Digital Personal Data Protection Act, 2023: A Critical Analysis

Samreen Ahmed[1] and Dr. Mohammad Nasir[2]

ARTICLE HISTORY
Received on: 06/05/2025
Revised on: 12/06/2025
Accepted on: 05/07/2025

ABSTRACT

India's first cross sectoral law on privacy—The Digital Personal Data Protection Act, 2023 (DPDPA), was anticipated to create a robust legal architecture for data protection. It is the culmination of numerous iterations, expert committee recommendations and was enacted in the backdrop of Apex Court's recognition of the right to privacy as a fundamental right under Article 21 of the India Constitution, with right to informational privacy as its subset. However, the legislation in its final shape as it stands today law has restricted its protective ambit to the personal data only, overlooking the broader aspects of data protection. This paper critically reviews the DPDPA, 2023 and the proposed Rules, highlighting the grey areas and their implications for individuals and business entities. It argues that beneath the rights this law is projected to protect lies a labyrinth of leaking valves, exposing its inherent weakness. The Act falls short on multiple fronts, including its limited scope, excessive exemptions to the government, and failure to provide exhaustive protective measures. By adopting a narrow approach to privacy, the Act overlooks the challenges posed by the evolving digital landscape. This paper critically reviews the privacy regime of India, specifically in the context of the DPDPA and the Rules framed thereunder.

Keywords: *Data Privacy, Digital Personal Data Protection Act, Personal Data Protection, Privacy Breach, Privacy Regime.*

INTRODUCTION

The Digital Personal Data Protection Act, 2023 (DPDPA), marked a watershed moment in the trajectory of privacy law in India. It is the first ever cross-sectoral law on personal data protection. It had a gestation period of approximately half a decade to be in the shape as it stands today, albeit

[1]ICSSR Doctoral Fellow, Department of Law, Aligarh Muslim University, Aligarh.
[2]Assistant Professor, Department of Law, Aligarh Muslim University, Aligarh.

unenforced. It is believed to be an outcome of the Apex Court's directive to the Union government to formulate "a carefully structured regime" for protecting individuals from the privacy harms from state and non-state actors. The court in *Puttaswamy* (2017) observed, "*Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state.*" The DPDPA signifies a shift in law and policy towards institutionalising privacy as fundamental right, even when it awaits enforcement.

The judgment cemented the right to privacy (RTP) in India by recognising it as a fundamental right protected under article 21 of the Indian Constitution and right of informational privacy as its subset. The court lad down three conditions that should be fulfilled by any incursion of privacy, namely, legality i.e., a legislative mandate, legitimate state aim, and proportionality (Kanwar & Manish, 2023). Taking this as the vantage point, the paper critically reviews the privacy regime envisioned for India under the DPDPA and the Rules framed thereunder.

METHODOLOGY

This study traces the origin and evolution of the data protection law in India employing the doctrinal method. The pre-legislative developments that propelled the law making (DPDP Act) were analysed to determine whether the provisions of the enacted law and their underlying legislative intent withstand the anvil of the RTP in the digitalised world. Other than weighing against the principles of "purpose limitation" and "data minimisation," the paper also analyses the implications of removing the distinction between sensitive and non-sensitive personal data, and the repeal of Section 43A of the Information Technology Act, 2000, to assess whether the new regime is responsive to the challenges of a digital and data-driven society.

THE TRAJECTORY OF THE MAKING OF PRIVACY LAW IN INDIA

Prior to 2017 judgment, various attempts were made to enact a comprehensive privacy law for India. In 2006 the "Personal Data Protection Bill" was introduced in the Parliament. It had a limited scope confined to

the protection, use and disclosure of personal data. It kindled debates on the concerns pertaining to the personal data: misuse, unauthorised sale and use for business purposes.

The Information Technology Act, 2000 was already in existence dealing with matters pertaining to digital transactions and data, when attempts at a separate data protection legislation were made. Subsequently, the Information Technology Act, 2000 (IT Act) was amended without any debates in the Parliament. However, later some provisions inserted by the Amendment were struck down and held as unconstitutional by the Apex Court. Section 43A (compensation for failure to protect data) was also inserted by this Amendment. It marked the first concrete step towards statutory protection of data. It mandates body corporates dealing with data to adopt reasonable security measures (Kessler, Ross, & Hickok, 2014).

In 2010, approximately two years later, an "Approach Paper for a Legislation on Privacy" was published on the website of the Department of Personnel and Training (DoPT). Drafted by group of privacy experts, the paper aimed to furnish a "*conceptual framework that could serve the country's balance of interests and concern on privacy, data protection, and security...*" It reviewed laws pertaining to privacy prevailing in thirteen jurisdictions and gave recommendations for India's privacy regime (Rahul Matthan & Group of Officers, 2010), primarily focusing on data protection. The document defines privacy (for the paper's purpose) as "the expectation that confidential personal information disclosed by any individual to Government or non-Government entity should not be disclosed to third parties without consent of the person and sufficient safeguards need to be adopted while processing and storing the information." Significant observations include:

1. In India we do not have a culture of privacy.
2. An increasing trend of centralization of governmental databases.
3. Privacy concerns emanating from the Unique Identification project.
4. Increasing collection of personal data by private sector entities.
5. India's approach to privacy regulation was kind of 'hybrid' a mix of statutes and soft laws.

