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

A CRITICAL STUDY OF DATA PROTECTION AND PRIVACY LAWS IN INDIA IN THE DIGITAL AGE

ADESH KUMAR SRIVASTAV

ABSTRACT

Digital technologies have quickly evolved and changed the way that personal information is collected, processed, stored and exchanged. India is now one of the world's biggest digital economies, boasting tremendous growth in internet usage, digital payment systems, e-governance initiatives and data-based services. These advancements have made life easier and more efficient but have brought up many notable issues in relation to privacy, surveillance, cybersecurity, and the misuse of personal information.

As digital platforms become more integral to life and their importance grows, personal information is a resource that can be valuable for governments and applications. The desirability of a general legal/human rights-based approach to data protection is therefore more urgent than ever. The Supreme Court's interpretation of privacy as a right and initiating a quest to create a comprehensive data protection law in the country has brought resurgent efforts to build a new data protection framework in India.

This paper is a critical analysis of the development of privacy rights in India, and the challenges of privacy protection in the digital age with the ***Digital Personal Data Protection Act, 2023***[1] introduction of and the framework of Data protection before and after the Digital act. It also compares the current legal framework with other international, national and regional approaches and suggests possible reforms to improve the protection of privacy and yet accommodate technological innovation and economic growth.

[1] Digital Personal Data Protection Act, 2023

Keywords: Privacy, Data Protection, Digital Personal Data Protection Act, Fundamental Rights, Digital Governance, Surveillance.

I. INTRODUCTION

In the modern era of the 21st century, technology has advanced in ways never seen, that has transformed the role and interaction of one individual, a business and a government. Smartphones, Cloud Computing, Artificial Intelligence, social media, and Digital Payment System have become a part of our life. This creates a tremendous amount of personal information including much you did not know you had that is generated and processed every day, which makes it one of the most valuable resources in today's economy.

The digital journey has accelerated in India with the implementation of various initiatives like Digital India, Aadhaar-based Identification Systems, Unified Payments Interface (UPI), and various other e-governance initiatives. This has enhanced public services and financial inclusion and has gathered and processed vast amounts of information on a scale like never before.

In an era characterized by the widespread use of digital technologies, numerous issues related to autonomy, consent, transparency and accountability have risen to the forefront. Public authorities and private bodies regularly collect details of personality, money, health, conversation and web behavior. Without proper security measures in place, it could be prone to misuse, the disclosure of information, profile or surveillance.

Indian laws have had no thorough legislation providing specific protection to information data. Indian laws had no in-depth legislation focusing only on information data protection before. Some statutory measures referred to principals of privacy and information security but there was no coherent legal regime in place to effectively govern contemporary data processing activities. Thus, the protection of privacy relied mainly on interpretation of the Constitution and judicial action.

But it took a major change in the same when the Supreme Court deemed privacy to be a fundamental right under ***Article 21*** [2]of the Constitution of India. In doing so this recognition

[2] Article 21, Constitution of India

laid the basis for a constitutional concept of informational privacy and the need to enact legislation to manage the collection and use of personal information.

The Digital Personal Data Protection Act, 2023 is the most monumental step towards enforcing an all-encompassing framework for data protection in India. The purpose of the Act is to strike a balance between the legitimate needs of businesses and the State, and individuals' privacy rights. There is, however, several questions to be answered about the effectiveness, implementation and the effectiveness of international standards and can it be done.

Research Objectives

1. To analyze the development of privacy rights in the Indian Constitution.

2. To analyze the legal framework governing data protection before and after the DPDP Act.

3. To critically evaluate the Digital Personal Data Protection Act, 2023.

4. To identify contemporary challenges affecting privacy protection.

5. To highlight proposals that need to be done in order to enhance the data protection system in India.

II. The development of Privacy rights in India.

The approach towards the concept of privacy in India has been largely through the judiciary rather than in the constitution. The Constitution of India does not explicitly mention privacy rights, unlike a few modern constitutions which have made specific mention of privacy rights. Thus, privacy has been an important issue for courts defining the scope and content of privacy protection.

