Page 1841 - 1853 **DOI:** *https://doij.org/10.10000/IJLMH.115963*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 5

2023

Transforming Data Privacy: An Analysis of India's Digital Personal Data Protection Act

DR. ANIKET SHARMA[1]

ABSTRACT

The Digital Personal Data Protection Act of India (DPDP) represents a transformative milestone in India's data protection landscape. Enacted after years of deliberation and drawing inspiration from the GDPR, the DPDP Act aims to establish a comprehensive framework for the processing of personal data, encompassing both public and private entities regardless of their size. The Act introduces fundamental concepts such as "data fiduciaries" and "data principals," providing equal protection to all forms of personal data. Emphasizing consent as a primary basis for data processing, the Act grants certain rights to data principals, setting the stage for greater transparency and control over personal data. It also outlines responsibilities for data fiduciaries, focusing on data security, breach notification, and accountability. However, the Act has been met with some criticism, particularly concerning exemptions for journalistic purposes and the significant regulatory authority granted to the central government. Despite these concerns, the DPDP Act lays a strong foundation for the protection of personal data in India, aligning with the fundamental right to privacy recognized by the Supreme Court. It represents a crucial step forward, addressing the gaps in the previous data protection framework and positioning India in the global landscape as a country committed to safeguarding personal data.

Keywords: *Data Protection, Data Protection Act of India, Data Privacy.*

I. INTRODUCTION

After years of discussions, delays, and agreements, the Digital Personal Data Protection Act of India (DPDP) sped through its last steps last week, ending in its publishing in the Official Gazette on Friday, August 11, 2023. The Bill was approved by both the lower and upper Houses of Parliament and got presidential assent in a little more than a week. With over 1.4 billion inhabitants, India is the most populous nation in the world, the largest democracy, and the 19th G20 member to implement a complete personal data protection law, which it accomplished when it had the G20 Presidency.

[1] Author is a Guest Faculty at Himachal Pradesh University Institute Of Legal Studies, Shimla, India.

 [ISSN 2581-5369]

Following Justice *K.S. Puttaswamy v. Union of India*[2], a landmark case in which the Supreme Court of India recognised a fundamental right to privacy in India, including informational privacy, within the "right to life" provision of India's Constitution, the DPDP Bill was adopted by the Parliament six years later. A nine-judge Supreme Court panel advised the Indian government to implement "a carefully structured regime" for the protection of personal data in this ruling. There have been numerous rounds of expert discussions and studies as part of India's continuous efforts to establish this regime, and two prior versions of the bill were tabled in Parliament in 2019 and 2022.

The law is transformative in its current version. It extends coverage to all entities that process personal data regardless of size or private status and uses the General Data Protection Regulation (GDPR) approach to define "personal data" in order to have a broad scope of application. Significant extraterritorial application is also a feature of the legislation. The DPDP imposes broad obligations, establishing purpose limitation obligations and their corollary—a duty to erase the data once the purpose is met, leaving seemingly no room for secondary uses of personal data—as well as a set of rights for people whose personal data are collected and used, including rights to notice, access, and erasure. The law also establishes a supervisory body, the Data Protection Board of India (Board), with the jurisdiction to look into complaints and levy fines but not to develop policies or guidelines.

The degree of the exception depends on the function of the government body in question (such as law enforcement), although the legislation also makes considerable exclusions for the federal government and other government entities. Other exemptions cover processing for research and statistical purposes, processing for most publicly accessible personal data, and processing foreigners' personal data by Indian companies in accordance with a contract with a foreign company (such as outsourcing firms). If the government notifies startups, some processing may also be excused. The Act also gives the central government the authority to act on the Board's notification and request access to any information from a party processing personal data, an intermediary (as defined by the Information Technology Act, 2000, or the "IT Act"), or from the Board, as well as to order the suspension of the public's access to a particular piece of information. The Central Government is also given the authority to enact several "rules" (like to the regulations under state privacy laws in the US) that specify how the legislation will be applied.[3]

[2] (2017) 10 SCC 1

[3] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264 (Last Visited On 20-08-2023)

 [ISSN 2581-5369]

Understanding that the law won't take effect until the government announces an effective date is crucial. The DPDP Act does not have a required transitional time like the GDPR's two-year delay between its legislation in 2016 and its implementation in May 2018. Instead, it gives the government the authority to choose the dates on which the Act's various provisions—including those controlling the creation of the new Board that would monitor adherence to the law—will go into effect.

