19

THE NASCENCE OF DATA PRIVACY LAWS IN INDIA: AN ANALYSIS OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023

ANU SINGH & MEGHA MISHRA

ASSISTANT PROFESSORS, FACULTY OF LAW, INVERTIS UNIVERSITY, BAREILLY, UTTAR PRADESH

Abstract

"The walls have ears", is the idiom inspired from the tale of Dionysius of Syracuse who made an ear-shaped tunnel and connected it to the chambers of his palace so that he could hear what was being spoken in another room. Modern technology has adapted from this story with some additional features. Data collecting has become so sophisticated that occasionally even a simple notion will appear on our screens right away. What could seem unsettling to the average user generates enormous financial rewards for businesses that survive on, deal with, and trade on this data. Everything we do now, including purchasing, browsing, and viewing, is done online, and this increase in online activity has given businesses access to vast amounts of data that have been used to analyze customer behaviour and habits. By 2025, 900 million Indians are expected to utilize the Internet, making the Data Protection Act essential**.**

The regulation intended to safeguard citizen privacy and, more critically, consumer data. The Digital Personal Data Protection (DPDP) Bill, which has been under consideration for years, was approved by the Monsoon Session of Parliament and is now an Act after President Droupadi Murmu's signature.

In this chapter the following discussions will be made-

I. Analyze the key features of the Digital Personal Data Protection (DPDP) Act, 2023;
II. Compare DPDP Act with its contemporary General Data Protection Regulation of the European Union;
III. Discuss the adequacy of the DPDP Act concerning data protection required in India.

Introduction

India promulgated the Digital Personal Data Protection Act, 2023 (DPDP Act) on 11th August 2023, establishing new standards for the handling of digital personal data. The primary goal of the DPDP Act is to give legal acknowledgement to certain aspects of confidentiality while balancing the requirement to process personal data in accordance with the law.

However, India has only had a right to privacy as a fundamental right for the past six years after the *Justice K.S. Puttuswamy case*[1], previously it was denied by the Indian Supreme Court *in the Kharak Singh case*[2] due to a judicial interpretation that the fundamental rights in the Indian Constitution do not encompass right to privacy. Legislation on the protection of digital data is considerably different from the one that was discussed for half a decade, the reason being changes in public discerning and constantly changing technologies and related issues. While this is going on, personal data pools are being assembled and processed everywhere.

Personal data protection necessitates a combination of data security and the rights granted to the individual depicted by the data. Though data security is a significant facet of data protection it is also approached by laws addressing the protection of electronic data storage, other important aspects of data protection such as an individual's right to be informed and his prior approval for data collection, processing, and sharing, data quality, and remedies available to the individual as a result of these rights, are frequently overlooked. In India, statutory data protection is not limited to information technology regulations. Other laws exist that secure critical features of data protection, even if such protection is secondary to their primary goal. Recognizing the provisions of law ensuring such rights, as well as a study of the procedures set forth for their execution, might be the first step toward optimal data protection under current laws and, finally, the formulation of a complete data protection system.

Information that may be used to identify or contact a specific individual is known as personal data. Personal data is processed by both businesses and governmental organisations in order to supply goods and services. Processing personal data enables comprehension of user preferences, which may be helpful for customization, targeted advertising, and suggestion development. Law enforcement may benefit from the processing of personal data. Unchecked processing may have detrimental effects on people's privacy, which has been acknowledged as a basic right. Individuals may suffer harm from it including financial loss, reputational damage, and profiling.

In the seventy-seventh year of independence, India's experimentation with data privacy laws has finally come to an end with the passing of the Digital Personal Data Protection Bill, of 2023. The journey of this legislation from a Bill to an Act was an arduous one. India lacked a stand-alone data protection law although the Information Technology (IT) Act of 2000 governed the use of personal data, it has been noted that this framework is insufficient to guarantee the protection of personal data. The voyage of this legislation in the vast sea of possibilities started with a Committee of Experts on Data Protection, headed by

[1] Justice K.S. Puttaswamy (Retd) Vs Union of India (2017) 10 SCC 1
[2] KharakSinghvsTheStateofU.P.&Ors.,1964 SCR (1)332

Justice B. N. Srikrishna, which was established by the national government in 2017 to look into matters pertaining to data protection in the nation. In July 2018, the Committee turned in its report and the Personal Data Protection Bill, 2019 was presented in Lok Sabha in December 2019 based on the Committee's recommendations. A Joint Parliamentary Committee was given the Bill for review, and it delivered its report in December 2021. But the Bill was withdrawn from Parliament in August 2022 due to the remorse of stakeholders and data hoarders. With an increasing population, India is the biggest market for business companies like 'Meta' and Google, and a comprehensive data protection law in India will be unfavourable for them.