A. Early Judicial Approach

The Supreme Court took a narrow view on privacy to begin with. In ***M.P. Sharma v. Satish Chandra*** [3]the Court noted that the Constitution did not have a standalone right to privacy like that which was recognized in the United States Constitution. The judgement construed

[3] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300

privacy and the right to free from government interference narrowly and understood privacy rights as weak.

In ***Kharak Singh v. State of Uttar Pradesh***[4], a similar argument was used, and the Court studied the police surveillance. In the face of a few invalidations of certain intrusive practices, the bulk of the courts decided not to recognize privacy as a constitutional right in and of itself.

C. Invasion By Conquest 27-28

Passage of ***Maneka Gandhi v Union of India*** [5]led to a widening of personal liberty. The Supreme Court has given a wider interpretation of Article 21 and in its judgment stated that any restriction on the right to personal liberty must meet the test of 'fairness,' 'reasonableness' and 'due' process. This progressive method paved the way for the judiciary to ascribe to Article 21 some rights that were not listed.

In ***Gobind v. State of Madhya Pradesh***[6], the Court recognized that the right to privacy was a right based on fundamental rights enshrined under the Constitution. The judgment did not acknowledge a right to privacy per se but did agree that privacy interests were worthy of constitutional protection.

The jurisprudence furthered developed in ***R. Rajagopal v. State of Tamil Nadu*** [7]where the Court identified an individual's right to block the use of their personal information in an unauthorized publication. Likewise, in the case of ***People's Union for Civil Liberties v. Union of India***[8], it laid down the procedures that must be observed before a telephone can be intercepted and drew links between privacy and personal liberty.

C. Privacy in the Digital Age

The character of privacy concerns has changed due to fast technology developments. The growing reliance on digital databases, biometric identification systems, data platforms and data analytics introduced new risks in terms of surveillance and unauthorized processing of

[4] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295
[5] Maneka Gandhi v. Union of India, (1978) 1 SCC 248
[6] Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148
[7] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632
[8] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301

personal data. Conceptions of privacy were found to have grown limited and unhelpful to cope with these new challenges.

D. The Puttaswamy Judgment

Justice K.S. Puttaswamy (Retd.) v. Union of India[9] was a landmark judgment. In its unanimous decision, which was delivered by a bench of 9 Judges, the Supreme Court had clearly established privacy as a fundamental right as enshrined in the Constitution of India, under ***Articles 14, 19 and 21***[10].

The Court acknowledged that privacy is a multi-dimensional concept that includes bodily integrity, decisional autonomy and informational privacy aspects. It highlighted the importance of respecting dignity, liberty and individual autonomy without providing protection for privacy.

Significantly, the judiciary had set out constitutional principles for meaningful curtailment of privacy. Restriction must meet the tests of legality, legitimate state purpose, proportionality and procedural safeguards. These principles remain relevant to judicial review of state's conduct with respect to surveillance, data collection, and informational privacy.

The Puttaswamy judgment created a constitutional precedent for the broad data protection law and revolutionized the Indian concept of privacy. It also gave an impetus to the recommendations of the Justice ***B.N. Srikrishna Committee Report*** [11]which later went on to shape the impetus of the modern framework of data protection laws in India.

IV. EXISTING DATA PROTECTION FRAMEWORK BEFORE THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Previously, there was no single law in India that focused solely on personal data protection issues and concerns until the Digital Personal Data Protection Act, 2023 was enacted. Rather, appraising privacy and data security was governed by a mix of laws, secondary legal documents, contractual requirements and judicial decisions. All these measures offered some

[9] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[10] Articles 14, 19 and 21, Constitution of India
[11] Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018)

protection, but they were not enough to cover the challenges of today's digital technologies and large data processing.

The ***Information Technology Act, 2000*** [12]was the main law pertaining to electronic information. It was not originally intended to be a data protection law but rather was passed to allow for electronic commerce and to give legal recognition to an electronic record. However, there are some indirect clauses that did cover privacy issues. The Act made a default liability for an organization to be liable if its failure to take reasonable security measures caused any wrongful loss or gain. Additionally, it also imposed a deterrent against the unauthorized disclosure of personal information acquired with contractual arrangements.