II. The "data fiduciaries," "significant data fiduciaries," and "data principals" are covered by the DPDP Act

The DPDP Act aims to create a comprehensive national framework for processing personal data in place of the IT Act's much more constrained data protection framework and existing regulations that only offer minimal protections for a small number of "sensitive" categories of personal data, such as sexual orientation and health information. Contrarily, the new law offers equal protection for all "personal data" and does not prioritise any one kind of data. Personal data is defined as "any data about an individual who is identifiable by or in relation to such data." The GDPR's broad "identifiability" requirement, which is used to define "personal data," is thus used in this definition. The regulation only applies to "digital" personal data, which are personal data gathered via non-digital methods and later converted to digital form.

The phrase "data principal" (the DPDP Act's equivalent of "data subject" under the GDPR) designates the person to whom the personal data relates. A "data fiduciary" is the same as a "data controller" under GDPR and is the organisation that chooses the goals and methods of processing personal data, either alone or in collaboration with others. While possible joint fiduciaries are mentioned in the definition of data fiduciaries, the Act makes no other mention of this relationship.

Fiduciaries can technically be anyone as long as the other requirements of the law are satisfied because the definition makes no distinction between private and public, natural and legal individuals.

There are some basic exceptions to the rule that apply to all government organisations, and others that only apply to certain types of processing. For instance, the law permits the government to exempt activities that are in the interests of the security of the State, the maintenance of public order, the preservation of the sovereignty and integrity of India, friendly relations with foreign States, or the prevention of incitement to commit crimes, provided that it notifies the public of the exemptions. Several Members of Parliament during the legislative debate as well as Justice Srikrishna, who served as the chairman of the expert committee that

 [ISSN 2581-5369]

was established to develop a data privacy law in India, have criticised these government exclusions.[4]

Companies are subject to a few focused exclusions that are either clearly outlined in the law or left up to the discretion of the executive branch. Under what is known as a "outsourcing exception," the Act exempts companies based in India from the core DPDP obligations, including the access and erasure rights typically held by data principals, when they process the personal data of individuals outside of India as part of a contract with a company based outside of India. Instead, these businesses are mostly just required to adhere to data security obligations.

The DPDP itself refers to "startups" in this sense, and the government is also allowed to exempt any type of data fiduciaries from all or part of the law. These are fairly wide provisions, and there is no explanation of how they will be used or who will stand to gain from them. To be effective, this exception requires a special designation from the government.

According to a set of criteria without quantitative thresholds, the DPDP Act gives the government the authority to designate any data fiduciary or class of data fiduciaries as a "Significant Data Fiduciary" (SDF). These considerations range from evaluating processing operation characteristics (volume and sensitivity of personal data processed and risk posed to data principals' rights) to broader societal and even national sovereignty concerns (possible impact of processing on India's sovereignty and integrity; risk to electoral democracy; state security; and public order).

The designation of businesses as SDFs has consequences because it carries with it more stringent responsibilities. A Data Protection Officer (DPO), who must be based in India and serve as the point of contact for a necessary grievance redressal process, will be the most important of these. Additionally, SDFs are required to designate an impartial data auditor to conduct data audits, assess the SDF's compliance with the DPDP Act, and conduct routine Data Protection Impact Assessments.

It is significant to remember that not all data fiduciaries are required to designate a DPO. However, all fiduciaries are required to set up a "readily available" procedure for promptly resolving complaints by data principals. Typically, an internal privacy compliance role or a dedicated privacy officer would be useful for such a process to be operationalized.

The DPDP Act, which clearly states that fiduciaries may employ, appoint, or otherwise involve processors to process personal data on their behalf "only under a valid contract" (Section 8(2)),

[4] https://www.meity.gov.in/writereaddata/files Digital%20Personal%20Data%20Protection%20Act%202023.pdf (Last Visited On 20-08-2023).

 [ISSN 2581-5369]

recognises the existence of data processors. There are no established guidelines for what should be included in a processing contract. The DPDP Act, however, places all responsibility on data fiduciaries, who are nevertheless responsible for abiding by the law.

