Library Progress International *Print version ISSN 0970 1052*
Vol.44 No. 3, Jul-Dec 2024: P. 11776-11782 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

India's New Data Frontier: A Critical Legal Insight of the Personal Data Protection Act, 2023.

Abhishek Kumar*[1], Prabhat Deep*, Shivam Raghuvanshi*, Vivek Kumar*

*Research Scholar, Department of Law & Governance, Central University of South Bihar.

How to cite this article: Abhishek Kumar , Prabhat Deep, Shivam Raghuvanshi, Vivek Kumar (2024). India's New Data Frontier: A Critical Legal Insight of the Personal Data Protection Act, 2023. *Library Progress International*, 44(3), 11776-11782.

ABSTRACT
In the digital era, robust data protection laws are essential to safeguard individual privacy and to ensure responsible data handling. Data profoundly influences societal interactions and economic frameworks. This article critically examines the Digital Personal Data Protection Act, 2023 (DPDP Act) as part of the growing data protection law of India. Beginning with an overview of the Act's key provisions, the analysis delves into its implications for individual privacy rights and businesses. By examining the Act's scope and other provisions, the article identifies both strengths and weaknesses inherent in the legislation. While the DPDP Act marks a significant milestone in India's journey towards data governance, its limitations, including its narrow scope, broad exemptions, and the structure of the Data Protection Board, pose challenges to its effectiveness. The Act's impact on other legislative frameworks, such as the Right to Information Act of 2005, raises concerns regarding transparency and accountability. Through this critical analysis, the article contributes to the broader discourse on privacy, data governance, and regulatory frameworks, shedding light on the complexities of balancing individual rights with technological advancements in the digital age.

KEYWORDS: Data, Digital personal data, Data Principal, Data Fiduciary, Processing and Personal Data Breach

INTRODUCTION

Clive Humby, a British mathematician declared data as new oil in 2006.[2] What oil was in the 20th century, data is in the 21st century. It is changing the economy. Not only do big companies control huge data and most of the economy but the developed countries also prey on the data of the common man while interacting online through mass surveillance and buying from the organisations. The whole world was shocked when the whistle-blower Edward Snowden leaks happened in 2013.[3] The intelligence of the US and UK governments run surveillance on law-abiding citizens.[4] As the data economy is rising in the 21st century. In 2000, the European Union (EU) signed an accord with the US to transfer personal data for commercial purposes.[5] But in 2015 Court of Justice of the European Union in the case of Maximillian Schrems v. Digital

[2] Dag, "Data is the New Oil: Understanding Its Impact on Today's Internet Users" *tomipioneers*, 2024 *available at*: https://medium.com/tomipioneers/data-is-the-new-oil-understanding-its-impact-on-todays-internet-users-13de2bba9688 (last visited October 9, 2024).
[3] Mirren Gidda, "Edward Snowden and the NSA files – timeline" *The Guardian*, 21 August 2013, section US news.
[4] "Edward Snowden discloses U.S. government operations | June 5, 2013," *HISTORY available at*: https://www.history.com/this-day-in-history/edward-snowden-discloses-u-s-government-operations (last visited October 9, 2024).
[5] Martin A. Weiss and Kristin Archick, "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield" *UNT Digital Library* (Library of Congress. Congressional Research Service., 2016), United States *available at*:

Rights Ireland Ltd. invalidated the accord. This era is the modern digital era. Data stands out as the foremost priority and critical factor shaping our world. Today almost every activity of our lives can be digitalized, tracked and used by big companies for the purpose of targeted advertisement and various other influences. Our personal data, including our picture, every journey, purchase, and even health information and more of our personal information is collected, stored, and traded by companies and government entities. Severally undermining Judge Cooley right "to be let alone".[6] It has been found necessary to define and protect a new extent of digital personal data protection. With the increase in the volume of data collected and stored, there is a risk of a greater impact on the right to privacy in case of a data breach, so there is a need of data protection. Organizations that collect data must proactively safeguard data and regularly update their protective measures. The core principle and significance of data protection lie in securing and preserving data against various threats and in different circumstances.

