INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 1 [2025] | Page 412 - 422

NAVIGATING INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT: CRITICAL IMPLICATIONS AND EMERGING CHALLENGES

-Bharvi Shahi and Anand Raj Dev[1]

ABSTRACT

The Digital Personal Data Protection (DPDP) Act, 2023, is milestone legislation as it is India's move towards gaining an orderly corpus of law to regulate protection of data and privacy. With the acceleration of digital transactions, data collection, and data processing, having exhaustive regulation was the hour of need. The DPDP Act encompasses the basic principles such as consent-based processing of data principal rights, data fiduciary obligations, rules of cross-border data transfer, and penal fines for default. It is designed to bring India's data protection law at par with international best practices such as that of the European Union's General Data Protection Regulation (GDPR) but in the framework of the country's own socio-economic and security. A central pillar of the Act is empowering data principals (individuals) by providing them with rights of access, rectification, and erasure of their personal data. The Act also places strict obligations upon data fiduciaries (organizations that process personal data) to conduct responsible data processing, security, and accountability. The Act requires explicit consent prior to processing personal data, which enhances individual control of personal information. Moreover, the legislation permits cross-border data transfers to only government-notified countries that could affect that business dependent upon international data processing models. Even though the DPDP Act was meant to be progressive, it has generated much controversy because of its general exemptions in favour of the government and its institutions. The Act authorizes the government to process personal data without consent based on the reasons of "public interest," "national security," and "public order". These provisions have been attacked as inviting state surveillance and undermining individual privacy rights. Besides, unlike the GDPR, which vests regulatory powers in a separate data protection authority, the DPDP Act grants regulatory powers to the government, which is a concern for transparency, accountability, and abuse of power. The DPDP

[1] Students at School of Legal Studies, REVA University, Bengaluru

Act also creates uncertainty about enforcement and judicial supervision. Because some provisions such as definitions of "public interest" and "national security" are poorly drafted, liberal interpretation space is created. Legal uncertainty may lead to differential application and discriminatory enforcement and thus discriminate against individuals and business firms. While the Act is a welcome step toward consolidating India's data protection regime, the key to its success will ultimately rest in effective implementation, regulatory clarity, and enforcement. In order to protect privacy while striking a balance between economic growth and security interests, ensuring an independent oversight authority, more explicit exemption guidelines, and mitigating business concerns will prove critical.

Keywords: DPDP Act, data fiduciary, data principal, public interest, regulatory powers, personal data, consent.

INTRODUCTION

In a global age where digital transactions, online services, and data-based decision-making have become the very fabric of day-to-day life, data protection has emerged as a milestone legal and policy issue. As the Indian digital economy expanded manifold, so has there been an increasing imperative for a sound data protection regime. The Digital Personal Data Protection (DPDP) Act, 2023, is another step along the path of India's protection of personal data and promoting accountability in data processing. The groundbreaking legislation seeks to find a balance between the privacy rights of the individual and the legitimate state and business interests, and invites an orderly march to data governance within one of the world's largest digital economies. The DPDP Act was enacted to deal with the increasing issue of data privacy, security incidents, and abuse of personal data by both government and private bodies. India did not have a robust legal regime focused on protecting personal data, but rather relied on dispersed provisions in the Information Technology (IT) Act, 2000 and guidelines issued by the regulatory authorities. But with the Supreme Court's 2017 judgment in *Justice K.S. Puttaswamy v. Union of India*[2], upholding the right to privacy as a fundamental right, the need for a standalone data protection law became more pressing. Following years of debate, several drafts, and widespread consultations, the DPDP Act was passed to establish a clear framework for the collection, storage, processing, and transfer of personal data within India's legal framework. One of the defining features of the DPDP Act is its focus on consent-driven data processing, in which individuals ("Data Principals") gain control

[2]Justice K.S. Puttaswamy (Retd.), and ANR v. Union of India and ORS, [2017] 10 S.C.R. 569, 2017/ Volume 10

over their own personal information. The Act requires organizations ("Data Fiduciaries") to seek clear user consent before they process the user's data, with the exception of cases involving legal necessity. Along with that, it gives data localization provisions, fines, and establishment of a Data Protection Board for implementation. In being harmonized with international data protection laws, such as the European Union's General Data Protection Regulation (GDPR), the DPDP Act is aimed to promote confidence in India's digital economy while ensuring ethical data-handling practices[3].

Nonetheless, although the DPDP Act is a welcome step, it is not without its challenges. There have been concerns over the sweeping exemptions accorded to the government, which may enable surveillance and access to data without sufficient protection. Further, companies particularly startups and small businesses might struggle with compliance requirements, potentially leading to enhanced regulatory costs. The lack of stringent requirements on data portability and the right to erasure is also questioned if the Act indeed enables people enough in the handling of their digital identities.

