerging issues of artificial intelligence, cloud computing, e-commerce, healthcare and cross border transfer of data. The landmark case of Justice K.S. Puttaswamy (Retd.) v. Union of India changed constitutional

¹⁵ Manindra Singh Hanspal, *supra* note 1.

¹⁶ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

¹⁷ Gauri Goyal, *supra* note 2.

¹⁸ Manindra Singh Hanspal, *supra* note 1.

¹⁹ Digital Personal Data Protection Act, No. 22 of 2023 (India)

scenario by placing a positive duty on State to formulate data protection legislation. Subsequently, Government set up Justice B.N. Srikrishna Committee to recommend an appropriate legislation in this regard and drafted Personal Data Protection Bill, 2019. However, although this bill was received positively as an essential legislative act, it was criticized for having large government exemptions, compulsory data localization, lack of institutional autonomy and burdensome compliance requirements for businesses. Finally, following these discussions within Parliament, recommendations by committees and consultations with stakeholders, it led to passage of DPDP Act, 2023, which aimed to strike a balance between privacy rights and development needs.²⁰

Another notable feature of legislation process is that there was an effort to reconcile constitutional rules of country with emerging standards of international data protection regulations. The influence of General Data Protection Regulation (GDPR) in European Union on process of drafting was remarkable in terms of highlighting informed consent, purpose limitation, transparency, accountability and data minimization. However, Indian legislature deliberately opted for a flexible approach relevant to conditions of country. As opposed to GDPR that provides for a thorough rights-based regime along with establishment of an independent supervisory authority and heavy responsibility for accountability, DPDP Act introduces a relatively pragmatic regime that takes into account not only privacy of individual but also governmental activities, digital public infrastructure and economic growth as well. The literature suggests that although many provisions are similar to international good practices, Indian legislation differs from European one in providing greater government exemptions and flexible approach to cross-border data flows.²¹

IV. Salient Features of Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 lays out a robust statutory framework for processing of digital personal data in India. The act applies to processing of digital personal data in India and in certain scenarios, will apply to processing carried out outside India if goods or services are offered to persons situated in Indian jurisdiction. There are some fundamental concepts laid down under Act, which together constitute legislative architecture of India's data protection framework. Data Principal is term used for individual whose personal data is being

²⁰ Manindra Singh Hanspal, *supra* note 1.

²¹ Gauri Goyal, *supra* note 2.

processed. Similarly, Data Fiduciary is term used to refer to person/entity determining purpose and manner of processing such personal data. The introduction of these concepts by Act implies establishment of a relationship built on foundation of rights of individuals to corporations carrying out processing of their personal data. This shift in focus of data governance regime from compliance to individual autonomy can be noted from these definitions.²²

The Act pays a lot of attention to lawful processing on basis of informed consent. The consent needs to be free, specific, informed, unqualified and revocable by Data Principal at any point in time. Besides, there are some other legitimate instances in which personal data could be processed without any explicit consent, such as designated governmental functions, legal requirements, employment-related matters and health emergencies.²³ At same time, Act has imposed many obligations on Data Fiduciaries, which include use of security measures to protect personal information, maintaining accuracy of data, reporting of data breaches, transparency of processing operations, redressal of grievances and deletion of personal data on achieving intended purpose.²⁴

The institutional structure put in place through DPDP Act goes even further to enhance regulatory oversight through creation of Data Protection Board of India, which is mandated to conduct investigations, decide on complaints, impose fines and ensure statutory obligations are met. Unlike previous enforcement structures that were fragmented, this board acts as an adjudicator of sorts whose main role is to oversee implementation of DPDP Act. The Act further provides for heavy financial penalties for failure to comply, especially for companies who do not provide sufficient security or who neglect statutory requirements of breach notification and data protection. According to academic literature, setting up of such a regulatory body is one of most important changes made by DPDP Act, notwithstanding concerns that have been raised about issues of institutional independence and government appointment powers. This means that, even as DPDP Act improves India's regulatory system greatly, its success will ultimately depend on performance of Data Protection Board in enforcing statutory requirements.²⁵

²² Digital Personal Data Protection Act, No. 22 of 2023 (India) ss 2–3

²³ Manik Inder Singh Sethi et al., *Navigating India's Evolving Healthcare Data Landscape: Implications of Digital Personal Data Protection Act, 2023*, *Nat'l Med. J. India* (2026).