Analysis of the DPDP Act, 2023

The DPDP Act, 2023 divided into nine chapters, 44 sections and one schedule of penalties, lacks a sunrise clause and is most likely to be implemented gradually through various notices in the Official Gazette. After implementation, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011 (SPDI Rules) and Section 43A of the Information Technology Act, 2000 will no longer be in effect. As long as they do not contradict the DPDP Act, other relevant data processing regulations, including sectoral ones, will still be in effect. The Data Protection Board of India (DPBI), which would be in charge of implementation, investigation, and adjudication under the DPDP Act, is also to be established. Different portions of the DPDP Act are concentrated on tried-and-true core data processing principles, with specifics left up to rule-making. Application of the DPDP Act is made easier with limited exceptions, the DPDP Act is pertinent to Data Fiduciaries and Data Processors handling digital personal data inside or outside of India. Some key features of the Act are discussed below-

1. **Digital Personal Data**- Section 2(n) of the Act defines digital personal data (DPD) *as "personal data in digital form"*. A natural person i.e., a data principal who can be recognised or located using such data is said to be the subject of any organised representation of information, facts, thoughts, views, or instructions in digital form. It will contain personal data that was gathered digitally or non-digital sets that were later converted to digital format. Pseudonymized data will be considered personal data and covered by the DPDP Act since it can be paired with identifiers to reveal the identity of the Data Principal.
Furthermore, although it may be an important factor in determining the categorization of Data Fiduciaries and the imposition of fines, the DPDP Act's applicability is independent of whether personal data sensitive, such as health, financial, biometric, etc. Since the SPDI Rules currently only apply to the processing of sensitive personal data, many businesses that do not deal with sensitive data nonetheless handle personal data as needed to meet actual business requirements. Any entity that processes any personal data after the DPDP Act is implemented will need to comprehend it and abide by its requirements.

2. **Processing-**Processing includes the complete data processing lifespan, from data collection to deletion, and includes wholly or partly "automated" activities done on personal data. Any digital data processing that may operate automatically in response to commands or otherwise is considered automated. So, only non-automated procedures are excluded, and semi-automated processing will be covered.
3. **Territorial nexus-** The Digital Personal Data Protection Act must be followed whenever a person whether natural or legal, processes personal data inside of India, regardless of whether they are physically present or have an Indian incorporation and regardless of whether the personal data belongs to the Data Principal inside or outside of India. For instance, the DPDP Act will be applicable to the processing of personal data of Data Principals based in Russia but inside of India by a Russian enterprise.

The DPDP Act only applies when processing takes place outside of India and is done so in order to provide data principals with goods or services within Indian territory. Processing carried out only for the aim of profiling people is not considered to be an extraterritorial application.

4. **Exemptions-** According to the DPDP Act, processing of personal data (PD) for the following reasons is exempted-

(i) For domestic or personal use; and

(ii) If personal data becomes publicly available as a result of the Data Principal's voluntary actions, such as comments made on social media or as a result of disclosures made in accordance with applicable law;

(iii) Furthermore, for the sake of specific protective grounds like sovereignty, maintaining public order, etc., the Central Government has the authority to inform authorities from the state government that would be excluded from the DPDP Act. Also, for a period of five years from the DPDP Act's start date, the central government may exclude various categories of Data Fiduciaries from any of its provisions.

5. The prerequisite of 'Consent' for data processing- The key legal justification for personal data processing is consent. The DPDP Act goes into detail on the qualitative and practical characteristics of valid consent. According to Section 6 of the Act 'consent' must have the following qualities: it must be *"free, specific, informed, unconditional, and unambiguous*". The technical definition of consent is a data principal's unambiguous affirmative action indicating approval of PD processing for a certain purpose. What this entails for companies is an issue that arises because the DPDP Act does not go into detail on this.