IMPLICATIONS OF DIGITAL PERSONAL DATA PROTECTION ACT IN INDIA

The Digital Personal Data Protection (DPDP) Act, 2023 is a path-breaking legislation that seeks to protect the privacy and personal data of individuals in India. In a rapidly digitalizing world, where personal data is being collected by governments, businesses, and technology platforms on a regular basis, this law aims to empower Indian citizens by providing them with more control over their data. While the Act provides robust protection, it is also subject to government exemptions, surveillance threats, and potential restrictions on digital rights. Its influence on citizens is complex, touching upon dimensions of privacy, consumer rights, access to digital services, and government accountability[4]. Another significant aspect of the DPDP Act is that it focuses on data security and data breach notifications. As there have been ongoing cyberattacks and data breaches, Indian citizens have been put at risk for identity theft, financial fraud, and unauthorized disclosure of data. Under the new law, organizations that handle personal data the Data Fiduciaries will have to implement stringent security practices and report data breaches

[3]Latham & Watkins(LLP), India's Digital Personal Data Protection Act 2023 vs. The GDPR: A comparison, Dec. 2023, https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf.

[4]The Digital Personal Data Protection Bill, 2023. Bill No. 113 of 2023.

within a reasonable period of time. This renders it more transparent and accountable, allowing those who are affected to take adequate measures against being victimized by such abuse. The Act thereby becomes an important step towards making digital security more robust and less vulnerable in terms of data abuse[5].

HOW DOES DPDP ACT GIVES STRONGER PROTECTIONS FOR CHILDREN'S DATA?

The Digital Personal Data Protection Act, 2023, has amassed stringent provisions for protecting children's data in India. The rapid growth of technology and online services today also opens children up to a multiple set of risks like unauthorised data collection, behavioural profiling, targeted advertising, and also the risk of being abused over the Internet. Realizing these risks, the DPDP Act has introduced certain provisions to safeguard the privacy and security of children's online interactions. These are mandatory parental consent, prohibitions on targeted advertising, and curbs on tracking and profiling, making it one of the strongest child data protection regimes in India.

One of the most critical components of the DPDP Act is that companies intending to collect or process personal data on children those defined as being under the age of Eighteen must first obtain verifiable parental consent. This ensures that children are not unknowingly broadcasting sensitive information on online forums without adult supervision. Because children, by nature, are not as developed as adults, they are easily prone to being victimized and abused by the misuse of data, so their perspectives about any sharing of personal data may not be very clear to them. For instance, mobile applications, educational sites, social networks ask users for some personal details such as names, ages, locations, and browsing history. Under the DPDP Act, now companies need to put in place mechanisms to verify the personal consent of users before collecting data, thus reducing the risk of unauthorized data collection. This provision is especially important for younger children who might unknowingly give permission that could compromise their privacy[6]. One key protection in the DPDP Act rests in the restrictions put upon excessive data collection and long-term retention of children's data. Organizations are to gather the most minimal data necessary for the rendering of their services and delete such data once it is no longer

[5] Anirudh Burman, Understanding India's New Data Protection Law, (Oct. 3, 2023) Carnegie Endowment for International Peace, https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en/

[6]Digital Personal Data Protection Act, 2023, section 9.

needed. This avoids the storage of delicate private data for an indefinite period and possible use for unscrupulous, practical reasons in the future. For example, an online learning platform gathers personal data about students in order to register for courses, but does not permit that data to be kept indefinitely or shared for any reason other than original intentions. Moreover, if a child no longer uses the service, the organization should delete the data involved to curb future misuse. By doing this, this would greatly reduce the possibility for breaches of children's data and any unauthorized sharing of children's personal information. For example, take a 12-year-old boy named Aarav, who watches educational videos and plays video games on a favourite streaming site. Previously, the sites tracked his history, constructed individual data, and used it to display extremely tailored advertisements for gaming accessories and in-game items. This established more than indulgence in the purchases of in-game features and increased reliance on digital content. With the DPDP Act in place, the website is now required to take explicit consent from parents prior to collecting Aarav's information. The website is also unable to track what he watched and display him targeted advertisements based on his activities. If his parents wish, the website is also mandated to make all the information it collects on Aarav available and destroy it upon request. This makes Aarav's internet life secure and devoid of deceptive advertising tactics.