Regardless of any agreements to the contrary with data processors, data fiduciaries are nonetheless responsible for overall compliance. According to the DPDP Bill, data fiduciaries must order a processor to remove data when a data principal withdraws consent, and they must be able to give information about the processors they have hired when a data subject requests it.

III. Broad extraterritorial effects of the DPDP Act and nearly no restrictions on international data transfers

The processing of "digital personal data" within India is governed by the DPDP Act. Importantly, the definition of "data principal" does not mention any requirement relating to residence or citizenship, which suggests that (outside of the "outsourcing exception" mentioned above) fiduciaries based in India who process the personal data of foreigners within the country may be subject to the Act.

If the processing of digital personal data takes place outside of India and is connected to any activity that involves providing goods or services to data principals inside of India, the Act also applies extraterritorially to such processing. The extraterritorial effect's breadth is comparable to that of the GDPR, and the inclusion of "any activity" associated with the provision of goods or services may allow for a broader interpretation.

The transmission of personal data outside of India is not currently prohibited by the DPDP Act. By assuming that transfers may occur without restrictions, it flips the conventional paradigm of international data transfer provisions in laws like the GDPR. This is true unless the government specifically forbids transfers to certain countries (blacklisting) or enacts any other kind of restriction (Section 16). The law contains no specifications for these limitations. This is a substantial change from earlier versions of the Bill, which at one time (2022) morphed into a "whitelisting" of nations and at another stage (2018) featured data localization obligations.

It should be emphasised that there are currently regulations on cross-border transfers of specific types of data under other existing sectoral laws (e.g., those governing specialised industries like banking and telecommunications). The DPDP Act makes it clear that the new law won't have an impact on current localization regulations.[5]

[5] The Digital Personal Data Protection Act, 2023 | Commercial Law Publications | Bare Acts |

 [ISSN 2581-5369]

IV. The Act's primary method for the processing of personal data is still consent

Data fiduciaries are required to process personal data for authorised purposes only, and only if they do so with the data principal's consent or by establishing a "legitimate use" that complies with Section 4. This procedure is essentially similar to the GDPR's suggested strategy in that it demands a legal basis before any personal data is gathered or otherwise handled. But in contrast to the GDPR, which lists six potential legal justifications, the DPDP Act only mentions two: "legitimate use" and "strictly defined consent."

It is consequential which legal basis is employed for a processing procedure. According to the Act's language and in the absence of additional clarification, the obligations of fiduciaries to provide notice and respond to requests for access, correction, and erasure (see Section 4 of this blog) only apply if the processing is driven by the principal's informed consent and voluntary sharing of personal data.

In accordance with the DPDP Act, consent for the processing of personal data must be "free, specific, informed, unconditional, and unambiguous with a clear affirmative action." These requirements are just as stringent as those stipulated by the GDPR, emphasising that the consent of the individuals whose personal data is processed must be freely given and cannot be conditional.

The Act stipulates that principals must get notice prior to or at the time they are requested to offer approval in order to satisfy the "informed" condition. Information concerning the personal data to be gathered, the reason it will be processed, how data principals can exercise their rights under the DPDP Act, and how to file a complaint with the Board must all be included in the notification. Data subjects must be given the choice of receiving information in either English or one of the Constitution's designated local languages.

The DPDP Act deals with the problem of legacy data, for which businesses may have gotten permission before the law was passed. These data principals should receive the same warning from fiduciaries as soon as "reasonably practicable." However, if that happens, data processing may go on until the data principal withdraws their consent.

Data fiduciaries are only permitted to use personal data for the particular purposes that the data principal has authorised; all other uses of the data require supplementary authorization. This will really make it challenging for data fiduciaries to depend on "bundled consent." The Act

 [ISSN 2581-5369]

does not address "compatible purposes" or "secondary uses" of personal data, making the purpose limitation requirements stringent.

Data fiduciaries must make sure that the method for withdrawing consent is as simple as the process for granting it. Data principals have the right to withdraw their consent at any moment. Unless a legal requirement to maintain data occurs, personal data must be erased if consent is withdrawn. In addition, in the absence of legislative requirements requiring data retention, data fiduciaries must request that processors stop using any personal data for which consent has been revoked.

