THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A Milestone Of Digital India

-By Yesh Gangal (5th year, BLS/LL.B)

1. INTRODUCTION

In todays technologically advanced world, we engage in innumerable kinds of digital transactions and processes on a daily basis. As far as India is concerned, it has emerged as one of the largest countries, where digital payment platforms, services, processes etc. are used by a huge chunk of population on a daily basis.

Technology has made our daily activities easier and more accessible without any doubt. But while doing so, it has also culminated into citizens of our country creating their digital imprints unknowingly by way of creating, giving access and gaining access of digital data on a daily basis.

When we speak of digital data what comes to our mind first and foremost, is the creation and protection of privacy of our digital data.

But what exactly is meant by “Data Privacy”?

[1]Data privacy, also called "information privacy," is the principle that a person should have control over their personal data, including the ability to decide how organizations collect, store and use their data.

[1] https://www.ibm.com/topics/data-privacy

2. **CASE LAW**

Justice K.S.Puttaswamy(Retd) vs Union Of India

(AIR 2018 SC (SUPP) 1841)

[2]This case was initiated through a petition filed by Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court in relation to the Aadhaar Project, which was spearheaded by the Unique Identification Authority of India (UIDAI). The Aadhaar number was a 12-digit identification number issued by the UIDAI to the residents of India. The Aadhaar project was linked with several welfare schemes, with a view to streamline the process of service delivery and remove false beneficiaries. The petition filed by Justice Puttaswamy was a case which sought to challenge the constitutional validity of the Aadhaar card scheme. Over time, other petitions challenging different aspects of Aadhaar were also referred to the Supreme Court.

This case is the cornerstone of the 'Right to Privacy' jurisprudence in India. The nine Judge Bench in this case unanimously reaffirmed the right to privacy as a fundamental right under the Constitution of India. The Court held that the right to privacy was integral to freedoms guaranteed across fundamental rights, and was an intrinsic aspect of dignity, autonomy and liberty.

It can rightly be said that the concept of privacy, especially digital privacy of personal data had emerged from this case.

[2] https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors#:~:text=Case%20Brief&text=The%20nine%20Judge%20Bench%20in,of%20dignity%2C%20autonomy%20and%20liberty.

When we take a look at the objective and scope of the DPDP act, the following comes to our attention.

The digital personal data protection act, 2023(DPDP act) is an "[3]Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto."

This Legislative piece has been enacted for the sole purpose of Protecting, handling and processing of the personal data of the citizens of the country.

The DPDP act has also classified persons into different classes like the Data Fiduciaries and Data Principals.

To understand this better we will have to take a look at some of the key definitions provided in the act.

3 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

3. KEY DEFINITIONS

a) [4]"Consent Manager" means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

b) "data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means.

c) "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

d) "Data Principal" means the individual to whom the personal data relates and where such individual is—
   i) a child, includes the parents or lawful guardian of such a child.
   ii) a person with disability, includes her lawful guardian, acting on her behalf.

[4] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

e) “Data Processor” means any person who processes personal data on behalf of a Data Fiduciary.

f) “Data Protection Officer” means an individual appointed by the Significant Data Fiduciary under clause (a) of sub-section (2) of section 10.

g) “digital personal data” means personal data in digital form.

h) “personal data” means any data about an individual who is identifiable by or in relation to such data.

i) “personal data breach” means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.

Now, having seen some of the key definitions included in the act let us understand the applicability of the DPDP act.

4. APPLICABILITY

The DPDP Act applies to the processing of personal data collected in digital or non-digital form and then subsequently digitized.

The DPDP Act does not apply to personal data processed by an individual for domestic or personal use and any personal data that is made or caused to be made publicly available by either the data subject or by an individual under legal authority to do so.

If digital personal data processing is associated with providing goods or services to data principals within India, the DPDP Act has an extraterritorial application.

Additionally, the Central Government of India may, within five years of the commencement of the DPDP Act, exclude data fiduciaries or classes of data fiduciaries from the application of any provision of the DPDP Act for a notified period.

As now it is vividly clear from the above points that certain duties are cast on the Data Fiduciaries, let us have a brief look at them.

5. DUTIES OF DATA FIDUCIARY

1. Lawful Basis of Processing

Personal data may only be processed for a lawful purpose for which the data principal has given or is deemed to have given his/her consent or for certain legitimate uses. Any purpose that the law does not specifically and explicitly prohibit is known as a lawful basis. The DPDP Act's provisions and any other applicable rules or regulations that may be adopted under the DPDP Act must be implemented when processing personal data.

2. Consent Requirements

The consent given by the data principal shall be free, specific, informed, unconditional, and unambiguous with clear affirmative action, and shall signify an agreement to the processing of their personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.

The data principal must be given access to any request for consent made in accordance with the provisions of this Act or any related rules in clear, plain language, with the option to access the request in either English or any other language listed in the Eighth Schedule to the Constitution of India.

3. Notice Requirements

The data fiduciary must notify the data principal when obtaining or receiving their consent. The notice should include the exact personal data being processed and the intended purpose of the data processing.

The notice shall also explain the procedures through which the data principal can exercise their right to withdraw consent, as well as information regarding how to submit a complaint with the data fiduciary and the Board. The data fiduciary must make the notification available to the data principal, allowing them to read it in English or any other language listed in Schedule 8 of the Indian Constitution.