In order to enhance the safeguards of personal data, the government enacted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These rules put in place classified private data to incorporate passwords, financial details, health-related information, biometric information and comparable groups. Collected such data had to be from organizations that had to seek consent, provide privacy policies and adopt reasonable security measures.

These gains were not secured without building weaknesses in the structure of the framework. Its range of applications was one of the main shortcomings. Although government agencies gather vast amounts of citizen data, the SPDI Rules applied mostly to the bodies corporate and weren't comprehensive enough to regulate them. In addition, the rules did not apply to ordinary personal information, while they did apply to sensitive personal information.

One drawback was that there was no dedicated regulatory body. In contrast to several other countries at the international level, which created an independent data protection regulator, India primarily used general enforcement mechanisms. As a result, people were frequently unable to get adequate remedies for invasions of their rights of privacy.

Another weak spot of the structure was that it could not accommodate technological developments. New privacy challenges were emerging with the use of cloud services, social media, artificial intelligence, digital payments and data analytics, which could not be tackled effectively with provisions.

[12] Information Technology Act, 2000, No. 21 of 2000.

The challenge of enforcement was another issue. There was limited knowledge among many organizations about their duties in protecting privacy, and limited knowledge among individuals of their rights. A weak legal structure made it uncomfortable for both the regulators and the businesses. All these weaknesses eventually identified the need for a more comprehensive law that could help strike a balance between innovation, economic growth, and personal privacy.

In the recent Justice K.S. Puttaswamy (Retd.) v. Union of India declaration of the right to privacy as a fundamental right also showed the pressing need for a contemporary data protection law. This measure, in conjunction with recommendations made in the Justice B.N. Srikrishna Committee Report, paved the way for the Digital Personal Data Protection Act, 2023.

V. ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

A. Background of the Act

DPDP Act, 2023 is the first all-encompassing personal data protection legislation specifically for personal data protection in India. It took several years of policy discussions, recommendations by expert committees, and deliberations in the legislative bodies for the enactment of the law. One crucial step towards this has been the recommendation on "Right to Privacy" by Justice B.N. Srikrishna Committee Report which highlights the imperative need of devising a framework based on fundamental rights which is effective at ensuring the privacy of digital citizens while also fostering digital innovation.

The aim of the Act is to strike a balance between the protection of personal data on the one hand and its lawful processing for government and business practices on the other. To do so, it tries to alleviate concerns raised over a lack of compliance burden despite fast digitalization on businesses.

B. Key Definitions

A number of key terms are introduced in the Act which give rise to the framework of regulation. A Data Principal is a person to which the personal data is related. The Data Fiduciary are those who decide on the purpose and means of processing personal data. Depending on the characteristics of the information processed, the sensitivity of data and the

possible impact upon individuals, certain entities may be considered as the Significant Data Fiduciary.

The law is primarily applicable to digital personal data and will also be applicable in certain situations when processing takes place abroad while goods or services are provided to people within India.

C. Rights of Data Principals

One characteristic that is particularly remarkable about the Act is that it grants rights that give people power. Owners of Data have right to access information related to treatment of personal data. They can ask for the impossible, untrue or misleading information to be corrected, omitted, amended or deleted, as applicable.

Access to grievance redressal procedure is also provided in the Act. Any person who thinks that his rights have been infringed upon can avail remedies in prescribed steps. The law also allows people to name someone to take care of their rights if they have died or are incapacitated.

These measures contribute to the goal of fostering information autonomy by allowing people to have more control over their personal data.

D. Obligations of Data Fiduciaries

The Act places a number of obligations on those that handle personal data. Data Fiduciaries should ensure that data is processed for lawful purposes and that suitable security measures are put in place to keep data out of the hands of those who unauthorized access to, or disclosure or misuse of, it.

Organizations should also strive to ensure that personal information is correct and eliminate it after the purpose of processing is completed, provided that this is not required by law. Significant Data Fiduciaries has further compliance requirements such as performing audits periodically and appointing Data Fiduciary Officers to monitor compliance and ensure the company is following the legal requirements.