The following year (2011) witnessed four significant developments in this regard. A Press Information Bureau release stated that the government proposed to bring a law for protecting against breach of individual's privacy by unlawful means. Secondly, newspapers reported that in the aftermath of

the Niira Radia Tape controversy, the Government of India drafted 'Right to Privacy Bill, 2011' with the objective of creating a statutory right to privacy. However, owing to the internal disagreements between the stakeholder Ministries, the Bill could not see the light of the day. The DoIT through the Official Gazette published the IT Rules, 2011. These Rules incorporate some principles of the OECD Guidelines, albeit to an extent only. They include "collection limitation, purpose specification, use limitation and individual participation". In the latter part of the year, the Planning Commission of India (now NITI Ayog) constituted an Expert Group (chaired by Justice AP Shah) to study the privacy legal regimes in various jurisdictions and to examine their relevant policies.

The Group submitted its Report in 2012, comprehensively analysing the SPDP Rules, 2011. The Report outlined nine "National Privacy Principles" which were to be applied across all sectors for harmonizing law and policy. These principles were proposed to be adhered by all data controllers and any person aggrieved by non-compliance was to be provided an adequate remedy. The Report also identified key features for a model privacy law: "(i) technological neutrality and interoperability with international standards, (ii) multi-dimensional privacy, (iii) horizontal applicability, (iv) conformity with privacy principles, and (v) co-regulatory enforcement regime." Notably, some recommendations of the Report were included in the then proposed Draft Privacy Bill.

Years later in 2017, MeitY constituted (Srikrishna, Sundarajan, Pandey, Kumar, Moona, Rai & Krishnen, 2018) Committee to "examine issues related to data protection, recommend methods to address them, and draft a data protection Bill". Based on the recommendations (although partially) of the Committee, the Personal Data Protection Bill, 2019 was introduced in the Parliament. However, it was sent to the Joint Parliamentary Committee (JPC) which after extensive consultative process of over 2 years and clause by clause examination of the proposed law released its report in 2021. In midst of it, in July 2020, (Gopalakrishnan, Ghosh, Verma, Katragadda, Kumaraguru, Singh, Narayanan, Dayasindhu & Matthan, 2020) Committee of Experts released its report on the Non-Personal Data Governance Framework.

The revised report of the JPC (November 2021) proposed 81 amendments to the original Bill and recommended significant expansion of the scope of law—protect both personal and non-personal data. Set to be tabled in the budget session of 2022, the draft Bill garnered much criticism from

stakeholders, especially, business, as unreasonably inclined towards the interests of the State. Thus, the Bill was withdrawn from the Parliament in August 2022. In the thick of the uncertainties around the data protection law, the MeitY in February (2022) released the Draft India Data Accessibility and Usage Policy, with the objective of capitalising the value of public sector data. The primary objective of this Policy was to recognise open data—defined as a dataset that is freely accessible for use, reuse, and redistribution by anybody, as a valuable public resource and to address the current barrier in data accessibility. In November 2022, MeitY published the Draft Bill for public consultation. Approximately a year later in August 2023, the DPDP Bill was passed by the Parliament. However, the enacted law has stark differences from the version of the Bill released for public consultation.

Notably, a cursory glance at the trajectory of the development of privacy legislation in India, at various junctures, appear to suggest that India requires only robust data protection law, while at other instances, there appears a necessity for a more comprehensive law recognising the RTP.

DISCUSSION

"The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data", reads a paragraph in the preface to the (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2002). It aptly underscores the ubiquitousness of processing of personal data in private and public sectors, the complexities of cross-border data transfers, propelled by the rampant digitalisation of the economy and emphasises on the need for a protective legal architecture. Data inherently possesses value, which is further enhanced when shared, resulting in the creation of substantial efficiency. The contemporary digital environment is characterized by the fact that almost every task undertaken by a person involves data transaction of one kind or the other. The IoT is credited to have ushered new entities in the market industry: entities dealing with data—processing, collecting and/or processing personal data as an integral element of their business model. For instance, the Indian Supreme Court also noted that many companies outsourcing services and operating online are all dependent on data. "'Uber', the world's largest taxi company, owns no vehicles. 'Facebook', the world's most popular media owner, creates no

content. 'Alibaba', the most valuable retailer, has no inventory and 'Airbnb', the world's largest accommodation provider, owns no real estate", the court noted in *Puttaswamy* (2017) judgement. Nonetheless, all these companies deal with personal data as part of their B to B and B to C transactions. These global trends find sharp resonance in India, where demographic and technological shifts have significantly expanded the scale and complexity of data generation and use.

