A CONSTITUTIONAL APPRAISAL OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: BALANCING PRIVACY AND NATIONAL INTEREST

Aniket Dwivedi, Research Scholar, United University

Riddhi Rastogi, LLM, NIMS University

ABSTRACT

The Digital Personal Data Protection Act of 2023 enables citizens to maintain control over their information by creating standards for handling personal data. The Transparency, accountability and data governance of telecom service providers, mobile application developers and data collection, storage or processing companies is expected to improve considerably with the enacted DPDP Act. Organizations will be compelled to follow this law due to its emphasis on safeguarding the "Right to Privacy," which means these organizations will have to be responsible for their policies and practices regarding the use of personal information strengthening privacy and data protection. Thus, considering the Digital Personal Data Protection Act, 2023 in terms of the privacy rights of individuals is both important and relevant. Anonymity and confidentiality have become integral parts of the right to privacy. Now more than ever, especially in the contemporary digital age where online interaction is the new norm, this right needs to be protected. The Digital Personal Data Protection Act of 2023 holds great significance as it enables citizens and reinforces their rights by establishing concrete guidelines for handling personal data. Activities like operating mobile apps, or even working as a telecom service provider or a business dealing with individual data, require one to be vigilant, ethical, and responsible. Enhanced transparency and accountability will stem from the proper following of Indian laws. This policy reinforces ethical accountability by safeguarding the "Right to Privacy." Organizations are now held responsible for their handling of personal information, which enhances individual privacy and data protection. Therefore, analyzing the Digital Personal Data Protection Act, 2023 within the context of privacy rights is both critical and timely.

Keywords: personal data, data fiduciary, telecom service, transparency, consent-based data processing, right to privacy, personal information, cross-border data transfer, data principal rights, accountability, cross-border data transfer.

Introduction

The rapid explosion of digital content, as well as ongoing technological advances, have made protecting personal data a matter of concern for individuals and entities across the world. Many scholars have argued whether social networking sites impact on the right of individuals to privacy. With the global shift to digitization in recent years with India's current engagement, concerns for data privacy have technology and digitization driven to new heights. The concept of privacy has followed human beings since the beginnings of civilization. It is, however, a fluid concept. For a long time, academics have tried to define privacy in a consistently accepted manner devoid of success as it is culturally and historically interpreted differently. Over the years the right to privacy has grown to include many aspects of what is personal and private which includes anonymity and confidentiality. In present digital times which see on line platforms take center stage in our day to day lives it is very much so that we protect this freedom. The Digital Personal Data Protection Act of 2023 is a key player which empowers citizens and which stands for the put forth of clear rules around the use of personal information.[1] What the DPDP Act does mainly is to improve the degree of transparency, account ability and due care among entities which fall under the Indian legislation's scope including telecom companies, mobile app developers, and businesses which collect, store, or process individual data.

The Landmark Digital Personal Data Protection Act, 2023

The Indian Parliament passed the groundbreaking Digital Personal Data Protection Act (DPDPA), 2023, in August 2023, in efforts to find a balance between the interests of the state and the rights of individuals and businesses by regulating the status of collection, control and retention of the digital personal data. The act is an indication of the strong move depicted by the Indian government to facilitate the control of personal information to the person in the contemporary digital world where personal data is widely transferable on various platforms. It is exclusively modified to the Indian socio-legal context with regards to synchronization of emerging data governance leaders, including the European General Data Protection Regulation (GDPR). The continuous flow of digital information and dynamic technological environment have made the protection of personal data a top priority of individuals, commercial organizations, and state bodies as well. The digital revolution has not merely transformed the

[1] The Digital Personal Data Protection Act, 2023, No.22, Acts of Parliament, 2023.

way we interact, work and live, but it has also become a matter of urgency that we have stringent guidelines that govern privacy and data security[2]. This Act constituted a turning point in the Indian treatment of data, particularly among the governmental agencies, the IT industries, and even the institutions in the private sector. These industries have huge databanks of data, and such data is used in a number of manners including the provision of public services, internet innovations, and advertising. Although the privacy framework is typical of large-scale data initiatives, cooperation between state and commercial actors gives rise to major questions of who may or may not own the data and what access control mechanisms should be applied.

Data Protection and the Right to Privacy

A blurred relationship has existed between data security legislations and the right to privacy. These two are theoretically different concepts, but in reality, they are inseparable. Regarding the privacy as a constitutional right is the major starting point of promoting strict information protection policies. The right to privacy should be well-defined, however, to enable the realization of data protection laws. The term is in fact a controversial one, with different nations having different interpretations and methods of pursuing the concept based on political and cultural lines.