4. Security and Data Breach Notification

A data fiduciary must implement the necessary organizational and technical security measures to protect personal data and ensure compliance with the DPDP Act. The Board and each impacted data principal must be notified in the event of a personal data breach by the data fiduciary or data processor.[5]

After having seen the duties given under the DPDP act, let us now look at the Rights provided for Data Principals.

[5] https://securiti.ai/india-digital-personal-data-protection-act-vs-gdpr/#:~:text=Both%20India's%20DPDP%20Act%20and,compliance%20with%20the%20DPDP%20Act.

6. RIGHTS OF DATA PRINCIPALS

1. Right to Information and Access to Personal Information

The data principal has the right to inquire the data fiduciary about their personal data, including whether it is being processed, how it is being processed, who is processing it, with whom it has been shared, and what categories of personal data have been shared.

2. Right to Correction & Erasure

A data principal has the right to update and delete their personal data. A data fiduciary is obligated to update a data principal's personal data in the systems in accordance with any updates made after receiving a request for such correction of the personal data from a data principal. The data fiduciary is also required to destroy any personal data that is no longer required for the original reason it was collected and processed unless retention is required by law.

3. Right to Grievance Redressal

A data principal can lodge a complaint with the Consent Manager or a data fiduciary. The data principal must use this right prior to bringing any grievances to the Board for any grievance redressal.

4. Right to Revoke Consent (opting out)

When the data principal's consent is the foundation for processing personal data, he has the right to revoke his consent at any time, using a withdrawal process that is just as straightforward as giving the original consent.

To understand the overall provisions of the act in a realistic manner, let us compare them with the provisions of European Union’s General Data Protection Regulation (GDPR).

We would be making this comparison on the basis of the basic provisions, definitions, structure and penalties given in both these acts.

7. COMPARATIVE ANALYSIS

1. Structure

   The EU's GDPR is divided into articles and schedules.

   Meanwhile the DPDP act is divided into sections and schedules.

2. Definitions and Terminology

   India's DPDP Act defines 'personal data' as any data pertaining to an identifiable individual. Anyone who, alone or in conjunction with others, determines the purpose and means of processing personal data is known as a Data Fiduciary.

   GDPR, on the other hand, defines personal data as any information that relates to an individual who can be directly or indirectly identified. The GDPR regards the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing personal data as a Data Controller.[6]

[6] https://securiti.ai/india-digital-personal-data-protection-act-vs-gdpr/#:~:text=Both%20India's%20DPDP%20Act%20and,compliance%20with%20the%20DPDP%20Act.

3. Scope and Jurisdiction

The DPDP Act applies to the processing of digital personal data within the territory of India, where the personal data is collected in digital form or in non-digital form and is subsequently digitized.

The GDPR has a more advanced approach towards its applicability, covering both territorial and material aspects.

It is so because, as per the GDPR Processing of personal data of data subjects in the EU, regardless of whether the controller or processor is located may be done, if the EU data subjects are targeted with goods or services or their behaviour is monitored.

But in the DPDP act, the monitoring of behavioural aspects of Data Principals is not brought within the ambit of the act and hence this can form a serious loophole regarding the privacy of such data.

4. Approach to Cross-Border Data Transfers

The DPDP Act does not expressly prohibit cross-border data transfers or prescribe any specific compliance requirements (like obliging with standard contractual clauses, transfer impact assessments, etc.) for transferring personal data outside India.

However, in the case of the GDPR, a transfer of personal data to a third country or an international organization may take place where the European Commission has determined that the third country, a specific territory, one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection such as SCCs, BCRs, impact assessments, etc.

5. Enforcement Mechanisms and Penalties

The Indian government has nominated the Data Protection Board of India as the regulatory authority to implement the provisions of the DPDP Act. The Board may also direct data fiduciaries to adopt any urgent measures - in the event of a data breach - to remedy such personal data breach or mitigate any harm caused to data principals. Fines range from ten thousand Indian Rupees to two hundred and fifty crore Indian Rupees. Under the DPDP Act, the data principals are required to exhaust the remedy available to them for redressal of grievances by approaching data fiduciaries or consent managers before approaching the Data Protection Board.

Under the GDPR, each Member State is responsible for assigning independent public authorities ('supervisory authority') to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union. Less severe infringements can result in a fine of €10 million or 2% of a firm's entire global turnover of the preceding financial year, depending on which amount is higher. More serious violations can result in a fine of up to €20 million or 4% of a firm's entire global turnover of the preceding year, depending on what is higher.[7]

[7] https://securiti.ai/india-digital-personal-data-protection-act-vs-gdpr/#:~:text=Both%20India's%20DPDP%20Act%20and,compliance%20with%20the%20DPDP%20Act.

8. CONCLUSION

The digital personal data protection act, 2023 marks an important advancement in establishing a data protection framework in India, while navigating a complex terrain.

But despite that being true, certain refinements in the Act's provisions, particularly in reinforcing checks on governmental powers and placing a greater focus on privacy rights and increasing the applicability and scope of the act could enhance its effectiveness in creating a more robust data protection regime in India.