The estimated population in India was approximately 1.43 billion in 2023. This figure is expected rise to 1.5 billion by 2029 (United Nations, 2024). Notably, the median age in India was 27 years old in 2020 making India a vast reservoir of youth population—contributing to proliferation of smartphones, social media and e-commerce. The (Ericsson, 2024) Mobility Report estimates that India's mobile traffic data will reach approximately 264 exabytes annually by 2025. In 2017, India had around 340 million users, surpassing the USA, which had 223 million users. By 2040, the users of smartphone are anticipated to reach approximately 1.55 billion (Statista, 2023). With increasing technological proliferation more data will become vulnerable to breach. Given this exponential growth in data and its vulnerabilities, it becomes essential to scrutinize the adequacy of India's current legal framework, particularly the DPDPA. This paper seeks to outline the grey areas of DPDPA highlighting their potential consequences for individuals and businesses.

The Act regulates collecting, storing, processing, and transferring individuals' personal data within the digital landscape. It is asserted to have been drafted with the backdrop of the Indian aims and aspirations. Nevertheless, it has raised many eyebrows. (BS Web Team, 2023) reported, "Experts have noted a "sense of panic" among companies concerning the timelines stipulated by the legislation." *The Economic Times* reported that even big tech companies are grappling with and facing severe challenges in ensuring compliance under the new law (Indo Asian News Service, 2023). (Bal & Kashyap, 2024) suggest that approximately 85% of data fiduciaries had begun preliminary deliberations on compliance, which was marred by the absentia of DPDP Rules which were expected to constitute the very substance for various provisions' implementation. The notification of the draft Rules in January 2025 came a sigh of relief for them, albeit short-lived.

The draft Rules aim to provide guidance on the operationalisation of the parent Act, breathing life and spirit into the recurrently used phrase 'as may

be prescribed' in the Act (26 times). It's being hailed as a landmark in India's data governance regime, though underneath its projected intentions lay a labyrinth of provisions requiring closer examination.

EXCESSIVE BURDEN ON DATA FIDUCIARIES

This Act applies to data fiduciaries[1] and those entities "who collect or process data for various reasons including, amongst others, financial, social security benefits, medical records, insurance claims" (Nidumuri and Shetty, 2020). Companies having trans-national operations were complying with international principles of data protection with the DPDPA law in force, they'll have to identify the solution for navigating complexities arising from the conflicting provisions of the two law.

The Act mandates data fiduciaries to ensure the correctness of data, thus these entities shall now have to cautiously safeguard the personal data of individuals even when it is in the hands of third parties they hire (outsourcing). A herculean task would be safeguarding data available with the companies or shared by them prior to the enactment of the DPDPA. To ascertain and document 'why' and 'how' the data was obtained, the 'duration' for which it has to be retained, who has 'access' to such data and trace 'third parties' who may have become privy to such data would be difficult.

INTIMATING DATA BREACH TO THE DATA PROTECTION BOARD

Section 7(2)[2] of the Act requires the data fiduciaries (DF) to report to

1 Section 2(i) of the DPDP Act reads as "Data Fiduciary means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data."

2 Section 7(2) of the DPDP Act, 2023 provides that "on becoming aware of any personal data breach, the Data Fiduciary shall intimate to the Board, —

(a) without delay, a description of the breach, including its nature, extent, timing and location of occurrence and the likely impact";

(b) "within seventy-two hours of becoming aware of the same, or within such longer period as the Board may allow on a request made in writing in this behalf,"—

(i) updated and detailed information in respect of such description;

(ii) the broad facts related to the events, circumstances and reasons leading to the breach;

(iii) measures implemented or proposed, if any, to mitigate risk;

(iv) any findings regarding the person who caused the breach;

(v) remedial measures taken to prevent recurrence of such breach; and

the Data Protection Board (DPB) within 72 hours (except when the DPB extends time on DF's written request) all actions that they have undertaken and mitigate the risk posed by breach and the remedial measures undertaken to prevent recurrence. Although a welcome step, it is practically impossible for the data fiduciaries to gather much information within the given time-frame.

OPENINGS IN THE PROTECTIVE VALVE

Noting down online available data on paper makes it offline, as the processing will be non-automated, making it beyond the remit of the DPDPA. The Act also does not include in its ambit processing of data by individuals for domestic or personal purposes.

Exacerbating the situation further, the 2023 Act ignores the recommendation of the JPC to omit the definition 'harm' which was present in the prior iteration, i.e., PDP Bill, 2019, as including "(i) mental injury, (ii) identity theft, (iii) financial loss, (iv) reputational loss, (v) discriminatory treatment, and (vi) observation or surveillance not reasonably expected by the data principal". The Bill mandated data fiduciaries to take steps to mitigate such harms but the enacted law omits such a mandate, thereby negatively impacts companies dealing with data.

'PERSONA' AND 'DIGITAL' ONLY

In reading the RTP as a penumbra right under Article 21, the Apex Court did not outline the ambit of the right or ascertain its applicability to only a particular kind of data. Unlike European Union's GDPR, the DPDPA does not extends its protective cover to the non-personal data, non-digital personal data and anonymised data.

The Preamble of the Act explicitly mentions 'personal digital data', indicating the ambit and scope of the law are confined to 'personal' data, which is digitized. A cursory glance clarifies that the law presumes that the risks of breach of privacy exist only in the processing of personal data—data which identifies an individual (Section 2(t)). The fallacy lies in the assumption that only personal data has the potential to identify an individual. The anonymised data can be de-anonymised and may be combined with personal data to make specific inferences about individuals. The Act could have included a provision imposing pecuniary penalties on data-processing entities indulging in deanonymization or reidentification of anonymized data.