Constitutional Basis

The Digital Personal Data Protection Act, 2023 came into force partially due to a very important Supreme Court judgment in the case of Justice K.S. Puttaswamy v. Union of India. The Right to Privacy declared in this ruling as a very important aspect of the Right to Life under Article 21 of the Indian Constitution was upheld. It also recommended that the central government was to come up with a special framework that would protect the personal data of the individuals. Most human rights documents all over the world recognize the right of privacy as one of the fundamental human rights. These are the Universal Declaration of Human Rights (1948), International Covenant on Civil and Political Rights (1976), UN Convention on Rights of Child (2003) and UN Convention on protection of rights of all migrant workers and members of their families. This is the fundamental meaning of such right as applied to the data information: the power of the individual to control the way his or her data is being collected, distributed, stored, and used. The concept of privacy is one of the oldest, having been traced to

[2] Duraiswami, D. R. *Privacy and Data Protection in India*, 6 J.L. & Cyber Warfare, 169–172 (2017).

the classical distinction between the role of the public (Polis) and the role of the privately owned (Oikos), in Greek civilization; however, the formal expression of a right to privacy is quite modern. This has changed today as privacy has taken on more than a physical sense whereby one is in a place on their own, it has come to mean informational independence as well. The focus of privacy has been changed with the emergence of mass means of communication like print media, television and lately the internet to control digital information. The prevalence of spies by the government and the violation of personal communication that was exposed by Edward snowden and the currently ongoing Pegasus spyware scandal are major examples of the insecurity of the personal data in our hyper-connected world.[3]

Relevance and Modern Impact

The Digital Personal Data Protection Act, 2023 arose as a logical next step towards the protection of privacy and data laws in India. This law aims to build a proactive system which, on one hand, takes into account the advantages of digital advancement but, on the other hand, it considers the need to guarantee the right to privacy to every person.

The Centre of Privacy and Data Protection

The key to protection of personal data is the notion of privacy. Under this principle, individuals, companies, or institutions have a right to make decisions on the way, time, and to which level to disclose or share their personal information privately. This liberty is very subjective and is critical to the successful operation of any democratic society. Nevertheless, it should not come at the expense of privacy, which can only be achieved where data security is strong. Data protection can be defined as the mechanism, rules and laws meant to allow people to be in control of their personal data. It forms the authority over which data to share, who to share it with, how long to share and to what given purpose. The term processing in essence entails the collection, maintenance, utilization, and transmission of information. The main aim of data protection laws is to safeguard the information about a person and organisation against its mishandling, loss or unauthorised access.

[3] Kamath, Nandan. Law Relating to Computers, Internet, and E-Commerce: A Guide to Cyber Laws and the Information Technology Act, 2000, Kamal Law House, Calcutta, 1st ed. 2020.

India's Legal Framework for Data Protection

The Indian type of legal environment of data privacy lays considerable focus on human informational endowment and self-regulation to support the morality of personal data in terms of the reasonable data treatment. These laws have been brought to the spotlight by the increasing number of digital economy with more attention being made to the right to privacy. Indian data protection laws aim at enhancing fairness and accountability by overseeing the processes of the data collection, dissemination, usage and disposal, storage and ultimate destruction of personal data within the international best practice.

The Digital Personal Data Protection Act, 2023, presents new principles, like:

• Confirmation of the right to privacy,

• Purpose limitation: data are to be only used with reasons as initially mentioned, Fair Processing, Lawful Processing,

• And the right to be forgotten giving people freedom to demand that their data be deleted. This law presents the obligations and responsibilities of data principals (data owners, to whom the data refers) and data fiduciaries (the organization that stores and manages the data), thus, creating a well-regulated system of making sure personal data is secure and intact.[4]

A Critical Review of Digital Personal Data Protection Act, 2023

In India the processing of personal data under the DPDP Act occurs in two significant situations namely:

1. Where data is gathered directly and directly through digital format in individuals.

2. Where it has been in physical or non-digital form once, and has been digitised.

Among the remarkable points about this law, there is its extraterritorial jurisdiction. In this case this can go across the Indian borders and apply to data processing performed by foreign parties when selling goods or services to persons in India. But, the Act never confirms explicitly the

[4] Saurabh, S. (2024). "The Digital Personal Data Protection Act of 2023: Strengthening Privacy in the Digital Age." International Journal of Law in Changing World, 3(2), 77–94.

