VOLUME 4 | ISSUE 1

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

# AN ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION BILL 2023

- Sourabh Gupta[1]

## ABSTRACT

In the rapidly evolving global world and the change of trend from everything being accessible just a click away, it becomes equally necessary to protect such personal data, which is being shared and accessed digitally. It is essential to note that India ranks 2nd in data breaches worldwide in 2022. India accounts for 20% of the 2.29 billion data records breached worldwide.[2] The honorable Supreme Court of India has identified the right to privacy as a fundamental right[3]. To secure the rights of individuals related to the protection of personal digital data, India has gone long from setting up committees to presenting bills in Parliament to finally passing the **Protection of Digital Personal Data Bill 2023**. This research paper analyzes the various aspects of the recently passed Protection of Digital Personal Data Bill 2023.

KEYWORDS- Personal data, Right To Privacy, Fundamental Rights, Protection Of Personal Data Bill 2023

## INTRODUCTION

The need for protection of the data goes way long back. From various circumstances, cases, and judgments, the market has been felt time and again to protect digital personal data, as the violation of personal data is a direct infringement on an individual's privacy[4]. Multiple governments have taken various initiatives, such as bringing The Information Technology Amendment Act 2008, which inserted Article 43A and fixed the liability of a company, firm or sole proprietorship that failed to store and protect the data. Still, no particular statute was

[1] Pursuing LLM, Gujarat National Law University
[2] https://www.business-standard.com/article/current-affairs/india-ranks-2nd-in-total-number-of-data-breaches-exposed-in-2022-report-123030100878_1.html
[3] K.S. Puttaswamy and Anr. vs. Union of India 2017 10 SCC 1
[4] K.S. Puttaswamy and Anr. vs. Union of India 2017 10 SCC 1

to exclusively and comprehensively safeguard personal data. Only after the 2017 judgment of the Supreme Court recognizing the right to privacy a committee under Justice BN Srikrishna was set up to make recommendations on digital data protection. After many deliberations and the withdrawal of various bills, The Digital Personal Data Protection Bill 2023 passed in both houses of parliament. It aims at protecting the rights of individuals by protecting their data. It also provides a mechanism to process data only for lawful purposes. Another key feature of the Digital Personal Data Protection Bill is that it extends its jurisdiction outside India.

## NEED FOR DATA PROTECTION IN INDIA

The foremost essential need for data protection is to protect an individual's privacy. The number of internet consumers in India has drastically increased, especially after COVID-19. As the data suggests, there will be 833,710,000 internet users in India in July 2022. [5]As The Right To Privacy has been recognized as a Fundamental Right by a nine-judge bench of the Supreme Court Of India in **KS Puttaswamy And Anr V Union Of India And Ors,**it becomes necessary for the state to protect such right. The internet is a medium that contains abundant personal, sensitive information of an individual, such as bank account details, contact details, details of ATM cards, etc. So it becomes necessary to regulate it so that no loss is made to the personal digital data of an individual.

## BACKGROUND OF THE BILL,

The traces of Data Protection in India go back long before the actual data protection bill was introduced. It was traced in Section 43A of The Information Technology Amendment Act 2008 for the first time[6]. The mentioned section provides for the liability of a company, firm, sole proprietorship, or any association of individuals who fail to protect information from unauthorized access, damage, or use of the sensitive personal data they possess, deal with, or handle. The Justice Srikrishna Committee proposed the Personal Data Protection Bill 2018, which the Ministry of Electronics and Information Technology set up. The committee provided various recommendations, such as the setting up of DPA (Data Protection Authority) and the obligations of fiduciaries, such as registration with DPA. [7] Personal Data Protection Bill 2019 was brought in the Lok Sabha by making certain modifications tothe Personal Data Protection Bill 2018, as proposed by Justice Srikrishna Committee. This bill was referred to

[5] https://www.internetworldstats.com/asia.htm#in
[6] https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf
[7] https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

the Joint Parliamentary Committee (JPC) for recommendation.

Due to the delay caused by the pandemic, the Joint Parliamentary Committee submitted its report after two years in December 2021. The report was accompanied by a new draft bill by the JPC, The Data Protection Bill 2021. The government subsequently withdrew the bill, citing that the draft bill 2021 brings extensive changes to the 2019 proposed bill. In the 2021 bill, 81 amendments were offered, and 12 recommendations were made.[8]

The Digital Data Protection Bill 2023 was introduced in Parliament on August 2023. On August 7, 2023, it was passed in Lok Sabha, and subsequently, on August 9, 2023, the bill was passed in Rajya Sabha.