(vi) a report regarding the intimations given to affected Data Principals."

REASONABLE SECURITY SAFEGUARDS

Crucial aspects like 'obfuscation' and 'masking' have been overlooked by the legislators. They are not defined in the Act. Absence of definition makes implementation mechanism ambiguous and gives much discretion to the data fiduciaries, thereby increasing the risk of data breaches.

EMPLOYEE PRIVACY

Employees' control over the data and information their employer gathers and processes about them is known as informational privacy in the workplace. This includes handling personally identifiable information gathered from tools, technologies, and equipment used in the value-creation process, hiring and employee management. Employee's control over their employment directly affects their "rights" and "protections" (Wang & Bai, 2024). Often, the organization's business objectives and the employee's right to privacy are at odds. The law ought to perform the task of balancing out.

The Act places employers under a statutory duty to safeguard data by earmarking them as data fiduciaries, but distressing is section 7(i), which permits non-consensual processing of employee's data for legitimate purposes including 'purposes necessary for employment'. A purpose is deemed legitimate merely by being related to employment. The open-ended phrasing of this provision, creating room for arbitrary use and exploitation. The purposes should have been illustrated as a list considering the sensitivity of the data. The Act nowhere clarifies or defines 'relatedness' as to what kind of relatedness with employment will attract exemption under this subsection. The examples of purposes listed in sub-section (i) include, "*corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit*." These purposes pertain to the requirement of legal confidentiality and the corporation's intellectual property rights. (Ravindran, Panda & Jauhar, 2023) argue that these purposes could be taken as valid grounds for prosecution of a person in case of violation of statutory or contractual rules on confidentiality but cannot serve as valid grounds for violation an individual's privacy. Hence, the purposes pertaining to confidentiality and IPRs should be deleted. Arguably, closed list that does not include these purposes would have been appropriate.

For safeguarding data, non-consensual processing should be sparingly allowed, restricted only to cases where obtaining an employee's consent is not feasible or appropriate. The Act should furnish data principal, the choice to opt out of such processing. Arguably, the bargaining power disparity between

employers and employees warrants legal protections for the less advantaged, i.e. employees. For instance, an airline stewardess may be asked to furnish her children's and her parents' personal details. Children's data can be taken for legitimate use for employment benefits, but collecting parents' data by the airline does not appear legitimate, where they are not dependants. To avoid the risk of losing job, the stewardess will furnish her parents' personal data.

Similarly, the group companies inevitably share data amongst their constituent companies. The shared data often includes the relevant employee data for salary standardization. The company should have a legitimate interest in sharing such data; otherwise, it can attract implications under the Act (Guha and Tiwari, 2022).

Another instance could spur from the mandatory submission of PAN and Aadhaar number by employees for inclusion in the payroll with the employer and social security schemes in India. The employers often outsource services and share personal data with private agencies and organizations. This sharing of personal data must be in compliance of the guidelines laid down by the Apex Court in (***Puttaswamy* 2019)**. These guidelines are in form a check and balance mechanism to minimise the sharing and processing of such sensitive information. Given the open-ended exception under the DPDPA, the employer may claim that the data sharing with a third party is within the purview of employment purposes. Although, the third-party partners are crucial in a business ecosystem but they pose significant challenges to a reliable, secure, and strong digital future. Statistics suggest data mishandling, (World Economic Forum & Accenture, 2024) found in a scrutiny of 49 countries, including India that 41% of the firms experienced a significant breach in the previous 12 months; uniformly, a third party was believed to have caused it.

Notably, with reference to the non-consensual processing for the purposes of employment, the Srikrishna Committee had also suggested that it should be confined to cases where giving consent requires unreasonable efforts on the apart of the employer.

GOVERNMENT EXEMPTIONS

The SC in ***Puttaswamy*** (2017) held that "any infringement of the right to privacy should be proportionate to the need for such interference." Nonetheless, the Act extends pervasive powers to the union government, including the power to exempt itself from the remit of certain provisions for the purposes mentioned under section 17(2). Such sweeping exemptions to the State concerning data processing can potentially violate the fundamental

RTP of an individual. Also, the law does not enumerate the time limit or any procedural safeguard, in this context. The State may access and process personal data and retain it for a period longer than required. Further, under the Constitutional scheme of fundamental rights 'State' (Article 12) includes "(i) central government, (ii) state government, (iii) local bodies, and (iv) authorities and companies set up by the government". Fairness demands that such exemptions do not extent to entities other than those specified under Article 12. The DPDPA however, allows exemptions to be extended to any agency designated by the Central government. A member of the Pratap Jadhav chaired Standing Committee had given dissenting note on this provision. Nevertheless, the provision was retained in the Act.