The passing of the new Digital Personal Data Protection Act, 2023 (DPDP Act) makes look like India's supreme law-making body the Indian Parliament has finally woken up on privacy protection matters. Earlier this protection of data and privacy was often dealt with by the other organ judiciary only. The new legislation, the DPDP Act passed in August 2023, first time developed a framework for personal data protection in India. It includes information that could identify individuals, such as names, contact details, computer location, race and sexual orientation. The Act enables individuals to govern their digital data and will drive enterprises who are Data Fiduciaries to process the personal data of individuals lawfully. With a user base of 90 crore people engaging in the digital realm, the Act plays a crucial role in regulating this expansive digital landscape.[7]

The Act is the outcome of several years of consultation among the stakeholders. The legislative journey of the DPDP Act of 2023 began with The Personal Data Protection Bill, 2018 which was prepared by an expert committee and circulated for public feedback, followed by the Personal Data Protection Bill, 2019. The 2019 bill was withdrawn following parliamentary review, and in November 2022 a new draft known as the Digital Personal Data Protection Bill, 2022, was made available for public comment. This draft serves as the main basis for the DPDP Act, 2023.[8]

The DPDP Act is the result of the landmark judgment of the Supreme Court of India in *Justice K.S. Pettaway and Anr. (Retd) v. Union of India and Ors*.[9] in which the right to privacy was recognized as a fundamental right protected under Articles 14, 19, and 21 of the Constitution of India. The DPDP Act gives a specific outline to the right to privacy and it lays down specific mechanisms for the protection of the right to privacy. It also introduces key provisions on consent, data fiduciary responsibilities, and the rights of data principals, reflecting a significant effort to align with global data protection standards.

This article critically analyzes the DPDP Act within the context of India's evolving data protection framework. It provides an overview of the Act's key provisions and examines its implications for individual privacy rights and businesses. The goal is to illuminate the challenges of balancing individual rights with technological advancements, with the ultimate aim of promoting a more secure and privacy-conscious digital space in India.

Operational Definitions under the Digital Personal Data Protection Act 2023

"Data means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means".[10] It may be represented in various forms like text, numbers, images, or any other format that can convey meaning. Data can also be understood and utilized by automated means. "Automated means is any equipment capable of operating automatically in response to instructions given for the purpose of processing data".[11] It can encompass technologies related to artificial intelligence (AI). "Personal data means any data about an individual who is identifiable by or in relation to such data".[12] The term "identifiable" can be subjective and its interpretation may vary. What may identify an individual in one context may not do so in another. "Personal data breach means any unauthorised processing of personal data or

https://digital.library.unt.edu/ark:/67531/metadc855920/ (last visited October 9, 2024).

[6] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," 4 *Harvard Law Review* 193–220 (1890).

[7] "Lok Sabha Debates," Session Number-XII 785–820 (2023).

[8] Anirudh Burman, "Understanding India's New Data Protection Law" *Carnegie Indiaavailable at*: https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624 (last visited January 10, 2024).

[9] 2019 (1) SCC(1); AIR 2017 SC 4161.

[10] The Digital Personal Data Protection Act, 2023 (Act No. 22 OF 2023), s.2(h)

[11] *Id.,* s.2(b)

[12] Id.*,* s.2(t)

accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, which compromises the confidentiality, integrity or availability of personal data".[13] "Processing in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction".[14] In The Personal Data Protection Bill, 2019, in place of "Digital personal data" "personal data" was used which has a wider meaning. "Data Fiduciary means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data".[15] It includes the State, a company, any digital platforms, any juristic entity or any individual. "Data Processor covers in its ambit 'any person who processes personal data on behalf of a Data Fiduciary".[16] "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 a disability, includes her lawful guardian, acting on her behalf".

Global Data Protection Models

The General Data Protection Regulation (GDPR) is the main legislative instrument for data protection in the European Union (EU), providing a comprehensive framework for protecting personal data. The legal basis for Data processing is consent, contract performance, legal obligation, vital interests, public interest, or legitimate interests. Under GDPR, individuals have rights including access to their data, correction, erasure (right to be forgotten), restriction of processing, data portability, and not to be subject to automated decision-making. The EU's GDPR puts high standards on enterprises to make sure that personal data is well protected, and it requires evidence of compliance. Adapting GDPR to emerging technologies like artificial intelligence, facial recognition, and the Internet of Things presents future challenges. Compliance and enforcement issues, especially for small and midsize enterprises (SMEs) and data protection authorities, are also highlighted.[17] The United States employs a sectoral approach to data privacy protection, which means there is no comprehensive federal legislation that ensures the privacy and protection of personal data across all sectors. Instead, the U.S. relies on a combination of federal and state legislation, administrative regulations, and industry-specific self-regulation guidelines. U.S. data privacy laws are tailored to particular sectors like healthcare, education, and financial services. Privacy protection is a combination of federal laws, state regulations, and industry self-regulation guidelines. Industry organizations like the Network Advertising Initiative (NAI) enforce self-regulatory codes of conduct.[18]

KEY PROVISIONS OF THE ACT

The preamble of the Act mentions two clear objects of the Act. The Act aims to recognize the right of individuals to protect their digital personal data. Additionally, it seeks to regulate the processing of digital personal data for lawful purposes, along with related and incidental matters.