(i) Free- It would likely refer to the consent given voluntarily and without compulsion, undue influence, fraud, deception, or error as defined under the Indian Contract Act of 1872. The burden of evidence would be on Data Fiduciary, and in this case, it would be necessary to show that all other consent standards have been met. Whether consent is free or not will be based on facts.

(ii) Specific- It is used for concepts of purpose restriction and data reduction. Consent should only be granted for well-defined, clearly defined, and acknowledged legitimate objectives. Additionally, the consent that is being sought should only apply to the processing of personal data that is required for the particular purpose. For instance, a healthcare app gets the user's approval before processing their health information and gaining access to their phone contacts. Data Principal agrees to both, if

the service provider utilises the phone contact list for mass marketing messages the consent due to the absence of the legal purpose or the personal data required for it, will be considered invalid, and the processing that results will be illegal.

The majority of consent languages are now hosted generically and open to a variety of use cases. A wide range of data is gathered in advance of potential applications and repurposing. Such permission letters are likely to become invalid with the introduction of the DPDP Act, thus organisations must start the appropriate internal data screening, examine their data inventory and segregation capabilities, and assess both critical and non-critical business use cases as a first step. In essence, precise data mapping is what is required right now.

(iii) Informed- The idea of being informed derives from the transparency concept and calls for informing the Data Principal about personal data processing. To this end, Data Fiduciary would have to inform Data Principal in writing before or at the time consent is requested. This notice should provide the Data Principal with information about-

(a) the personal data that will be processed;

(b) the reason for processing;

(c) how to exercise their right to withdraw consent (as discussed later) and address grievances;

(d) how to file a complaint with DPBI; and

(e) the contact information of the Data Fiduciary's authorised person acting as SPOC with the Data Principal regarding their data rights.

Compared to what was envisioned in the prior suggested versions, the aforementioned information flow is quite constrained. However, it also highlights the necessity for enterprises to be aware of their managed and owned data pools, sources of collection, and use cases. As a result, itemised consent notices are now required. The learnings would then need to be incorporated into consent notifications to meet the requirements of the DPDP Act.

(iv) Unconditional- This refers to the idea that permission shouldn't be tied to the provision of goods or services. The capacity of the Data Principal to revoke permission is an essential consequence. Data fiduciaries are required to put in place simple withdrawal procedures. When consent is revoked, already completed processing is not deemed invalid. After withdrawal, however, Data Fiduciaries must order their Data Processors to stop processing, unless doing so is allowed or required by the DPDP Act or another legal provision

Take the situation of a Data Principal who, after giving their consent to the processing of their data on an e-commerce platform for the purpose of making a purchase, pays for a specific order and then withdraws their consent. The e-commerce platform must stop processing PD, although it may continue to do so in order to fulfil the order that has been placed.

In a roundabout way, this means that policies and procedures must evaluate the requirement for deploying privacy enhancement tools (PETs) and employ selective personal data retention techniques in order to carry out necessary processing operations after permission has been revoked, either by law or contract. Additionally, businesses must begin enhancing or adopting consent management and consent preference architecture that would enable people to examine, modify, and withdraw their consent.

(v) Unambiguous- It would be necessary for consent wording to be unambiguous if it weren't clear and concise. The verbose and generalised consent languages are now in use. This outdated practice must be evaluated since such permission papers would weaken the requirements of the DPDP Act. Additionally, the DPDP Act requires Data Fiduciaries to offer consent methods in both English and other Indian official languages.

A definite positive response is a sign of expressed consent. It denotes that the Data Principal actively chooses to consent to data processing by taking particular, intentional action. The DPDP Act's criterion would not be met by the current practice of presumed consent resulting from default settings or opt-out methods.

Pre-ticked permission boxes are no longer acceptable. Businesses will be prodded by this technological element to change default settings, adopt granular opt-in methods (with explicit banners and action items like swiping, clicking, or voice recordings), and begin analysing the need to improve consent gathering and administration systems.