applicability of the provisions to the processing of the data of the individuals residing in a country other than India, which creates grey area in the rights of the jurisdiction.[5]

The law classifies the concept of personal data as any information referring to an identifiable person. It gives the data fiduciaries an obligation to establish mechanisms that provide data safety and makes them keep records of incidents of breach and to notify the regulatory Data Protection Board as well as the affected information subjects. Under the Act, processing of personal information covers a broad scope of activities counting collection, registration, categorization, storing, adjusting, accessing, using, synchronizing and matching of personal data.[6]

Definite and Consent

The Digital Personal Data Protection (DPDP) Act extends the meaning of the data principal to include parents, legal guardians of minors and persons with disabilities. Anyone or entity that decides on goals and methods of processing personal information is termed as a data fiduciary. Agreement within the scope of this law should be:

• Provided with consent, Explicit and definite,

• Well-informed,

• Incompetent, and

• Unequivocal.

Those are only the lawful purposes of the use of data. To have a valid consent, there are legal requirements that it should satisfy. The request of consent should be formulated in easily readable language and should be written either in English or any of the 22 official languages mentioned in the Eighth Schedule of the Indian Constitution. It should also contain the contact of the company-nominated Data Protection Officer or any other authorised individual.

[5] Asbury, J., McClelland, M., Torgerson, K., Vincent, I., & Boling, J. *Law and Business Technology*.
[6] Suri, Isha & Kathuria, Rajat. "Digital Personal Data Protection Act: The Speedbumps Ahead", *The Indian Express*, February 1, 2025

Security Practices in Data

To guarantee the security of personal data of users and to reduce the likelihood of data leakage, organizations are bound to introduce relevant security models. These are clear data governance policies, and standard operating procedures, and technical safeguards. The new guidelines impose some specified protection measures that a data fiduciary is supposed to follow.

Liberties accorded to social media users

The DPDP Act bestows diverse rights on data principals, which enables them to have increased power over their personal information. The following are the entitlements:

1. **Right to Information**

The subjects are entitled to be notified of the character of the personal data that is being collected and the reasons towards its collection and how it will be processed or used. This disclosure allows those using it to make informed choices when sharing their data.[7]

2. **Rectification and Erasure**

The information related to data principals has the right to ask to change anything inappropriate or misleading about them. Those also reserve the rights to require the deletion of information which is no longer to its intended purpose or is determined to be not necessary.

3. **Right of Data Portability**

The individuals also have the right to obtain the transfer of their personal data between service providers in a form commonly used and technical feasibility. Even though the right to data portability is not explicitly coded in the Digital Personal Data Protection Act (DPDPA), which is the case in other jurisdictions, including the General Data Protection Regulation (GDPR) in the EU, the regulation does give individuals some level of autonomy in the process of managing and transferring their personal information to various platforms.

4. **Protection to Make Objections**

[7] Patel, Mamtaben Danabhai (2023). "Critical analysis of Digital Personal Data Protection Act, 2023

One has a right to refuse processing of his/her personal data in certain situations especially when it comes to the utilisation of such data to some purposes which do not align with the purpose in accordance with which the data was initially obtained.

Grievance Resolution Mechanism (Data Protection Board)

If a data principal feels that their rights have been infringed upon or that their personal information has been misused, they have the right to lodge a formal grievance with the *Data Protection Board of India (DPBI)*. To facilitate the implementation of the DPDPA, the central government is responsible for establishing this board, which serves as a regulatory and quasi-judicial body.

The Data Protection Board (DPB) will:

- Oversee compliance with the DPDPA,
- Investigate reported data breaches,
- Monitor adherence to data protection regulations by data fiduciaries,
- Function primarily through digital platforms to encourage accessibility and streamline procedures.

In cases of non-compliance, the board holds the power to:

- Suspend operations of the offending entity,
- Issue corrective directives,
- Revoke or annul business registrations.

If a party disagrees with the DPB's determination, they may file an appeal with the *Appellate Tribunal*. All such appeals are required to be submitted electronically.[8]

[8] Ministry of Law and Justice, *The Digital Personal Data Protection Act, 2023*, No. 22 of 2023, Gazette of India, August 11, 2023

Children and Social Media Usage

The DPDP Act mandates that minors defined as individuals under the age of eighteen—must secure verified *parental consent* to access or register on social media platforms like YouTube, Meta (formerly Facebook), or Tinder.

In these cases, social media service providers must:

- Verify the age of the minor user,
- Authenticate the identity and consent of the parent or legal guardian.