Another crucial aspect is that the rights extended to the data principles[1] under the Act and the obligations imposed on the data fiduciaries fall flat during investigation, prevention or prosecution for offences. This is in violation of the constitutionally protected right against self-incrimination under Article 20(3). Moreover, the government agencies are not mandated to erase people's personal data on fulfillment of the required purpose—this impinges on the right to be forgotten. Under the guise of surveillance or investigation, state agencies can develop and collect the 360-degree profile of any individual—raising a serious question—whether the exemptions extended by the Act meet the proportionality test. Surprisingly, Act turned a deaf ear to the recommendations of the (Srikrishna et al., 2018) that "in case of processing on grounds such as national security and prevention and prosecution of offences, obligations other than fair and reasonable processing and security safeguards should not apply".

The DPDPA is modelled on the EU's GDPR, which provides similar national security and defense exemptions. However, the EU law has a check and balance mechanism, unlike the Indian law. For instance, under the UK Investigatory Powers Act of 2016 the processing of personal datasets in bulk by government agencies for either intelligence or/and law enforcement activities is preceded by a warrant by the Secretary of State (counterpart of Minister of Home Affairs in India) with a-priori approval of a Judicial Commissioner. Absence of mechanisms to meet markers of necessity and proportionality in Indian law is a classic case of sheer parliamentary oversight.

Whether an individual's right to data erasure will have precedence over

1 Under Section 2(j) of the Act, 'data principal' is defined as "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."

the data retention requirement of the government, is left answered by the Act.

FREE AND INFORMED CONSENT

The Act prescribes obtaining 'consent' from the data principal for processing of their personal data; it omits to prescribe the mode or mechanism for obtaining such consent or any safeguards as such. The draft Rules however, have specified that the consent seeking notice should include the list of purposes and the notice should be drafted in a simple and understandable language. The said notice must necessarily mention the details that are necessary for enabling the data principal to furnish informed consent. The Rules outline the information that should be furnished in the notice—

(i) an itemised description of such personal data; and
(ii) the specified purpose of, and an itemised description of the goods or services to be provided or uses to be enabled by, such processing;

However, as a general practise, data fiduciaries/processors obtain the consent primarily through online shrink-wrap or click-wrap agreements. (Kumar, 2022) highlights the problem with these agreements, as entities collecting the data are not under the obligation to explain the implications of data processing to the data principal giving consent. Tested on the anvil of Section 15 of the Indian Contract Act 1872, such consent may not be considered as "free" and thus, may be perceived as vitiated. Moreover, shrink-wrap agreements are modelled on the take-it-or-leave-it policy; from the standpoint of the Indian contract law, such consent is not deemed to be free. How such entities shall ensure free and informed consent will have to be ascertained in the due course.

Another concerning aspect is pointed out by (Shah, 2023). He argues that given the data's potential to travel, it can travel very fast and far, alienated from the subject itself, creating temporal and digital distance that consent becomes irrelevant, i.e., it is no longer required or possible to obtain. This prompts the need to pay heed to legal scholars' insistence that data must be considered an inalienable resource. The regulations governing the maximum distance data can travel without losing its consent and provenance must be revised to effectively operationalise the new data protection law.

CONSENT MANAGERS

Under Section 2(g) consent managers are a via media through which a person can "give, manage, review or withdraw" their consent given to the data fiduciary. Given, the crucial role they play in data sharing, law should have

comprehensively dealt with them. Rule 4 of the draft DPDP Rules provides for the manner of registration and obligations of the consent managers. No other provision addresses the issues of data misuse and breach by consent managers.

Additionally, it is pertinent to note here that under Indian law, the consent model has not been tested yet. A framework for consent managers has to be created, tested, and implemented throughout the business landscape. This necessitates integration of consent management framework with the consent architecture of the data fiduciary. Therefore, to avoid transgressions, entities dealing with data must inventory their datasets and determine who has access to them, where they are located, etc. Gap analyses and privacy impact assessments shall be required to determine their "readiness" to adapt to the new law. Particularly, companies with e-commerce verticals will face issues in processing data as the platform providers will be data controllers (Sur, 2023).

With the increasing need of consent managers and their significant role in the data processing and protection, experts predict birth of a new kind of company called 'data companies'. The expanding network of such platforms/ companies warrants a separate legal framework as the DPDPA does include them in its regulatory framework for such entities. The stakeholders may consider the legal framework proposed by the (Gopalakrishnan et al., 2020) Committee for regulating data businesses.

INADEQUACY OF REMEDY

The Act specifies the penalty for data fiduciary in case of a compromise or misuse, does not provide for compensation to the aggrieved data principal. It only stipulates leveraging fine on data fiduciaries, which the objective of putting a check on them. Under the section 43A of IT Act, 2000 which the DPDPA shall repeal, remedy of compensation in case of breach was provided for the individual whose data was breached.

SIGNIFICANT DATA FIDUCIARY

The definition of 'significant data fiduciary' is vague and ambiguous. The ambiguity was reasonably expected to be resolved by the Rules; but they are silent. They do not outline any criteria or threshold for qualifying as a significant data fiduciary, leaving it on the government to earmark any data fiduciary as 'significant'.