In addition to the aforementioned, the DPDP Act stipulates particular consent-related conditions for the personal data of minors and people with disabilities. Additionally, it acknowledges consent flows via authorised consent managers.

Furthermore, it acknowledges consent flows via authorised consent managers. The DPDP Act also stipulates a few legal justifications for processing personal data. In our upcoming blogs, we'll delve into these elements. Additionally, it acknowledges consent flows via authorised consent managers. The DPDP Act also stipulates a few legal justifications for processing PD. In our upcoming blogs, we'll delve into these elements.

6. Data Processors: What's at Risk, exactly?-The DPDP Act imposes a number of duties on data fiduciaries, including permitting data principal rights and putting adequate security measures in place. Violations of these duties might result in severe fines. The Data Fiduciary is also responsible for making sure there are no data breaches. However, Data Processors are not independently obligated in any way. According to the DPDP Act, a Data Fiduciary may enter into a legally binding contract with a Data Processor to hire them for a variety of processing tasks. Additionally, it mandates that Data Fiduciaries be responsible for the deeds and omissions of Data Processors. Given that data processors manage personal data (PD) on behalf of data fiduciaries, this strategy makes sense and is in line with current worldwide legislative trends.

But it would no longer be optional to perform thorough data and infosec diligence before onboarding, to complete thorough data processing agreements, and to undertake periodic audits on the processor's ecosystem.

Data Fiduciaries must be aware of the administrative, technological, operational, and physical security measures employed by the Data Processor. Since the DPDP Act would serve as the fundamental eligibility requirement, Data Processors would naturally be subject to the same contractual covenants that would apply to Data Fiduciaries. Along with this, it will be crucial for data processors to assess the appropriateness and applicability of their current processing lifecycle, deployed security technologies, breach notification and mitigation measures, including business continuity plans, cyber and breach incident insurance coverages, the validity of their current standards and certifications, and, most importantly, the creation of a thorough communication strategy to set expectations and fulfil contractual obligations.

7. Processing of personal data only for a 'lawful reason'-Only legitimate uses of personal data may be carried out with the consent of the data subject. In some circumstances, consent may be assumed. There are many exclusions from the Bill that pertain to the State's handling of personal data. The State is defined as the following under Article 12 of the Constitution: (i) the central government; (ii) the state government; (iii) the local bodies; and (iv) the authorities and businesses established by the government. In 2017, the Supreme Court ruled that any violation of the right to privacy must be proportional to the justification for the intrusion. Data collection, processing, and retention may go beyond what is required as a result of the exemptions. This might not be reasonable and go against people's basic right to privacy.

The Act gives the central government the authority to exclude processing by government agencies from any regulations where doing so will benefit goals like maintaining public order and state security. Except for data security, no rights of data principals and no duties of data fiduciaries will apply in some circumstances, such as when processing data to prevent, investigate, and prosecute crimes. After the intended purpose of processing has been satisfied, the Bill does not mandate that government entities erase personal data. Using the aforementioned exceptions, a government agency may gather information on persons to build a 360-degree profile for monitoring on the grounds of national security. For this, it could make use of information stored by various government agencies. The question of whether these exemptions will pass the proportionality test is brought up by this. In *PUCL vs. Union of India*[1], the Supreme Court required a number of protections for communication interceptions, including (i) demonstrating need, (ii) purpose limitation, and (iii) storage limitation. These are comparable to the duties that data fiduciaries under the Bill, whose applicability has been prohibited.

The Srikrishna Committee in the year 2018 had suggested that responsibilities other than fair and reasonable processing and security precautions should not apply in cases of processing for reasons like as national security and the prevention and prosecution of crimes. It noted that responsibilities like purpose definition and storage restriction, if relevant, would be carried out by a different statute, there is no such legal system in India. Similar exclusions are provided for national security and defence under the 2018 data privacy law that was passed in the United Kingdom. The Secretary of State (i.e., the Home Minister) issues a warrant for such action, which needs previous approval by a Judicial Commissioner. It is necessary to prove the need and proportionality of such activities. Data retention is limited after the warrant's expiration date. Also included in this statute is legislative oversight. The Investigatory Powers Act, of 2016, however, regulates operations such as bulk processing of personal information for intelligence and law enforcement purposes by government entities.