According to the DPDP Act, principals may grant, manage, evaluate, and withdraw their consent through a "Consent Manager," which must offer an open, transparent, and interoperable platform and be registered with the Board. The "Data Empowerment And Protection Architecture" policy of India includes consent managers, and comparable organisations have been operational for some time in other industries, like the financial one. The DPDP Act mandates that Consent Managers answer to data principals and represent them in accordance with the requirements. The requirements for a corporation to register as a Consent Manager will be announced by the government (in the Gazette), and they may include meeting minimal technical or financial requirements.

All other legal justifications for processing personal data, outside permission, have been consolidated under the "legitimate uses" section. This includes certain justifications for processing that were previously listed under the "reasonable purposes" part in earlier draughts of the bill. Notably, the list of "legitimate uses" in Section 7 of the Act does not contain equivalent clauses to the justifications of "contractual necessity" and "legitimate interests" found in data protection laws modelled after the GDPR, giving private fiduciaries few options for justifying the processing of personal data in situations other than those requiring consent, such as routine or necessary processing operations.

The "voluntary sharing" of personal data under Section 7(a) and the "employment purposes" use under Section 7(i) are the two most pertinent "legitimate uses" among the ones that have been identified for processing personal data outside of a government, emergency, or public health context.

The legal justification that is most likely to give rise to interpretation issues is "voluntary sharing." It permits a data fiduciary to process personal data for a designated purpose if the principal has voluntarily provided the data fiduciary with their personal information (likely without the data fiduciary attempting to obtain consent) and if the principal hasn't

 [ISSN 2581-5369]

communicated to the data fiduciary their objection to the use of the personal information. For instance, the hypothetical scenario of a customer asking a retailer to send her a receipt of purchase to her phone number and allowing the retailer to use the number for that purpose is one of the examples provided in the law to explain Section 7(a). Future regulations may broaden this definition of "legitimate use" to include situations involving "contractual necessity" or "legitimate interests."

For employment-related purposes or those involving protecting the employer from harm or liability, such as preventing corporate espionage, maintaining the privacy of trade secrets, intellectual property, or classified information, or for the purpose of providing any service to employees, a fiduciary may also process personal data without consent.[6]

V. THERE IS A LIMITED SET OF "DATA SUBJECT RIGHTS," BUT THERE ARE ALSO OBLIGATIONS ON DATA PRINCIPLES

In comparison to modern data protection legislation like the GDPR, the DPDP Act only offers a small number of listed rights to data principals. Similar to the right to information in the GDPR, the DPDP guarantees a right to information, a right to access, a right to erasure and correction, and a right to notification before consent is requested. Therefore, there is a lack of a right to data portability, a right to object to processing on grounds other than permission, and a right to refrain from being the sole subject of automated decision-making.

Instead, the DPDP Act stipulates two additional rights: a right to "grievance redressal," which includes the right to an easily reachable point of contact provided by the fiduciary to address the principal's complaints; and a right to "appoint a nominee," which enables the principal to name someone to represent them in exercising rights in the event of death or incapacity.

Notably, the rights of access, erasure, and correction are only applicable to personal data processing based on consent or "voluntary disclosure," legitimate use. This means that whenever government entities or other fiduciaries rely on any of the "legitimate uses" grounds, they are not required to respond to requests for access or erasure/correction unless other rules adopted by the government specify otherwise.

The scope of the right of access is also extremely constrained. It only grants data principals the right to request and obtain a summary of the personal data being processed, of the relevant processing activities, and the identities of all fiduciaries and processors with whom the personal data has been shared by the fiduciary, along with a summary of the data being shared (as

[6] Ibid

 [ISSN 2581-5369]

opposed to obtaining a copy of the personal data). However, Section 11 of the statute leaves room for later regulations that can specify what more information must be made available.

According to Section 12(3), data principals have the right to request the deletion of their personal data, but it's crucial to note that deletion may sometimes be necessary automatically, such as following a consent withdrawal or when the intended purpose is no longer being met (Section 8(7)(a)). Similar to this, where personal information is "likely to be used to make a decision that affects" the principal (as defined in Section 8(3)), it must also be corrected, completed, and updated automatically.

Section 15 of the DPDP Act, like Article 10 of Vietnam's newly passed Personal Data Protection Decree (entitled "Obligations of data subjects"), imposes obligations on data principals, contrary to the majority of international data protection regulations.