APPLICATION OF THE ACT

The Personal Data Protection Act has both territorial and extra-territorial applications. Within the territory of India, it applies to the processing of digital personal data, whether initially collected in digital or non-digital formats, followed by digitisation. Outside the territory of India, the Act extends to the processing of digital personal data if it is in connection with activities that involve offering goods or services to data principals located within India's territory.[19] However, certain cases are exempted, including personal data processed for personal or domestic purposes, as well as data made publicly available by the Data Principal or other entities obligated under Indian law, are considered.

According to Section 4 of the Act, a person can only process the personal data of a data principal for a lawful purpose and with the data principal's consent or for certain legitimate uses. For this, he has to adhere to the provision of this

[13] *Id.,* s.2(u)
[14] *Id.,* s.2(x)
[15] *Id.,* s.2(i)
[16] *Id.,* s.2(k)
[17] VORONOVA Sofija, "Understanding EU data protection policy." available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651923/EPRS_BRI(2020)651923_EN.pdf
[18] Shawn Marie Boyne, "Data Protection in the United States," 66 *The American Journal of Comparative Law* 299–343 (2018).
[19] *The Digital Personal Data Protection Act, 2023 (Act No. 22 OF 2023)*., s.3

Act.[20]

CONSENT AND NOTICE

The DPDP Act allows the processing of data of the Data principal based on consent and an agreement. The consent of the Data Principal should be given freely, be specific, informed, unconditional, and clear with definitive affirmative action. Further, the processing of data must be limited only to the personal data required for that purpose.[21] Any part of consent that infringes the Act, regulations, or other laws shall be invalid to the extent of such infringement.[22] Such Data Principals have the right to withdraw consent at any time.[23]

Section 5 of the Act delineates procedures related to obtaining consent from Data Principals. Every request for consent under section 6 shall be accompanied or preceded by a notice from the Data Fiduciary to the Data Principal. This notice should include details about the personal data being processed, the purpose of processing, and the mechanisms for the Data Principal to exercise their rights and file complaints.[24] Additionally, Data Principals are given the option to access notice contents in either English or a language mentioned in the Constitution's Eighth Schedule. These provisions aim to ensure transparency, informing individuals about data processing and their rights.[25]

CERTAIN LEGITIMATE USES

As provided in Section 4 of the Act, consent is not needed to process personal data for certain legitimate uses, which are mentioned in Section 7 of the Act. These uses include specified purpose consent, state and other services, legal obligations, compliance with judgments, medical emergencies and treatment, safety and assistance, and employment and safeguarding.

OBLIGATIONS OF DATA FIDUCIARY

Section 8 of the Act provides certain general obligations of the data fiduciary which are as follows-

- A data fiduciary is obliged to comply with the provisions and the rules stipulated by the act, regardless of any contrary agreements or failure of the data principal to carry out his duty.
- A data fiduciary is allowed to appoint, engage, use, or otherwise involve a Data processor to process the personal data on its behalf.
- In processing personal data, one must ensure its completeness, accuracy, and consistency, especially if such processing is to be used for making decisions that affect the data principal or for disclosing personal data to another data fiduciary.
- He must protect personal data in his possession or under its control by implementing reasonable security measures.
- He is required to notify the Data Protection Board and each affected Data Principal in the event of a personal data breach.
- The personal data must be erased when the data principal withdraws consent or the specified purpose is fulfilled and retention is no longer required for legal reasons.

RIGHTS OF DATA PRINCIPAL

The data principal whose data is being processed have the following rights as mentioned in sections 11 to 14. These are-

- The right to receive a summary of personal data and the processing activities carried out by the data fiduciary, to whom consent was previously given, including the identities of any other data fiduciaries and data processors with whom her personal data has been shared, as well as a description of the shared personal data..
- The right to correct, complete, update, or erase her personal data for which she has previously given consent.
- The right to have means of grievance redressal provided by the data fiduciary.
- The right to nominate any other individual to exercise his rights in the event of her death or incapacity.

[20] *Id.,* s.4
[21] *Id.,* s.6(1)
[22] *Id.,* s.6(2)
[23] *Id.,* s.6(4)
[24] *Id.,* s.5(1)
[25] *Id.,* s.5(3)

DUTIES OF DATA PRINCIPAL

Section 15 of the Act outlines specific duties for data fiduciaries, which include:

- To adhere to all applicable laws in India while exercising their rights.
- To refrain from impersonating another while providing personal data.
- To avoid the omission of any material information when providing personal data.
- Not register a false or frivolous grievance or complaint with a data fiduciary or the board.
- • To provide only verifiable and authentic information while exercising the right to correction or erasure.