IMPLICATION OF THE DPDP ACT ON BUSINESS AND ORGANIZATIONS

The Digital Personal Data Protection (DPDP) Act, 2023 lays down a complete legal framework for data privacy in India having far-reaching implications for all businesses and organizations collecting, processing, and storing personal data. The act calls for new duty, compliance burden, and potential fines on Indian businesses in the digital space. While the Act aims to enhance data security and build consumer confidence, it also imposes strict regulatory obligations on companies, forcing them to rethink their data handling processes. The Act applies to all organizations that process digital personal data in India and even overseas companies handling Indian citizens' data, thereby broadening its scope. One of the most direct implications of the DPDP Act is the legal requirement to observe data protection principles, with companies compelled to process personal data fairly, lawfully, and transparently. Companies are also responsible for ensuring that data gathering is aimed at a particular purpose for which authorization was provided and that Data Principals have rights to access, rectify, and delete their own personal data. This requires building strong data governance processes among companies, which requires higher investments in compliance infrastructure, legal advice, and technical security

controls. Non-compliance will attract significant penalties, up to ₹250 crore per violation, and thus non-compliance risk will be expensive[7].Another significant implication is the need for explicit user consent[8] prior to processing their data. In contrast to the earlier regulations, where companies could harvest personal data with implied or vague consent, the DPDP Act necessitates an affirmative and clear action on the part of users to authorize data collection. This implies that companies need to re-engineer their user interfaces to facilitate open and informed consent processes. For instance, online commerce websites, finance companies, and apps are required to give notices with simplified consents, being clear about what data will be processed and saved. Organizations need to also introduce a system enabling withdrawal of consent anytime, adding further complexity for organizations that engage in long-term data storage from users for business analysis, promotions, and quality of service improvements.

Additionally, the Act dissuades cross-border data transfers by mandating organizations to ensure that the transfer of personal data is in accordance with government-approved protection protocols. This is especially true for multinational companies, information and communications technology firms, and cloud computing firms, as they will be forced to restructure their data storage and processing frameworks to meet local requirements. For example, an overseas social networking website or a financial technology company handling the data of Indian customers may be compelled to establish domestic data centres or enter into government-approved data transfer agreements in a bid to sustain their operations in India. This would thus lead to increased operating costs and discourage foreign organizations from engaging in trade in the Indian market. While many matters are entailed in adherence to legal obligations, the DPDP Act presents an opportunity for businesses to establish customer trust and differentiate themselves by being data protection ready. Businesses that make a genuine effort to possess good privacy policies, good cyber security measures, and ethical data handling practices will be better off, remembering that consumers increasingly care about data security and privacy when they consume digital goods and services. Additionally, organizations that respect customer privacy are likely to enjoy more loyal customers and improve brand reputation, therefore making data protection law compliance a business asset.

[7]Philip L. Gordon, Morgan J.Matson, Isha Malhotra, Ellie McPike, and Urvashi Morolia, Implication of India's protection law for US Multinational Employees, (Aug. 24, 2023), https://www.littler.com/publication-press/publication/implications-indias-new-data-protection-law-us-multinational-employers

[8] George Lawton, Digital Personal Data Protection, Act, 2023, definitions, Tech Targets, (May, 2024), https://www.techtarget.com/searchdatabackup/definition/Digital-Personal-Data-Protection-Act-2023.

ROLE OF GOVERNMENT UNDER DPDP ACT

The Digital Personal Data Protection (DPDP) Act of 2023 is a comprehensive body of data protection law for India, augmenting the ability of the government to regulate, oversee, and enforce data privacy legislation. The overarching role of the government in enforcing the Act is to ensure compliance with its provisions and reconcile the goals of data protection with the imperatives of economic growth and national security. In various provisions, it takes charge of regulating data fiduciaries, overseeing enforcement, and protecting citizens' rights while reserving important discretionary powers for certain exemptions and interventions. One of the key functions of the government under the Data Protection and Digital Privacy (DPDP) Act is to frame and regulate the Data Protection Board of India (DPBI). The DPBI is an adjudicatory board tasked with processing complaints, reviewing cases of data leaks, and levying penalties on organizations that fail to adhere to established rules. The board will be an independent entity tasked with ensuring public and private sector institutions adhere to data protection norms. The government also has the discretion of appointing members to the DPBI, establishing running guidelines for the board, and establishing the norms for conflict resolutions. While the framework tries to establish a complete enforcement system, there have been questions raised regarding how government control can undermine the independence of the board.