These obligations include, among others, a duty to refrain from impersonating another person while providing personal data for a specific purpose, a duty to refrain from withholding any relevant information while providing personal data for any document issued by the Government, and, perhaps most importantly, a duty to refrain from filing an unfounded or unjustified grievance or complaint. A fine could be assessed for noncompliance (see clause 5 of the Schedule). The submission of complaints to the Board may be hampered as a result, according to expert analysis.

VI. FIDUCIARIES HAVE DATA BREACH NOTIFICATION OBLIGATIONS AND ARE BOUND BY AN ACCOUNTABILITY PRINCIPLE

Although the DPDP Act does not explicitly state any Principles of Processing or Fair Information Practise Principles, it does emphasise responsibility and purpose limitation in some of its clauses, as previously discussed in this blog.

Multiple responsibilities for data fiduciaries are outlined in Section 8 of the Act, all falling under the general expectation in Paragraph 1 that they are "responsible for complying" with the Act's provisions and any ensuing implementation rules, both with regard to processing done by the data fiduciary and by any processor acting on its behalf. The accountability principle of the GDPR is echoed in this specification. Additionally, data fiduciaries are required to put in place the proper organisational and technical safeguards to guarantee the law's proper execution.

Data security is especially important since data fiduciaries are required to take reasonable security precautions to prevent personal data breaches and notify the Board and any others

 [ISSN 2581-5369]

affected if they do happen. Subsequent implementation guidelines will include specifics about notification modes and deadlines.

The establishment of a "readily available" system for promptly resolving "grievances" by data principals is the last duty of data fiduciaries to be highlighted. Given that data principals cannot file a complaint with the Board before they "exhaust the opportunity of redressing" the grievance through this process (Section 13(3)), the "grievance redress" method is of the utmost importance. The Act leaves it up to delegated legislation to decide how long corporations have to react to complaints, so there may be varying time limits for various business types.[7]

VII. Fiduciaries are required to confirm parental approval before processing a minor's under-18 personal information

With "children" being defined as minors under 18, the DPDP Act establishes major requirements for processing children's personal data without making any distinctions for older children or teens. Data fiduciaries are generally prohibited from processing kid data in a way that is "likely to cause any detrimental effect on the well-being of the child."

Data fiduciaries must secure verifiable parental consent before processing any child's personal information. Similar to this, permission from a legitimate guardian is required before processing a person's disability-related data. This requirement, which is becoming more prevalent in privacy and data protection regulations around the world, may provide numerous difficulties in real-life situations.

Last but not least, the Act forbids data fiduciaries from following or observing children's behaviour or directing targeted advertising to them. The government may grant exemptions from these requirements for particular kinds of data fiduciaries, or it may even reduce the age of digital consent for minors, where their personal data is processed by approved data fiduciaries. This is similar to how many other articles of the Act are written.

VIII. The law establishes a data protection board to uphold the law while reserving regulatory authority to the government

The Board will be tasked with executing the new law, and the DPDP Act gives the government the authority to create it as an autonomous entity. A Chairperson and Members of the Board shall be chosen by the government for a two-year term that is renewable.

[7] *Supra* note 5

 [ISSN 2581-5369]

The relevant data fiduciaries have given the Board the authority to receive and look into complaints from data principals, but only after the principal has used up any internal grievance redress options available to them. The Board has the authority to send parties to mediation, mandate immediate actions to mitigate or remedy a data breach, and issue enforceable orders against those who violate the law.

The Act expressly forbids any access to civil courts in the application of its provisions (Section 39), resulting in a de facto restriction on effective judicial remedy comparable to the relief provided in Article 82 GDPR, despite the Board being granted "the same powers as are vested in a civil court" (Section 28(7)). The Telecom Disputes Settlement and Appellate Tribunal, which was established by another Indian law, is the appellate tribunal designated by the Act to hear appeals from individuals impacted by Board decisions.

The DPDP Act's Schedule lists the penalties for breaking the law, and they range from the rupee equivalent of $120 to $30.2 million in dollars. Based on the offence, the Board may choose the punishment amount from a predetermined range.

The Board, however, lacks the authority to enact regulations that would further define specifics pertaining to the Act's execution. The Government has wide latitude in establishing delegated legislation to further define the Act's provisions, including the ways and times that fiduciaries must respond to data principals' requests, the standards for a valid notice to obtain a data principal's consent to processing, the specifics of data breach notifications, and more. The list of operational specifics that the Government may include in ensuing rules is unbounded and is described in Section 40(2)(a) through (z). This provision's catch-all subsection (z) gives the Central Government the freedom to impose regulations on "any other matter" connected to the implementation of the Act.