²⁴ Digital Personal Data Protection Act, No. 22 of 2023 (India) ss 4–15

²⁵ Digital Personal Data Protection Act, No. 22 of 2023 (India) ss 18–34

V. Rights of Data Principals and Obligations of Data Fiduciaries

Among most distinctive aspects of DPDP Act is its recognition of role of individuals as proactive participants who have enforceable statutory rights in respect of their personal information. Under provisions of law, Data Principals have right to receive information on processing activities, to have any inaccurate personal information corrected or updated, to have unnecessary information erased, to appoint other people for purpose of enforcing statutory rights in certain situations and to have access to grievance redressal measures.²⁶ Such rights complement constitutional recognition of informational privacy since, instead of being passive objects of processing, individuals can now take control of their personal information. The importance of informed consent lies in fact that individuals have a possibility to make informed decisions about whether to give consent to processing or not since processing is usually carried out after individuals are adequately informed about nature and purposes of such processing. The literature uploaded emphasizes that this particular aspect is among key strengths of DPDP Act.²⁷

In that vein, enactment provides for broad statutory obligations that are to be undertaken by Data Fiduciaries, with intent of promoting responsible, transparent and secure processing of personal information. Processing organizations must take necessary measures of ensuring technical and organizational safeguards for personal data, maintaining appropriate security practices, ensuring data accuracy, processing of information for legitimate reasons, informing individuals and regulatory authorities about any data breach incidents and ensuring that adequate measures for grievance redressal are established. In addition, there are some additional compliance obligations imposed on Significant Data Fiduciaries, such as appointment of Data Protection Officers and additional governance measures. All in all, these obligations aim at establishing institutional accountability and encouraging organizations to consider privacy in technological innovations and business activities. However, there are still many concerns voiced by scholars regarding fact that there are many issues related to implementation and operation that are to be resolved through subordinate legislation and rule-making.²⁸

²⁶ Digital Personal Data Protection Act, No. 22 of 2023 (India) ss 11–17

²⁷ Hiral Kapadiya & Nilesh Kumar Kapadiya, *User Privacy in Digital Libraries: Challenges, Implications and Strategies for Safeguarding Information*, 1 *Indian J. Libr. Sci. Res. & Info. Tech.* 37 (2024).

²⁸ Manik Inder Singh Sethi et al., *supra* note 21.

The rights-based regime underpinning DPDP Act shows India's attempt at striking a balance between privacy rights and government functions. Contrary to absolutist view on informational privacy, law accepts that certain forms of processing of data can take place for sake of governance, administration, medicine, employment and other lawful purposes. This is why Act includes a sophisticated set of mechanisms attempting to reconcile rights with regulatory needs. While balancing approach taken by law was appreciated due to its recognition of India's developmental priorities, it was warned that excessive exemptions and discretionary powers granted to government may affect efficiency of law if it is not subject to strict judicial review. Thus, future of DPDP Act depends not only on provisions of law, but also on its constitutional interpretation, independent enforcement and preservation of a fragile balance between privacy and governance.²⁹

VI. The Digital Personal Data Protection Act, 2023 and Artificial Intelligence

The advent of artificial intelligence (AI) has brought about changes in way personal data is collected, analyzed and commercially exploited. The machine learning models, generative AI, predictive analysis, facial recognition technologies, recommendation engines and decision-making algorithms rely on constant streams of large amounts of data that need to be trained, tested and deployed. Such data sets often include large amounts of personal data that are obtained from Internet, health-care systems, educational institutions, finance, social media and public records. Although introduction of AI-powered tools has improved efficiency and innovation in many industries, it has raised questions about informed consent, transparency of algorithm, discriminatory profiling, data ownership and accountability of automated decisions. Therefore, adoption of Digital Personal Data Protection Act, 2023 becomes especially relevant as it provides legal requirements for lawful processing of personal data regardless of whether such processing is performed through advanced AI systems.³⁰

The consent-based framework that is followed under DPDP Act mandates that processing of personal data usually takes place following receipt of voluntary, informed and specific consent of Data Principal. The requirement of said mandate imposes significant practical problems in regard to implementation on artificial intelligence systems that rely on training of models based on datasets with billions of data entries gathered from various sources over prolonged periods.