In addition, the government maintains significant control over the entities and companies under the DPDP Act. The government has the authority to classify certain entities as Significant Data Fiduciaries (SDFs)[9] based on the type and amount of data they handle. The organizations need to maintain high levels of compliance, for example, mandatory appointment of Data Protection Officers (DPOs)[10], routine audits, and application of impact assessments. Government intervention in the classification process makes sure that organizations handling lots of sensitive personal data maintain high standards so as to prevent misuse or unauthorized use. The government may have the power to grant exemptions to specific entities from compliance with some provisions of the Act if duly justified for example, the government authorities processing personal data for national security, law enforcement, or public interest grounds may grant themselves an exemption from certain provisions of the Act-these may include, but are not limited to, obtaining user consent for processing data. They were aimed at promoting national security operations, crime prevention, and emergency response mechanisms, but critics argue that these

[9]Digital Personal Data Protection Act, 2023, section 8(4).
[10]Digital Personal Data Protection Act, 2023, section 8(5).

exemptions could lead to possible violations of individual privacy and government overreach. If exemptions were to be permitted, then transparency and oversight mechanisms would take on a critical and pivotal role in preventing misuses for mass surveillance or unauthorized data collection[11].

CHALLENGES FACED BY DPDP ACT

The Digital Personal Data Protection (DPDP) Act, 2023, while introducing a robust data privacy regime in India, is marred with a series of implementation and enforcement issues. These encompass the challenges relating to ambiguity of compliance requirements, overreach of the government, inconsistency with international data protection principles, and practical challenges for firms and individuals. Several provisions of the Act have proven controversial and have been criticized, with concerns over how well it can weigh business interests, privacy rights, and national security. The strongest challenge is the blanket exemptions for the government under Section 18 of the DPDP Act. This section provides the central government with an opportunity to exempt any government organization from compliance on grounds of national security, public order, and crime prevention. Although this provision seeks to allow police and intelligence agencies to act without excessive obstruction, critics consider it inadequate to prevent the abuse of authority. It also risks mass surveillance and data collection with little or no oversight, infringing privacy and possibly breaching constitutional mandates under Article 21 of the Indian Constitution protecting the right to privacy.

Another grave concern is the lack of an independent data protection authority. The DPDP Act establishes the Data Protection Board of India (DPBI) under Section 19, but this board is government-appointed and government-controlled, and hence issues regarding its independence remain. Unlike the European Union's General Data Protection Regulation, which has independent data protection authorities, the DPDP Act's lack of autonomy in enforcement can lead to discriminatory judgments, selective enforcement, and lack of transparency in the resolution of data-related disputes. In the absence of an independent mechanism of oversight, individuals and companies might find it difficult to approach an impartial redressal for data privacy infringement. The Act is also challenging for implementation by enterprises, particularly start-ups and small organizations. Under Section 8 of the DPDP Act, strict consent-based processing of

[11]Anirudh Burman, Understanding India's New Data Protection Law, (Oct. 3, 2023) Carnegie Endowment for International Peace, https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en

data is required for businesses to ensure that they take clear, informed, and express consent from users prior to personal data collection. Although this requirement enhances user rights, it adds compliance challenges to smaller organizations as they do not have the requisite legal and technical capabilities to implement these requirements. The fees of hiring Data Protection Officers (DPOs), performing compliance audits, and safe data storage can be exorbitant, thus placing the startups and MSMEs (Micro, Small, and Medium Enterprises) under a strain in following the law. In addition, the cross-border data transfer provisions of the Act (Section 16) are a cause of concern for multinational companies. The Act empowers the government to designate countries to and from which data can or cannot be transferred but does not offer a clear system for determining these restrictions. This ambiguity poses challenges for cross-border businesses operating on cloud-based services and cross-border processing of data. Cross-border businesses may be faced with India's data localization policy and other global data protection laws, like the GDPR and the US CLOUD Act, as being conflicting. This ambiguity discourages global investment and prevents global operation, isolating India from global digital trade.

The second issue is the absence of obligatory aggressive data breach notice provisions. As opposed to the GDPR where an organization is required to give notice of a data breach to be filed within 72 hours, Section 20 of the DPDP Act grants the Data Protection Board general latitude on timelines for notice of breaches. This absence of a proper notification process will result in delayed response to cyber- attacks, loss of control and vulnerability to identity theft, fraud, and loss of financial assets. With the increased rate of cyberattacks and data breaches in India, the absence of specific timelines makes the Act ineffective in safeguarding personal dated Act also questions processing of children data under Section 10. Whereas the Act makes tracking, behaviour tracking, and targeted advertising impermissible for children, the child's age remains static at less than 18 years. The international standards like the GDPR prefer differential age intervals (e.g., 13 years or 16 years) based on data processing nature. The outright prohibition on processing children's data with parental consent prevents edtech platforms, social media platforms, and online service providers from effectively functioning. The provision, several experts say, does not consider teenagers' ability to make sound judgments and may limit access to beneficial digital services. Sanctions and enforcement are another hindrance, as offered by Section 25 of the Act. The fine for defaulting can go up to ₹250 crore and could be discouraging to large firms' non-compliance. But the law does not speak clearly about enforcement of lesser offences, and it is this which may result in selective penalties and asymmetrical trends of enforcement. Companies will exploit loopholes if fines are not uniformly enforced and make a mockery of the law, which in turn makes it ineffective.