8. **Penalty for violation**- The Schedule of the DPDP Act, provides for a penalty ranging from ten thousand rupees to five hundred Crore Rupees in case of breach by data fiduciaries and non-compliant companies which is also advantageous since it holds companies responsible for leaks. Businesses would be forced to strengthen their systems and implement the appropriate data protection measures by harsh criminal penalties. In the past several years, we have seen a rash of data breaches; from bra sizes to medical and financial details, cyber leaks are only getting worse. After the US, India is the country that is most frequently the target of cyberattacks. Digital corporations will be required to manage residents' data under "absolute legal responsibility," according to the Indian government, providing them a right to protect their data from exploitation.

Comparative analysis of the General Data Protection Regulation (GDPR) and Digital Personal Data Protection (DPDP) Act

The Indian Government has long recognised the need to implement a thorough and dedicated data protection framework that is on par with international norms due to the constantly conflicting need to respect individual privacy and allow data processing by corporate enterprises. One of the most important regulations that establish the precedent for and clarifies the necessity of preserving people's privacy in a globalised society is the General Data Protection Regulation (GDPR). It is the strictest privacy and security regulation in the world. Although it was created and approved by the European Union (EU), it imposes requirements on any organisations that target or gather information about individuals residing in the European Union. The rule becomes effective on May 25, 2018. The GDPR imposes severe fines—up to tens of millions of euros—on those who break its privacy and security criteria. In a time when more individuals are entrusting their data with cloud services and breaches are occurring on a daily basis, Europe is signalling with the GDPR its tough position on data privacy and security. The connection between Indian privacy law and its certain parallels to the GDPR is only reasonable. The similarities between the two laws are discussed below-

(i) Although the GDPR specifically excludes anonymised data from its application, the DPDP argues that it would not apply to data that is anonymized in such a way that it cannot be used to identify a specific person.

(ii) Data processing without consent is authorised under certain conditions. The DPDP outlines a number of "legitimate purposes" for the processing of personal data by data fiduciaries (data controllers) for a number of unique use cases. Such

[1] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.

"legitimate uses" (for which the data subject's consent is not necessary) include processing for employment-related purposes, responding to medical emergencies, carrying out any required legal obligations, or the State offering the data subject any service or benefit, among other things. Similar to this, the GDPR imposes some requirements on the data controller while giving the data controller the option to treat personal data without consent in certain circumstances.

(iii) One of the fundamental tenets under which a data fiduciary or data controller may treat personal data is the consent of the data principal. The fundamental requirements for permission under the DPDP and the GDPR, namely that it be free, specific, and informed, are broadly the same. Furthermore, in order to treat personal data, GDPR and DPDP both demand a legal basis. Another requirement shared by the GDPR and DPDP is that the data fiduciary must show that consent was acquired in accordance with the relevant laws. By mandating that the permission request be presented in a number of languages, at the data principal's choice, DPDP places extra requirements on accessibility.

(iv) Given the criteria used to determine whether a data fiduciary qualifies as a large data fiduciary under the DPDP (such as the amount and sensitivity of the data handled), additional duties like the appointment of data protection officers appear to be compliant with GDPR.

Even if the DPDP and GDPR have many parallels, the DPDP is distinctive in its own position. The distinctiveness of the two regulations has been discussed below in a tabular form-