REALISATION OF THE RIGHTS OF USERS

The autonomy of users is enhanced by the DPDPA, as it gives them the right to access, complete, correct, update as well as erase their data. But it does not prescribe the mechanism through which the rights are to be exercised. This has created a vacuum remains as even the Rules do not prescribe any *modus operandi* for making requests. They simply restate what Act lays down in paraphrased words. It is left on the discretion of the businesses (data processors) to identify the steps for user for making requests for exercising such rights. (Kakkar & Mohan, 2025) highlight that Indian courts have in a catena of cases asked Goggle to "de-list" certain links that feature on its public search engine. For clarity, the Rules could have specified the mechanism for such scenarios. Moreover, the Indian law does not explicitly define or extends the right to be forgotten to individuals.

THE AMBIGUITY AROUND THE PROTECTION OF CHILDREN'S DATA

With burgeoning digitisation, the susceptibility of breach of children's personal data has increased manifold. In the contemporary era, the digital life of children begins long before their biological birth (Rana, Gandhi & Sharma 2024). The access and use of web and online services by children (minor below 18 years of age) results into collection and processing and often exploitation of this data. The DPDPA and Rules aim to address this issue.

The Rules in requiring the data fiduciaries to obtain parental consent for minor users, neglect the fact that the minor registering on their platform may not furnish the correct details of their parents or may impersonate.

Similarly, it is difficult for the data processors to verify whether the person identifying as parent is actually the parent of the child. Alternatively, the child may provide incorrect age to the website and evade the process of parental consent at all. The mechanisms for verifying the age claims shall have to be explored by the websites. (Kakkar & Mohan, 2025) point out a situation very common to the Indian families, the adults and children generally use the same device for accessing digital platforms. In such situations, the child can easily bypass the entire process or may use the device to implicate as parent and give consent.

The proposed Rules do not take into account the implementation difficulties. The law puts the platform under the duty to prevent the minors (under 18 years of age) from evading their radar. They have to verify the age of every user invariably. The verification process is criticised by human rights activists. They perceive it as a potent threat to the freedom of expression.

Another dimension to this, is the literacy rate of India. Since, the literate population is quite low and lower is the proportion of people who are below digitally equipped. Only 20 percent of Indian parents can be expected to give 'informed consent' but the other 80 can only give assent, as they do not understand the implications of what they consent to.

It is suggested that India may, for the purposes of DPDPA, reduce the consent age, similar to EU and Korea where it is 16 years (reducible by States to 13) and 13 years, respectively.

THE FLAWED DESIGN OF THE DATA PROTECTION BOARD

Alok Prasanna Kumar (Kumar, 2022), a leading legal scholar, argues that considering the fact that the DPDPA is an offshoot of the Apex Court's recognition of informational privacy an off-shoot of RTP, therefore, the board established under this Act should be a "responsive regulatory body" independent and empowered to discharge its constitutional role (Mohamed, 2023). Enforcement of the data protection framework by a high-powered statutory authority was listed by the Srikrishna Committee as an essential principal of the data protection framework.

The Act left much for the Rules to provide; however, the Draft Rules contain nothing to strengthen or improve the capacity of the Board in order to make it a regulatory body India needs at this critical juncture. Additionally, pertinent questions with respect of the Board's constitutional validity and its capacity to implement to provisions of DPDPA remain unanswered in the Rules.

Further the institutional design of the DPB remains undefined. Although, it is unrealistic to expect any subordinate legislation to provide for the same, the parent Act should have taken care of it (Editorial, 2025).

The Act under section 27 prescribes the Board's composition and functions and outlines the procedure for their performance in section 28. The appointment, removal and eligibility criteria for appointment as Chairperson or members is also prescribed but a careful reading reveals the vagueness of provisions and over-dependence on the Rules.

1. The power of removal of chairperson and members vests with the central government but no procedure is prescribed for the same, except for the provision of an opportunity of being heard before removal.
2. The qualifications for members/chairperson listed under section 19(3) are too broad to be of any guidance on what ought to be the board's

composition.

3. The tenure of the functionaries is surprisingly very short, hence shall deprive them from developing any "meaningful capacity" in a nascent and fairly complex area of law (Ganesan, 2023).

Additionally, the Act divests the civil courts from jurisdiction over data protection matters (section 39) and repeals the provision of the IT Act, 2000 which provides for appointment of an "adjudicating officer" by the union government. Thus, under the new law, the Data Protection Board is the sole agency responsible for protecting the rights of a data principal in India, making it an important institution in the data protection landscape. The Board subsumes the powers of the adjudicating officer save the power to award compensation to the data principle for breach of data or leak. The key issues in the mechanisms envisaged for constitution and the functioning of the Board:

1. Rule 16 provides for the mechanism of appointment of the functionalities— Chairperson and the members through a Central government constituted search cum selection committee. The selection committee shall have officers of the government and two co-opted members who must be "experts" having practical experience in the domain area.
2. Section 19 (3) requires appointment of at least one member on the Board who is an 'expert in the field of law'. The search cum selection committee however entrusted with this task of appointment of a law person, is not required by the law to have legal expertise, save the Secretary in-charge of the department of legal affairs.
3. The premise of this requirement of Board having a legal member appears flawed as a person expert in law may or may not be an expert in adjudication. The law assumes that legal expertise includes adjudicatory expertise.
4. The final discretion in the matter of appointment of the chairperson and the members vests with the central government (Tiwari, 2025).
5. Rule 18 provides that procedure for board to carry out its functions, however the Rules do not lay down the procedure for holding inquiries (Kumar, 2025).
6. Rule 18 (9) prescribes that enquiries must be concluded within 6 months or 9 months (in case of extension).
7. In respect of "techno-legal measures" prescribed by the Act, the rules are silent and do not attempt to clarify the position. All they do is reproduce the contents of section 28(1) to state that the board may

adopt techno-legal measures to conduct proceedings so that physical presence of the parties is dispensed with.