These obligations introduce transparency and accountability and foster good governance of data.

E. Consent Framework

Consent is one of the key components of the law. Consent must be free, informed, specific and unambiguous, according to the Act. The beneficiaries should be acquainted with the purpose of data collection and processing.

Meantime the Act acknowledges certain conditions under which processing could be carried out without explicit authorization. These are when there is a legal requirement, providing state services, Medical emergency and legal uses included in the legislation.

The aim is to achieve a fine equilibrium between freedom and everyday issues for governance and public well being.

F. Data Breach Reporting

With the rise in incidents and data breaches, the necessity of incident reporting has become a crucial aspect of current data protection law. The Act calls on organizations to adopt reasonable security safeguards and appropriate measures to ensure the safety of personal information.

The affected entities are required to inform authorities and affected people if there is a personal data breach, following the prescribed procedures. This is a method to achieve transparency and to ensure that there is some mitigation of potential harm when it does occur, at the right time.

G. Penalties and Enforcement Mechanism

The Act sets out a much tougher penalty regime to incentivise compliance. Fines and penalties are likely to be significant depending on the failure/violation.

Penalty regime demonstrates a ‘harder line' approach and distinguishes between the need for effective and effective means of deterrent. The hefty fines should motivate companies to focus on privacy and data security.

The Data Protection Board has a crucial role to play.

The prime enforcement body for the legislation is the Data Protection Board of India. The Board shall have the authority to investigate complaint(s), make inquiries, give directions and penalties in cases where violations are found.

It is significant that the establishment of a specialised authority is considered an important institutional step, as it offers a vacuum that can be filled with an institutional mechanism for management of privacy-related disputes. But the functionality of the Board will rely much on its functional ability, skill and independence.

I. Cross-Border Data Transfers

Cross-border data flows are key to modern digital economies. The Act's view of this reality is reflected in its rather flexible stance on international transfers of personal data.

Rather than setting strict localization mandates, the law leaves it up to jurisdictions outside the government's restrictions. It is a framework that aims to ease international trade and technological development, whilst making sure national security interests remain protected.

Questions still remain about the effectiveness of the measures that can be applied around data transfer and how it might be difficult to police in different jurisdictions.

VI. CRITICAL ANALYSIS AND CHALLENGES

While DPDP 2023 is a major stride in protection regulations, there are still a few issues left to be addressed with respect to implementation and effectiveness.

One of the hotly contested issues in the bill revolves around government entities and what exceptions are made for them. There are some exemptions in the Act based on the concepts of national security, public order and sovereignty. Although these are good goals, overemphasis on exemptions could be a risk to the privacy rights upheld by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India. The safeguards must be proportionate, necessary and supervised.

Other problems relate to consent fatigue. Many web users are subject to extended privacy notices and consent forms from several online platforms. In reality, many users give their consent without reading the terms of consenting to data processing, allowing it to be understood only partially, if at all. Thus there is a question of true informed consent when it comes to formal consent.

There has been also raised a question about the independence of the Data Protection Board in the institution. The threat of executive influence could have a negative impact on the public

confidence in an effective system of oversight as regulatory authorities are a key player in protecting privacy rights.

Another complicated issue within GDPR is cross-border data transfers. Many jurisdictions have different legal regimes surrounding personal information, and the information is often transferred between them and is commonly shared across the various jurisdictions. To ensure the consistent protection of these kinds of information, it is necessary to collaborate between regulators and create efficient international frameworks.

Recent technologies add to the difficulty of privacy regulation. AI systems continue to draw on vast amounts of data to inform algorithms and provide predictions. Such technologies present significant opportunities, and also risks for profiling, discrimination, surveillance and automated decision-making aspects. Current law might not be sufficient to adequately address these concerns.

It can be seen from the international standards that there are some limitations. The European approach focuses more on regulatory independence, transparency requirements and on individual rights linked to automated decision making. There are opportunities therefore to improve several aspects of the Indian framework.

Implementation of the new regulation is also a big challenge. Four pillars of effective privacy protection include institutional capacity, public awareness, technological expertise and regulatory resources. In absence of these, even well-drafted legislation would not be able to accomplish what it was meant to.