The table of comparison

S. No.	Basis of Comparison	GDPR	DPDP
(i)	**No division of classes of data**	The GDPR divides personal data into a number of distinct components. These types of personal data must adhere to specific regulations, which also include their intended uses.	However, compliance with the DPDP is not based on the kind of personal data; all types of personal data are subject to the same requirements.
(ii)	**Notice for taking consent**	The notification obligations under GDPR are applicable whenever data is obtained from the data subject and are not just tied to consent.	Only in cases where permission is the justification for data processing does the DPDP require notification to be given (and not for legitimate uses).
(iii)	**Composition of such notice**	The breadth of the information that must be disclosed to a data subject under the GDPR is significantly broader and does not appear to be limited to situations when the data subject's consent is necessary.	The DPDP specifies the components a disclosure must include in order for a data principal to give their permission. These components include details on the type of personal data being collected, the reason it is gathered, how consent may be withdrawn, information about grievance redressal, and details about how a complaint may be filed to an enforcement body.
(iv)	**Monitoring of data related to children**	The GDPR does not specifically forbid behavioural tracking or child-targeted advertising.	DPDP requires verified parental permission or its unequivocal and comprehensive restriction on processing data that is likely to have a negative impact on a child's well-being.
(v)	**Grievance Redressal**	The GDPR does not mandate that a data subject seek remedies from the controller before filing a complaint with the relevant Supervisory Authority or in court.	DPDP mandates an aggrieved person to apply before the Data Protection Board of India.
(vi)	**Transmission of data to other territories**	Under the GDPR, the permissibility of the transfer of personal data ranges from restricted authorisation to transfer under specific conditions to unfettered transferability to a country or an international organisation authorised by an adequacy judgement.	The DPDP gives the Central Government the ability to limit a data fiduciary's transfer of personal information to specified nations or territories outside of India. Personal data can therefore be transferred freely, with the exception of nations that are on the Central Government's forthcoming negative list.
(vii)	**Consent Managers**	No such concept is present in the GDPR.	This is a novel idea in the DPDP. An individual who has registered with the Data Protection Board is known as a "consent manager." This person is responsible for the data principle and serves as a single point of

			contact for the data principal so they may manage their consent through easily accessible platforms. The regulations will specify the duties and other technical, operational, financial, and other requirements that apply to consent managers.

Conclusion

The proactive legislative approach taken by India in the digital sphere is more than simply a precaution; it is a vision for a reliable, secure, and safe digital future. The action strengthens both the rights of its citizens and India's status as a digital maestro. The Government must uphold our commitment to keeping the Internet a safe place for citizens as the role of the Internet in sustainable economic growth expands daily.

The DPDP Act and the laws that followed it provide a hopeful framework for a future in which technology supports mankind rather than subjugates it. To ensure that India's digital journey is both forward-thinking and safe, the Government must work nonstop.

The language of the Act underlines the necessity for enterprises to start comprehending the DPDP Act's contents in order to examine current procedures and policies and decide on the next course of action, even if rules established under the DPDP Act will contain details. It would necessitate dealing with a new set of regulatory obligations for many organisations, such as those not handling sensitive personal data, and hence a longer gestation period to comply.

Critics point out that while the DPDP Act provides businesses and people with clarity on how personal data will be used, there is little information on how it will really be put into practise. Startups are requesting at least a two-year implementation period, although the government has given a 10-month timeline. Contrary to initial expectations, early-stage firms may not be exempt, and if they are, what kind of exemptions will they receive? Startups would require time to assess and improve their infrastructure, and perhaps even to reorganise the collecting and mapping of data while making provisions for data deletion popularly known as right to erasure as well.

Furthermore, there are enough issues being brought up regarding the expansive powers granted to the government. To achieve neutrality, the Data Protection Board (DPB) that will be established must be fiercely independent. The central government would notify and appoint members, along with a chairperson. How impartial can the DPB be when the government holds the selecting reins? And in a highly heated context, is a fair selection process really possible? And who guarantees that the DPB is impartial? The federal government can also limit data transfers to specific nations and freely gather personal and business data. It is being considered as the largest stumbling block because, despite the DPDP Act giving consumers control over data sharing, it provides the government unlimited authority to violate these laws. The DPDP promotes a lack of corporate and individual privacy. In its current form, the Act has the power to stymie the Right to Information (RTI), control publishing platforms, and maybe even snoop on people. While businesses' latitude has been limited to avoid data abuse, the government has granted itself excessive authority by claiming the "interest of the general public." Where are the safeguards against abuse present?

Although the Act is facing backlash from various jurists, at this digital age this step by the government was more of a necessity but the Digital Personal Data Protection Act, 2023 has already inscribed its name in the history. Foreign data protection organisations and governments, including those in Norway, New Zealand, and South Africa, have shown interest in and admiration for the DPDP Act. News media refer to it as a "landmark" policy and state that foreign authorities would closely monitor the law's execution and effectiveness in the days to come. The present version of DPDP succeeds in protecting children's privacy and requiring parental approval for data processing. It will always be remembered as the 'landmark legislation'.