It is pertinent to note that the Srikrishna Committee recommended three major functions of the authority (now DPB) to be established under the Act: 1. monitoring, enforcement and investigation, 2. setting standards, 3. generating awareness. Under the scheme of the DPDP Act and the Rules performance of the third function (generating awareness) by the Board, doesn't find any mention.

ACCUMULATION AND PENDENCY

Post-enactment of the Act, all data breaches will be adjudicated by the DPB only. Since the DPB has not been constituted yet, all cases of breach are left to hang in abeyance. This will naturally result in accumulation of cases, resulting in long pendency considering there is no time-bound mechanism of dispute redressal.

UNSPECIFIED ADJUDICATION TIMEFRAME

The time bound adjudication mechanism aspect seems to be hit by legislative oversight in the case of DPDPA and Rules. They do not specify any timeframe within which a complaint made by a data fiduciary to the Board has to be adjudicated upon by the Board. Absence of a time-bound dispute settlement mechanism similar to Insolvency and Bankruptcy Code, 2016, may become a significant roadblock for the ease of doing business in India.

CONCERNS REGARDING CROSS BORDER DATA TRANSFER OF DATA

DPDPA is modelled on the EU's GDPR but it diverges on various key facets. For instance, the GDPR contains specific provisions, permitting the transfer of personal data to third countries based on an assessment of adequacy and specified protective measures. In contrast, the DPDPA does not specify for any cross-border transfers.

The incoherent stand of the Act and the DPDP Rules, 2025 (draft) has created a problem for the companies operating in India, especially those based in the US. The Act adopts a blacklisting approach and permits cross border data transfers, except in cases of countries notified by the union government. Rule 12(4) states that data which is specified by the central government shall not be transferred along with the traffic data by the significant data fiduciaries (Parasnis, 2025).

The Reforming Intelligence and Securing America Act (RISAA) enacted by the USA in 2024 stands in direct conflict with the DPDP Rules, 2025 (draft). The US law expressly requires the US-based companies to share with the USA government all communications of data (including emails, texts, phone calls etc.) of foreign citizens availing their services. The legislative intent behind this provision is that such a measure is necessary for "national security" (Leo, 2024).

What will be the future course of American internet companies, will Indian government undertake measures like EU-US Privacy Sheild or will stand firm on its defensive stand to protect the data of Indians from USA's snooping.

CONCLUSION

With the rapidly expanding technological interface, the herculean task of balancing the individual's RTP and the legitimate interest of the State ought to be performed by the law. The GoI took concrete steps towards building a legal framework for data protection. However, despite recommendations of expert committees and many iterations of the draft law, India could not enact a comprehensive data protection law. The DPDP Act, enacted in August 2023, is disappointing—failing to deliver on many counts. It is not exhaustive and has unreasonably excluded much from its remit.

Particularly, wide exemptions to the government and the unrestricted wording of legitimate purposes under section 7, requires to be amended. Since, the Indian privacy regime is nascent, naturally, it shall be people-driven. Thus, companies dealing with personal data must ensure capacity building to avoid data breach and consequent penalties.

Ironically, the Act was projected as a protective valve for the rights of data principals, but in practice, it imposes duties on them. Invariably, legislative uncertainty repulses investors—the non-enforcement of the Act, coupled with the delay in the notification of the final Rules, has negatively impacted the ease of doing business in India.

REFERENCES

Bal, M., & Kashyap, S. (2024). *An Empirical Evaluation of the Implementation Challenges of the Digital Personal Data Protection Act 2023*. www.esyacentre.org.

BS Web Team. (2023, September 27). *DPDP Act: Firms in disarray, seek more time, clarity for implementation*. Business Standard. https://www.business-standard.com/industry/news/dpdp-act-firms-in-disarray-seek-more-time-clarity-for-implementation-123092700357_1.html.

No secret affair: on the draft Digital Personal Data Protection Rules, 2025. 2025 *The Hindu*. https://www.thehindu.com/opinion/editorial/no-secret-affair-on-the-draft-digital-personal-data-protection-rules-2025/article69064313.ece.

Ericsson. (2024). *Ericsson Mobility Report*. https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/november-2024

Ganesan, A. (2023, November 2). *Data Protection Board of India: Composition and its Impact*. Medianama. https://www.medianama.com/2023/11/223-composition-data-protection-board-impact/.

Gopalakrishnan, K., Ghosh, D., Verma, N., Katragadda, L., Kumaraguru, P., Singh, P. J., Narayanan, K., Dayasindhu, N., & Matthan, R. (2020). *Report by the Committee of Experts on Non-Personal Data Governance Framework*.