VII. COMPARATIVE STUDY WITH INTERNATIONAL DATA PROTECTION LAWS

International experience can offer valuable insight to be used in the appraisal of the data protection framework in India.

The General Data Protection Regulation (GDPR) of the European Union is the most impactful piece of privacy legislation in the world. The GDPR has a rights-based approach and offers people far-reaching protection. It provides rights on access, rectification, erasure, portability and restriction on processing. The requirements for the regulation also are very strict for organizations and introduce independent supervisory bodies for enforcement.

Indian Regulations take a relatively lenient viewpoint when contrasted to the GDPR. This could make it easier to comply with certain rules and enact economic activity, but it does not offer as many clear protections in other respects, like privacy of automated decisions and data portability.

It works quite differently in the United States. Instead of a single long and all-encompassing federal law, privacy law is primarily fragmented by industry/sectors. Healthcare information is subject to different laws, along with financial, consumer privacy, and children's information. This supersedes the concept of protection but can generate disorganized protections and inconsistent levels of protection.

The United Kingdom has adopted the European model as a framework in the Data Protection Act, 2018 and GDPR for the UK. Compliance and enforcement is a very strong part of the contribution of a robust independent regulatory framework. Good examples of the need to have legal clarity established and that effective institutional arrangements can follow this, can be seen in the UK experience.

There are a number of lessons to be drawn from those comparative models. First, the independence of the regulators adds to the confidence and accountability of the public. Secondly, with transparent processing obligations, users can trust between the parties. Third, broad rights of user enhance informational autonomy. Lastly, there are interdependent relations in a world of global flows of information.

India's framework is indicative of India's priorities and considerations for growth. However, the use of international best practices selectively – not blanket – could further enhance privacy protection without hampering technological innovation.

VIII. SUGGESTIONS AND RECOMMENDATIONS

The framework of data protection in India could be improved through a few reforms.

First, greater independence should be provided to the Data Protection Board. Clear and open appointments, institutional independence would enhance trust and impartial administration.

Secondly, increase public awareness campaigns. But plenty of privacy breaches happen because people are simply not mindful enough of what happens as a result of data sharing. Citizens can learn about empowering themselves by making informed decisions about personal information through digital literacy programming.

Third, for data breach response mechanisms, they need to be better developed by making detailed reporting standards and mandatory mitigation procedures. Safeguarding against breaches can minimize the potential damages to the information.

Fourth, more effective provisions should be in place for the control of the activities of state personnel. Violations of privacy must be consistent with constitutional values such as legality, necessity, proportionality and accountability.

Fifth, India needs to create a specific regulatory regime for artificial intelligence and automated machines. This should be a transparent, fair and accountable regime that should spur innovation.

Finally, alignment with the international standards would enable smoother cross border trade and build trust in the Indian digital ecosystem. A well-rounded, comprehensive and balanced approach that employs and incorporates best practices from around the world, while honouring domestic priorities, would make a significant contribution to long-term privacy protection.

IX. CONCLUSION

The way personal information is gathered and utilised has dramatically changed because of the digital age. With India making significant strides in the growth of technology and economy, the need of safeguarding personal information has become essential in ensuring the dignity, autonomy, and trust in digital systems are preserved.

However, the development of privacy jurisprudence, culminating in Justice K.S. Puttaswamy (Retd.) v. Union of India, created and laid the constitutional framework of contemporary data protection law. Further, the Digital Personal Data Protection Act, 2023 is the most important law in India to date in regulating processing of personal data.

An Act adds certain rights, obligations and enforcement procedures not available under the previous laws. However, there is still debate over whether current protections are sufficient considering issues with government exemptions, regulatory autonomy, new technologies and implementation.

At the end, supreme protection of privacy isn't achieved through the actions of the legislator only. Relys heavily on robust institutions, well-informed citizens, accountable organizations, and adaptations to constantly change in technology. Enhanced accountability, transparency

and protection and the adoption of thoughtfully designed reform would create a robust data protection mechanism in India that would balance innovation, economic growth and constitutional freedoms in the digital era.