²⁹ Aman Kumar Jha, Mohit Jain & Tanishk Bhawsar, *Intellectual Property and Personal Data in AI Datasets Under India's DPDP Act 2023*, 4 *Trends Intell. Prop. Res.* 1 (2026).

³⁰ *Id.*

It has been pointed out in uploaded literature that AI developers often face difficulty in establishing ownership of training datasets since Indian law does not provide for any proprietary right over data and also for any ownership rights in regard to aggregated data. However, under DPDP Act, individuals are recognized as having statutory rights in regard to their access, modification and deletion of personal information rather than personal data being treated as any other commercial property. As such, in order for developers of AI systems to establish that their data has been collected and processed according to statutory mandate of DPDP Act, they need to comply with same.³¹

The relationship between artificial intelligence and data protection is further complicated since machine learning algorithms tend to work with personal information in a manner that was unforeseeable and not explained to Data Principals when such data were collected. In many cases, AI technology extracts behavioural insights, predictive analysis, consumer preferences and automatic recommendations through a combination of several data sets that on their own seem not harmful; however, altogether produce very sensitive information about an individual's identity, health condition, financial state or behaviour patterns. This poses great risks related to purposes of data use, transparency, data minimization and informed consent – all being basic principles of DPDP Act. Thus, according to literature review, organizations using AI technologies should apply privacy by design principle throughout process of developing algorithms and make sure personal information is anonymous where possible, access control works effectively and processing of data corresponds to its original purposes explained to Data Principals.³²

VII. Healthcare Data Protection under DPDP Act

Among many different types of personal data being collected and used in digital economy, healthcare data has a special significance as it includes medical history, diagnostics, genetics, treatment data, insurance information and many more confidential aspects related to overall well-being of an individual. The digitization of India's healthcare industry with help of electronic health records, telemedicine services, artificial intelligence-based diagnoses and Ayushman Bharat Digital Mission has made significant improvements in making healthcare industry more accessible and efficient in administration. However, at same time, it has

³¹ Aman Kumar Jha, Mohit Jain & Tanishk Bhawsar, *supra* note 27.

³² *Id.*

increased exposure of such sensitive healthcare data to any kind of theft, ransomware, commercial use, fraud and discriminatory practices. The international examples of such thefts and hacks of healthcare data have proven that unauthorized disclosure of such sensitive information can lead to not only economic losses but even discrimination in employment opportunities, insurance and general social interaction. In this regard, protection of such healthcare data is one of most important applications of Digital Personal Data Protection Act, 2023.³³

Patient autonomy is supported by DPDP Act by treating patients as Data Principals who have rights about their health data. It requires healthcare institutions acting as Data Fiduciaries to process personal data in an appropriate way such that it can be done for legal reasons, there is an informed consent from patient and there is transparency in terms of processing of personal data along with adequate security measures and timely reporting of data breach, where applicable. The literature that has been uploaded notes that there should be a robust cybersecurity system in place at healthcare organizations through use of encryption technologies, access management, staff training, data breach protocols, cloud storage and appointment of Data Protection Officer, where applicable. The need for this arises due to use of artificial intelligence and interoperability of digital platforms in healthcare sector.³⁴

In addition, literature from healthcare industry also discusses DPDP Act in conjunction with India's Digital Public Infrastructure and Ayushman Bharat Digital Mission (ABDM). Whereas decentralized healthcare infrastructures exist in other countries, emerging digital health infrastructure of India is designed to foster interoperability through secure sharing of medical information between different healthcare providers while ensuring privacy of individuals. In this regard, DPDP Act works as a complementary legislation that establishes statutory norms for lawful processing, data minimization, storage limitations, accountability and privacy protections. However, scholars also note that implementation of such regulations would require consistent institutional oversight since cyber attacks against healthcare institutions are lucrative due to monetary value of medical information. Thus, implementation of DPDP Act in healthcare system is contingent not only on statutory requirements but also on technological readiness, accountability, cybersecurity and digital privacy awareness of individuals.³⁵

³³ Manik Inder Singh Sethi et al., *supra* note 21.