Indo Asian News Service. (2023). *Data protection bill: Big Tech coalition seeks 12-18 month extension to comply with India's DPDP Act*. The Economic Times. https://economictimes.indiatimes.com/tech/technology/big-tech-coalition-seeks-12-18-month-extension-to-comply-with-indias-dpdp-act/articleshow/104726843.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

Kakkar, J. M., & Mohan, S. (2025, January 13). How the draft rules for implementing data protection falls short- The Hindu. *The Hindu.* https://www.thehindu.com/sci-tech/technology/how-the-draft-rules-for-implementing-data-protection-falls-short/article69092017.ece.

Kanwar, S., & Manish, M. (2023). Evolution of India's Data Protection Law: A Primer. In *ICRIER Policy Brief 4*. Centre for Internet and Digital Economy. https://icrier.org/pdf/IPCIDE-Policy_Brief_4.pdf.

Kessler, D. J., Ross, S., & Hickok, E. (2014). A Comparative Analysis of Indian Privacy Law and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules. *National Law School of India Review*, *26*(1), 31–61.

Kumar, A. P. (2022). A Defective Data Protection Board. *Economic and Political Weekly*, *57*(52), 10–11.

Kumar, A. P. (2025). The Digital Personal Data Protection Board. *Economic and Political Weekly*, *60*(3), 10–12. https://www.epw.in/journal/2025/3/law-and-society/digital-personal-data-protection-board.html.

Leo, S. (2024, July 30). *On US surveillance on foreign citizens, and implications on India*. Medianama. https://www.medianama.com/2024/07/223-us-risaa-act-foreign-citizens-surveillance-implications-india/.

Mohamed, B. (2023). Designing an Effective Data Protection Regulator. *Economic and Political Weekly*, *58*(35). https://epw-nassdoc.refread.com/journal/2022/1/commentary/designing-effective-data-protection-regulator.html.

Nidumuri, L. K., & Shetty, T. (2020, May 15). *Right to Privacy of Companies vis-a-vis the Powers of the Central Government under Section 206(5) of The Companies Act, 2013 - Has the Balance Been Lost?* Mondaq. https://www.mondaq.com/india/privilege/934460/right-to-privacy-of-companies-vis-a-vis-the-powers-of-the-central-government-under-section-2065-of-the-companies-act-2013-has-the-balance-been-lost.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (2002). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. https://doi.org/10.1787/9789264196391-EN.

Parasnis, S. (2025, January 4). *Will The DPDP Rules Conflict With US Surveillance Law?* Medianama. https://www.medianama.com/2025/01/223-dpdp-rules-2025-conflict-us-surveillance-laws/.

Rahul Matthan, & Group of Officers. (2010). *Approach Paper for a Legislation on Privacy* (17; 1).

Rana, V., Gandhi, A., & Sharma, I. (2024, September 18). *Safeguarding Children's Data Under The DPDP Law*. Mondaq. https://www.mondaq.com/india/privacy-protection/1519120/safeguarding-childrens-data-under-the-dpdp-law.

Ravindran, S., Panda, L., & Jauhar, A. (2023). *Comments on the Draft Digital Personal Data Protection Bill, 2022*. https://vidhilegalpolicy.in/research/comments-on-the-draft-digital-personal-data-protection-bill-2022/.

Shah, N. (2023, September 27). No, data isn't the new oil – Data Protection Bill needs to realise that. *Indian Express*. https://indianexpress.com/article/opinion/columns/no-data-isnt-the-new-oil-data-protection-bill-needs-to-realise-that-8957684/.

Srikrishna, B. N., Sundarajan, A., Pandey, A. B., Kumar, A., Moona, R., Rai, G., & Krishnen. (2018). *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*.

Statista. (2023). *Mobile communications in India*. https://statista-nassdoc.refread.com/statistics/467163/forecast-of-smartphone-users-in-india/.

Sur, A. (2023, August 14). *Companies face tall task in complying with new data protection law*. Money Control. https://www.moneycontrol.com/news/business/companies-face-tall-task-in-complying-with-new-data-protection-law-11179671.html.

Tiwari, V. (2025, January 4). *DPDP Rules: India's Data Protection Board, Function and Appeals*. Medianama. https://www.medianama.com/2025/01/223-dpdp-rules-2025-india-data-protection-board-function-appeals/.

United Nations. (2024). India: median age of the population 1950-2100. In *Statistia*. https://statista-nassdoc.refread.com/statistics/254469/median-age-of-the-population-in-india/.

Wang, Y., & Bai, C. (2024). Eyes everywhere: the influence of digital surveillance on employee innovation performance in China. *Asia Pacific Business Review*. https://doi.org/10.1080/13602381.2024.2371357.

World Economic Forum, & Accenture. (2024). *Global Cybersecurity Outlook*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.

ETHICAL CONSIDERATION:

Plagiarism and AI Declaration: The author declares that this article is an original work. All sources used have been properly cited, and no part of the content has been plagiarized. Any use of AI-assisted tools was limited to language support and did not replace the author's original ideas, analysis, or conclusions.