Another concern is the absence of sector-specific provisions for new technologies, including blockchain, big data analytics, and the Internet of Things (IoT). These technologies entail decentralized processing of data, automated decision-making, and widespread data harvesting, which do not fit the model of consent-based data protection under the DPDP Act. Without sectoral regulation, companies working in these new industries may not be able to meet the requirements of the Act, which would lead to legal loopholes and operational inefficiencies. Lastly, public awareness and digital literacy are still gigantic issues in the success of the Act. Indian users are still not aware of their data protection rights and how to exercise them. Section 23 of the DPDP Act focuses on the government's initiative for organizing awareness campaigns, but with no solid strategy, it is possible that millions of users of the digital space, especially in rural communities, might still fall prey to abuse of data and fraud. Without large-scale education programs, the usefulness of the Act in enabling people to master their data is doubtful.

CONCLUSION

The Digital Personal Data Protection (DPDP) Act, 2023 is a step towards the establishment of an umbrella data protection regime in India which aims to find a balance between privacy rights of individuals, commercial interests, and national security. While the Act introduces several futuristic steps, it also throws up challenges and issues that must be clarified to ensure proper enforcement. The Act provides more powerful rights to citizens, such that they have greater control over their personal information through informed consent, the right of access, correction, and grievance redressal arrangements. Also prominent is protection of children's data, blocking tracking, behavioural monitoring, and targeted advertising, though the strict definition of minors as users below 18 years old has raised concerns about its effect on teen users and digital services designed for them.

For companies and organizations, the DPDP Act imposes stringent compliance requirements on them to maintain strong data processing systems, be transparent, and have security measures in place to avoid breaches. While this imposes greater accountability, it also imposes the financial and administrative cost on smaller firms and startups that cannot afford to adhere to stringent data protection practices. Additionally, the cross-border data transfer provisions remain ambiguous, creating uncertainties to multinational corporations and potential inconsistencies with international regulations such as the GDPR. The harsh non-compliance penalties, as important as they are for the enforcement of data protection norms, are questioned on their disproportionate impact on small businesses that may not be in a position to respond to compliance measures. The

government's role under the Act is controversial and pivotal. While the Act requires government agencies to comply with data protection principles, it also grants blanket exemptions to state agencies in some areas on the basis of national security, public order, and crime prevention. The absence of independent supervision, as with the Data Protection Board of India (DPBI) being under government control, is a source of concern for biased enforcement, selective application, and misuse of data by the state. In addition, public awareness and digital literacy are also major issues, as most people are not familiar with their rights under the DPDP Act, which hinders its effectiveness in empowering users to safeguard their personal data. But another sector of utmost concern is the convergence of the Act with new and upcoming technologies like artificial intelligence, blockchain, and big data analytics. The DPDP Act does not touch upon algorithmic decision-making, AI-driven processing of information, and automated profiling, and there are gaps in making digital platforms and enterprises using AI technologies accountable. Lacking explicit guidelines on AI bias, transparency, and ethical use of data, there is also the possibility of individuals being discriminated against in employment, credit allocation, and medical treatment decisions, which would defeat the very essence of data protection. Equally unclear are data breach notice provisions under the Act, which do not have a strict reporting deadline like the 72-hour requirement of the GDPR, and so can slow responses to cyber threats and decrease transparency in case of mass-data breaches.

Nonetheless, to ensure maximum effectiveness of the DPDP Act, some crucial improvements must be made towards greater independence of the regulator, stipulating guidelines for cross-border data flows, improving the regulation of AI, and better flexibility in processing data for businesses. The government also needs to take the time and resources to engage in a far-reaching public campaign of digital literacy and capacity-building in regulation to achieve compliance and understanding among people on a massive scale. Calling The DPDP Act, 2023, landmark is to raise a sturdy flower on a very tender implement of compliance, both in assurances for business sustainability and in the relishing of people with it while carefully avoiding crossing into unreasonable enforcement and, thus, into violations of privacy. With further tuning and collective efforts by all the involved stakeholder groups-the government, the industry, and civil society-the Act can shape a bright future for the digital economy in India, with individual privacy protection and the restoration of faith in the digital ecosystem.