³⁴ Digital Personal Data Protection Act, No. 22 of 2023 (India) ss 7–11.

³⁵ Manik Inder Singh Sethi et al., *supra* note 21.

VIII. Intellectual Property and Personal Data: Emerging Legal Challenges

The increasing intersection of AI, innovation and data has caused conventional divide between laws of intellectual property and personal data protection laws to become increasingly blurred. Traditionally, law of intellectual property endeavors to promote innovation and creativity through creation of proprietary rights in inventions, literary works, artistic works, databases and confidential information. On other hand, Digital Personal Data Protection Act, 2023 (DPDP Act) is premised on notion of rights, emphasizing individual autonomy, informational privacy and legitimate processing of personal data. With increasing reliance on data for innovation in digital age, there are frequent intersections between these legal systems resulting in questions regarding data sets, personal data commercialization, copyrighted AI training data and proprietary databases. Organizations operating in digital economy of India have to comply with both IP laws and statutory obligations under DPDP Act.³⁶

One of key areas of interest is issue related to AI training datasets. As already mentioned above, AI companies extensively use huge amounts of material in public domain, copyrighted material, customer information, health data, scientific databases and any other online material to train AI algorithms. While copyright law protects literary and artistic creations, it does not protect factual information. In addition, there is no sui generis database right like in European Union under Indian legislation. In order to secure their commercial interests and maintain value of datasets, organizations typically resort to contract agreements or trade secrets. The DPDP Act completely changes this perspective since under this Act, individuals can claim statutory rights to personal information regardless of whether or not such information was included in commercial databases. Thus, when consent is withdrawn or personal information is required to be deleted under statutory obligation, organizations will have to change their dataset which used to be a valuable intellectual asset for them.³⁷

The connection between trade secrets and personal data constitutes yet another significant legal issue. Companies tend to consider customer databases, behavioral analysis, recommendations engines and unique algorithms to be trade secrets that need to receive legal protection. At same time, provisions of DPDP Act require organizations to fulfill statutory duty to disclose personal information to Data Principals, rectify any inaccurate data, delete information when necessary

³⁶ Aman Kumar Jha, Mohit Jain & Tanishk Bhawsar, *supra* note 27.

³⁷ *Id.*

and process data lawfully. These obligations may, at times, be in opposition to business efforts aimed at keeping company's data secret. The literature therefore recommends that companies be able to make a distinction between personal information and proprietary analysis methods by using such approaches as anonymization, privacy-enabling technology, sound contractual protection and transparent governance framework that will protect innovations on part of business without violating rights of Data Principals as stipulated by Constitution.

IX. Challenges in Implementation of DPDP Act

While DPDP Act, 2023 is first attempt at providing an overarching legislative regime for regulation of digital personal data in India, there still exist several issues related to smooth implementation of this act. Perhaps most common of those is related to wide range of exceptions granted to government bodies under certain conditions. While ensuring national security, public order and effective governance is obviously one of purposes of any government, overbroad exceptions can possibly lead to weakening of actual protection provided to individuals and even to dilution of right to information privacy recognized in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.³⁸ For this reason, scholars point out necessity of strict interpretation of statutory exceptions and presence of judicial control over exercise of executive discretion in this regard.