It is anticipated that it will take some time to form the new Board and publish regulations in important areas of compliance.

The Central Government has additional substantial influence over how the law is applied in addition to its rule-making authority. According to Section 36, it is permitted to "call for" any information (perhaps including personal data) from the Board, data fiduciaries, and "intermediaries" as defined by the IT Act. Other than stating that such requests must be made "for the purposes of the Act," no other details are provided regarding such requests. Compared to the provisions on data access requests in the current IT Act and its subsidiary rules, this provision is more expansive and subject to fewer limitations.

 [ISSN 2581-5369]

In addition, the Central Government has the authority to direct or order any official or "intermediary" to deny access to material "in the interests of the general public." The Board must have sanctioned the data fiduciary in question at least twice in the past in order to issue such an order, and it must also advise the Central Government to do so. "Any computer resource" that enables data fiduciaries to provide products or services to data principals within the territory of India may be referred to in an order restricting public access. These provisions of the DPDP Act are unusual because the orders will come directly from the Government and also because they more closely resemble online platform regulation. While it is now common among modern comprehensive data protection laws around the world for independent supervisory authorities to order the erasure of personal data unlawfully processed, or to order an end to international data transfers or sharing of personal data, if conditions of the law are not met, these provisions of the DPDP Act are unusual because they will come from the Government.[8]

IX. There are some notable exceptions to using publicly available data and processing for AI training

It is important to draw attention to parts of the law that appear to be intended to facilitate the development of AI trained on personal data given that this law arrives at a time when there is a global discussion about how to regulate artificial intelligence and automated decision-making. The Act specifically exempts the majority of publicly accessible personal data from its application, provided that it was made public by the data subject – for instance, a blogger or social media user publishing their personal data directly – or by someone else under a legal obligation to publish the data, such as the personal information of shareholders that regulated companies are required by law to publicly disclose.

Additionally, Section 17(2)(b) of the Act exempts the processing of personal data required for statistical or research purposes. The Act will nevertheless apply to research and statistical processing if the processing activity is used to make "any decision specific to the data principal," which is the only restriction in the core text of this exemption.

Processing data to "make decisions" regarding a data principle is only mentioned once again in the DPDP Act. If personal information is used to make a choice that has an impact on the data subject, data fiduciaries have a responsibility to verify the "completeness, accuracy and consistency" of the data. In other words, even though the Act does not establish a GDPR-style

[8] *Supra* note 4

 [ISSN 2581-5369]

right to be exempt from automated decision-making, it does stipulate that personal data must be kept accurate, consistent, and complete when it is used to make any individual decisions, presumably including automated or algorithmic decisions.

Given the inclusive definitions of "processing" and "personal data," the DPDP Act also continues to be applicable to any processing of personal data by AI systems that satisfies the other legal requirements. Additional Central Government laws or other notices may offer greater direction in this area.

Notably, the Editors' Guild of India criticised the Act for not exempting the handling of personal data for journalistic purposes. This exemption was contained in earlier draughts of the Bill, including the expert version led by Justice Srikrishna in 2017. Delegated legislation from the Central Government may still be used to remedy this problem.

X. Conclusion

The DPDP Act's passage signifies a monumental leap in India's approach to personal data protection, bringing it in line with evolving global standards. By prioritizing consent and introducing a robust framework for data fiduciaries, the Act takes substantial steps toward empowering individuals with control over their personal data. Despite certain critiques and areas for improvement, the Act's comprehensive nature and alignment with fundamental rights, as underscored by the Supreme Court, are noteworthy.

The Act's provisions extend beyond individual rights, addressing data security, breach notification, and the accountability of data fiduciaries. While challenges and further refinements are expected, the DPDP Act stands as a critical enabler for fostering trust in digital transactions and bolstering data privacy. Its extraterritorial reach, applicability to various entities, and broad coverage of personal data underscore the ambitious scope of this legislation. As India joins the ranks of nations with robust data protection laws, effective implementation, ongoing evaluation, and potential amendments will be pivotal to ensuring a dynamic, adaptive, and balanced approach to personal data management in the digital age.

*****

 [ISSN 2581-5369]