The Act allows for two primary verification mechanisms:

- If the parent is already a user of the platform, their existing account information (age and identity) may be used to authenticate the request.
- In the absence of a parent account on the platform, an authorised institution—such as a governmental agency or certified digital locker provider—can validate the identities of both the child and the parent.

Union Minister of Electronics and Information Technology, Ashwini Vaishnaw, proposed a model where: "Virtual tokens connected to a parent's verified identity and age could be employed, voluntarily submitted by the parent. These tokens would be generated by the tech industry and could, over time, be integrated with various forms of identification."

However, the Act outlines certain exceptions. For example:

- Medical professionals may process a minor's personal data without parental approval if it is essential for providing healthcare or protecting the child's well-being.
- Academic institutions may handle data for educational functions.
- Governmental or certified bodies offering licenses, scholarships, benefits, or other public services may process a child's data under applicable legal authority.

Comparison Between India and Developed Nations

In the digital era the security of data is essential to avoid loss of individual dignity and confidentiality. The segment analyses and compares data privacy regulations of India and the United States, focusing on the differences caused by distinct legal cultures and socio-cultural environment. The United States follows the pattern of fragmented and sectoral regulation where the regulation of data is decentralized in the form of different laws addressing specific industries some of which are COPPA (children data), HIPAA (healthcare data), and CCPA (consumer rights) as well as encouraging voluntary regulation through a self-regulatory mechanism.[9]

German, by contrast, the Digital Personal Data Protection Act, 2023 (DPDP Act) of India, establishes a unified, integrated body of law that transcends industry and which is extraterritorial. It balances many state activities surrounding governance of data into one position and gives individuals rights over access and control of their data including the right to consent, remedy, and deletion.

Although the two countries want to have a balance between the privacy rights and the economic benefits, they differ in large measure in the mechanisms of enforcement, the extent of regulation as well as the government supervision. These divergent models provide an idea on how dynamic and changing data protection approaches can help digital transformation and personal rights within an evolving environmental framework.[10]

Conclusion

The enactment of the Digital Personal Data Protection Act, 2023 is a significant milestone in the progress of India as far as fulfilling a comprehensive data governance is concerned. The Act is trying to balance the pressure of the data-based economy and the need to safeguard individual privacy. Through its ability to give a systematic framework of how digital personal information can be collected, used and stored, the Act not only gives people rights over data, but it as well imposes duties legally on data fiduciaries.

[9] European Union, *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679, Official Journal of the European Union, May 4, 2016.
[10] Burman, Anirudh (Oct 2023). "Understanding India's New Data Protection Law." Carnegie Endowment for International Peace.

Nevertheless, there is still a number of unanswered questions:

• User control and consent architecture

• Processes of internationally transferring data

• High turnover of DPB member, which may affect stability of regulations

Since India went on an incessant bout of establishing itself as a digital powerhouse, it is predictable that the DPDPA will be iteratively rewritten to fit emerging technological realities as well as legal gray areas. The law creates a solid grounds in terms of ascertaining data autonomy as a part of the vision of a Digital India that upholds rights, innovation, and an inclusive governance system.

References

1- The Digital Personal Data Protection Act, 2023, No.22, Acts of Parliament, 2023.

2- Duraiswami, D. R. *Privacy and Data Protection in India*, 6 J.L. & Cyber Warfare, 169–172 (2017).

3- Kamath, Nandan. Law Relating to Computers, Internet, and E-Commerce: A Guide to Cyber Laws and the Information Technology Act, 2000, Kamal Law House, Calcutta, 1st ed. 2020.

4- Asbury, J., McClelland, M., Torgerson, K., Vincent, I., & Boling, J. *Law and Business Technology*.

5- Suri, Isha & Kathuria, Rajat. "Digital Personal Data Protection Act: The Speedbumps Ahead", *The Indian Express*, February 1, 2025.

6- Saurabh, S. (2024). "The Digital Personal Data Protection Act of 2023: Strengthening Privacy in the Digital Age." International Journal of Law in Changing World, 3(2), 77–94.

7- Patel, Mamtaben Danabhai (2023). "Critical analysis of Digital Personal Data Protection Act, 2023.

8- Ministry of Law and Justice, *The Digital Personal Data Protection Act, 2023*, No. 22 of 2023, Gazette of India, August 11, 2023

9- European Union, *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679, Official Journal of the European Union, May 4, 2016.

10- Burman, Anirudh (Oct 2023). "Understanding India's New Data Protection Law."