The other major issue relates to institutional capacity and regulation. The Data Protection Board of India holds a key place in statutory framework since it is tasked with handling complaints, conducting investigations, penalizing violations and ensuring compliance with Act. Nevertheless, efficiency of Board will depend on availability of funds, relevant expertise, autonomy of action, clear procedures of appointments and constant regulatory guidance. It should be pointed out that existing research constantly points to fact that effective enforcement cannot be ensured only through statutory means but needs constant institutional build-up, specialized training, technical expertise and close cooperation between various governmental and non-governmental entities. In absence of strong institutional capacity, best-drafted legislation would not protect from modern cyber attacks and data breaches.³⁹

The changing nature of digital technology adds another dimension to future viability of DPDP Act. The development of artificial intelligence, blockchain technology, quantum computing,

³⁸ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

³⁹ Manindra Singh Hanspal, *supra* note 1.

biometric identification, prediction analytics and cross-border cloud computing occurs in many cases faster than legislation is updated. AI technologies that have capability of making independent decisions, behavioral profiling, face recognition and extensive use of prediction analytics present complicated problems related to algorithm accountability, automated discrimination, obtaining consent from individuals and transparency which can not be entirely resolved by existing act. At same time, international data transfer conducted by multinational corporations presents issue of jurisdiction since personal data often crosses borders of jurisdictions having different levels of protection of people's right to privacy. Thus, it is noted that DPDP Act should be viewed as ever-changing law which needs ongoing revision, regulation and adaptation to changing global digital economy.⁴⁰

X. Conclusion

The passing of Digital Personal Data Protection Act, 2023 is a significant landmark in history of development of India's digital governance system and constitutional obligation regarding information privacy. Drawing from constitutional precedent set by Justice K.S. Puttaswamy (Retd.) v. Union of India, law not only recognizes privacy as a fundamental right but also provides a legal framework that deals with collecting, processing, storing and sharing of personal data in digital form. By creating enforceable rights for Data Principals, assigning statutory obligations to Data Fiduciaries and creating Data Protection Board of India, Act significantly increases India's ability to regulate personal information in a digitally evolving world. On other hand, legislation also attempts to strike a fine balance between constitutional freedom, state duties, business innovations, technology and development.

However, efficiency of DPDP Act will largely depend on how it is enforced and not only its wording. The independence of institutions, transparency of enforcement, strong cybersecurity framework, technological readiness, judicial review, public awareness and constant legislative fine-tuning are some of necessary factors that will allow Act to effectively respond to ever-changing technology. Issues emerging in regard to artificial intelligence, health care data, intellectual property, algorithms' accountability and cross-border transfer of data are clear illustrations of fact that data protection is not a static notion but a dynamic one of a constitutional nature. Hence, India will have to keep reinforcing its legal regime by implementing necessary regulations to foster innovation and at same time ensure constitutional

⁴⁰ Manik Inder Singh Sethi et al., *supra* note 21.

values of privacy, dignity, autonomy and freedom of an individual. Only such an approach can make Digital Personal Data Protection Act, 2023 effective.

References

Cases

- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
- *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
- *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

Statutes

- Digital Personal Data Protection Act, No. 22 of 2023 (India).
- Information Technology Act, No. 21 of 2000 (India).

Journal Articles

- Aman Kumar Jha, Mohit Jain & Tanishk Bhawsar, *Intellectual Property and Personal Data in AI Datasets Under India's DPDP Act 2023*, 4 Trends Intell. Prop. Res. 1 (2026).
- Hiral Kapadiya & Nilesh Kumar Kapadiya, *User Privacy in Digital Libraries: Challenges, Implications and Strategies for Safeguarding Information*, 1 Indian J. Libr. Sci. Res. & Info. Tech. 37 (2024).
- Manik Inder Singh Sethi et al., *Navigating India's Evolving Healthcare Data Landscape: Implications of Digital Personal Data Protection Act, 2023*, Nat'l Med. J. India (2026).
- Manindra Singh Hanspal, *The Digital Personal Data Protection Act, 2023: Key Provisions, Issues and Future Directions*, 6 DME J. L. 12 (2025).

Research Paper

- Gauri Goyal, *Privacy and Data Protection in India: A Critical Analysis of Legal Framework* (UPES Research Paper, 2025).