CROSS-BORDER TRANSFER OF DATA

Section 16 permits the transfer of data outside the territory of India except to restricted countries restricted by the central government through notification. It also requires a high level of protection for the transfer of personal data outside India.

EXEMPTIONS

Section 17(1) gives exemption to the data fiduciary from the obligation given in Chapter II and also does not give the right to data principle in Chapter III. These exemptions are where the processing of personal data is: -

I. Essential for the enforcing any legal rights or claim.
II. Necessary for the execution of any judicial, quasi-judicial, regulatory, or supervisory function.
III. Necessary for the prevention, detection, investigation, or prosecution of any offense or breach.
IV. Related to corporate activities like mergers or financial default assessments.

Other exemptions are given like

I. Certain government bodies may be informed in matters concerning the sovereignty and integrity of India, the security of its states, maintaining amicable relations with foreign nations, ensuring public order, or preventing any recognizable offenses against these interests.
II. Data processing for research, architecture, or statistical purposes is exempt, if it is not used for specific decisions affecting the data principal.

Exemptions from specific provisions may be granted to certain data fiduciaries or classes of data fiduciaries, including startups, through notification.

The state or any of its instrumentalities are exempted from the application of specific provisions related to consent and data processing, which do not affect the data principal.

DATA PROTECTION BOARD OF INDIA

The central government have the authority to establish the Data Protection Board of India consisting chairman and other members having special knowledge or practical experience in the field of data protection, governance, and other fields that may be helpful in data protection, and at least one member among them shall be expert in the field of law.

Powers and functions of the board- section 27 of the Act incorporates the powers and functions of the board. These are as follows: -

- To immediately implement urgent remedial or mitigation measures in the event of a personal data breach and to investigate and impose penalties as necessary.
- While discharging its function board may give the person concerned an opportunity to be heard and its direction shall be binding to such person.
- The board may modify, suspend, withdraw or cancel such direction
- The board may direct parties to a complaint to resolve the dispute through mediation.
- While discharging its function, the board will be a civil court under the Civil Procedure Code, 1908.
- It may require the services of any police officer or any officer to assist it in its function.

No civil court shall have jurisdiction over the matter for which the board is empowered and also court or other authorities could not grant an injunction in respect of any action or to be taken in pursuance of any power under the provisions of this Act.

APPEALS

Any aggrieved person may prefer an appeal against the board's decisions before the appellate tribunal, known as the

Telecom Disputes Settlement and Appellate Tribunal, which was established under section 14 of the Telecom Regulatory Authority of India Act, 1997. The time limit for filing an appeal is sixty days following the receipt of the direction or order. The prescribed time for disposing of the appeal is six months.

CRITICISM OF THE ACT

For many years, various platforms i.e., Data Fiduciaries have been taking the people's data in India without any accountability. The DPDP Act is the first attempt to fix accountability and protect digital personal data. However, there are many loopholes in the provisions of this Act.

I. **LIMITED SCOPE:** The applicability of the DPDP Act is limited, as non-digital personal data is not protected under the Act. There may chance that data is taken in non-digital form and later misused. On the other hand, the GDPR protects personal data on all levels. It protects personal data on all platforms, regardless of the technology used, and applies to manual and automated processing. It also applies regardless of how the data is stored, be it an IT system, paper, or video surveillance.

The DPDP Act excludes from its purview the personal data made publicly available by the data principal or any other person legally obliged to do so. However, it remains unclear if the personal data made public can be used for processing or can be viewed only.

II. **NO CLASSIFICATION OF PERSONAL DATA**

In the DPDP Act, there is no categorization of personal data like in the GDPR where personal data revealing racial or ethnic origin, political opinion, religious or philosophical, sexual orientation, etc. are categorized as “special categories of Personal Data”. Additional protection is given to these sensitive data.

In the previous version of the bill (The Personal Data Protection Bill, 2019) also, there was the classification of personal data as "sensitive personal data" which included such personal data that may reveal or is related to financial data, health data, sex life, sexual orientations, biometric, transgender status, genetic data, religious or political belief or affiliation, etc. There was a provision to obtain explicitly the consent of the data Principal in respect of the processing of any sensitive personal data.

III. **WIDER SCOPE OF EXEMPTION**

The central government may exempt certain data fiduciaries, including startups, from the provisions of sections 5, 10, and 11, without specifying the volume and nature of personal data processed. Additionally, the government has the authority to declare that any provision of this Act may not apply to specified data fiduciaries or classes thereof before the end of five years from the commencement of the Act. This period of five years grants substantial and broad discretionary power for exemption. Furthermore, there are no specified guidelines for granting such exemptions.

IV. **WEAK DATA PROTECTION BOARD**

The DPDP Act 2023, instead of the 2019 bill which proposed for establishment of an independent regulatory agency- the Data Protection Authority (DPA), establishes the Data Protection Board (DPB). The Indian DPA was intended to function independently, akin to EU agencies enforcing the GDPR. It was to have extensive powers, arguably more than EU DPAs, including regulation-making and supervisory roles.

Under the DPDP Act, 2023, the DPB is not a regulatory body. Under the Act, the Central Government has the power to appoint the Data Protection Board of India and its members. Also, the salary, allowances, and other terms and conditions of the chairman and other members shall be such as may be prescribed in rules framed by the Central Government. The term of office of the member of the board shall be only two years and they shall be eligible for re-appointment. Their short term of office and eligibility for re-appointment may affect the board's function as they may be influenced by the power of the central government to get re-appointment.

V. **NO CRIMINAL LIABILITY**

On the breach of the provisions of this Act or rules made thereunder by a person, only a monetary penalty can be imposed. There is no criminal liability under this Act. A mere monetary penalty may not be enough to hold the entities liable in serious data breach cases. The 2018 bill created several criminal offenses. The 2019 bill reduced this to just one—deanonymization.

VI. NO COMPENSATION MECHANISM

The DPDP Act focuses on penalties for breach of any of the provisions of the Act. It does not mention any compensation mechanism for data breach victims. Previously, Section 43A of the Information Technology Act (IT Act) provided compensation for failure to protect sensitive personal data. However, the DPDP Act repeals Section 43A and the rules framed under it.

VII. WEAKEN THE RIGHT TO INFORMATION (RTI) ACT,2005

Another major criticism of the DPDP Act 2023 is that it weakens the RTI Act 2005. Section 44(3) of the DPDP Act amends Section 8 (1) (j) which provides that if a RTI application seeks information related to personal information, there shall be no obligation on a public authority to give information on two grounds, firstly, if the discloser of such information that is not connected to any public activity or interest, or secondly, if it would result in an unwarranted invasion of an individual's privacy unless the appropriate authorities determine that the larger public interest justifies the disclosure of such information. Further, the proviso of the section provides that "the information which cannot be denied to the Parliament or a State Legislature shall not be denied to any person."

The amendment substitutes the clause "information which relates to personal information" in place of Section 8 (1) (j) of the Right to Information Act, 2005. The effect of this amendment is that the personal information of any individual cannot be accessed through the RTI application. The two mentioned grounds, that such information could be disclosed provided it serves a large public interest have been removed.

CONCLUSION

The Digital Personal Data Protection Act represents India's inaugural data protection statute. This novel legislation, marking the first comprehensive law on personal data protection across various sectors in India, has been established following extensive deliberations spanning over half a decade.[26] The Act aims to implement the judgment in the *Justice K.S. Puttaswamy case*. After the judiciary, this is the first attempt on the legislature's part to protect the man's data which is his new castle and make that castle impregnable often.[27] For the first time after the implementation of the Act, users will have a legal framework for the protection of their personal digital data, meeting the increasing demand for privacy and security in the digital era. The focus of the Act on consent, the obligations of data fiduciaries, and the entitlements of data principals highlights a dedication to protecting personal privacy. Whether the regulatory framework the Act provided and the institution it established is effective will be seen after its implementation.

Despite being modest and pragmatic, the critical analysis reveals numerous loopholes in the Act. The Act grants broad exemptions to certain entities and narrows the scope of the Act to digital personal data. The structural and authoritative weaknesses of the Data Protection Board pose significant challenges to the effectiveness of the Act. The Central Government has significant and wide unguided discretion to make rules under the Act.

For better effectiveness of the DPDP Act, it is crucial to consider reforms that address these weaknesses. This includes strengthening the independence and authority of the Data Protection Board, narrowing the scope of exemptions, and introducing robust enforcement mechanisms. Further, the rule to be framed under this Act is also crucial and sophisticated like the method through which digital platforms (Data Fiduciary) will obtain parental consent for processing the data of a child. The quality of data protection under this Act depends on the rule frames set by the Central government. Therefore, the Act's effectiveness relies on the government's commitment to protecting privacy and regulating data fiduciaries.

[26] "Lok Sabha Debates on August 07, 2023" Session Number-XII 785–820 (07-08-2023).
[27] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," 4 *Harvard Law Review* 193–220 (1890).