## OBJECTIVES OF THE BILL

- The foremost objective of the bill is to protect the rights of individuals by protecting their data.[9]
- Another objective of the bill is to process the personal data of individuals, which are stored digitally.[10] To be understood in easy language, the processing of data, put to meaning, denotes transferring the data into a piece of meaningful information.
  It is pertinent to note that such an objective is to be achieved by ensuring that data processing is done only for lawful purposes and connected matters. [11]
- Another unique objective of the bill is related to data processing outside India.[12]
- Another bill objective is establishing the Data Protection Board of India[13].
- The bill makes a provision to resolve the disputes, if possible, through mediation. [14]
- The bill provides for penalty in terms of monetary value in case any person breaches any provision.[15]

## KEY HIGHLIGHTS/FEATURES OF THE BILL

**A. DEFINITIONS:** Before delving into the key highlights/features of the bill, it is necessary to understand and look over specific definitions to understand the account better.

[8] https://www-livelaw-in.gnlu.remotlog.com/top-stories/centre-withdraws-data-protection-bill-from-lok-sabha-205603
[9]Preamble of the bill
[10]Preamble of the bill
[11]Preamble of the bill
[12]Section 16 of the bill
[13]Section 18 of the bill
[14]Section 31 of the bill
[15]Section 33 of the bill

**Data Principal-** It means a person whose data it is. It is pertinent to know that in the case of a child, the data principal also includes her parents or legal guardian. Inthe case of a person with a disability, she also has her lawful guardian.[16]

**A data fiduciary** is a person who processes the personal data of the data principal. It is important to note that the person may process the data alone or concur with others.[17]

**A data processor** is a person who processes data on behalf of or in place of a data fiduciary—for example, service providers, contractors, etc.[18]

**Consent Manager-** This means a person who is a medium between the Data Protection Board of India and the data principal. It must be registered with the board. The purpose of the medium relates to giving, managing, reviewing, or withdrawing consent.[19]

**Person** includes an individual, Hindu undivided family, Company, Firm, Association of persons or body of individuals, State (article 12 of the Indian Constitution)[20], or Artificial person.[21]

B. **APPLICABILITY OF THE BILL**: The bill will apply to the personal data collected in a digital form and even if data is contained in a non-digital form and is subsequently digitized. The statement also applies to any collection of personal data in digital format if the data relates to offers of goods and services to the data principal in India.[22]

C. **NON-APPLICABILITY OF THE BILL:** The bill doesn't apply if the data is processed by any individual for personal or domestic purposes. The statement also doesn't apply in scenarios where the data is made public by the data principal himself.

[16]Section 2(j) of the bill
[17]Section 2(I) of the bill
[18] Section 2(k) of the bill
[19]Section 2(g) of the bill
[20]Section 2(zb)of the bill
[21]Section 2(s) of the bill
[22]Section 3 of the bill

Also, the information would not apply in systems where the data is made public by a person who is under an obligation by law to make available such data in public.[23]

**D. PROCESSING OF PERSONAL DATA:** A data fiduciary can process the personal data of a data principal only by way of her **consent**. [24]

It is necessary to note that the support of the data principal must be free and clear in terms. It must not be ambiguous.[25] The license that the data fiduciary requests must be asked in clear and plain language. [26] The data principal has the right to consent through the consent manager[27]. It is necessary to note that at the time of the request for consent of the data principal or before requesting the permission of the data principal, a **notice** must be served upon the data principal.[28]The information shall contain the details related to the personal data for which the data principal has asked the consent to process it. It must also state the purpose for the processing of personal digital data.[29] It is important to note that the data principal can **withdraw her consent** at any time. The data principal can remove the permission through the consent manager.[30] After the data principal starts the support, the fiduciary must cease processing the personal digital data of the data principal. [31]

- It is not always necessary that the consent of the data principal is mandatory for the processing of the personal digital data of the data principal. The personal digital data of the principal can be processed without her consent when the data is to be processed for **legitimate uses**.[32]These legitimate uses are:
- In case the data principal has provided the personal data to the data fiduciary for a specific purpose, the fiduciary has no obligation to take consent before processing such data. But,data processing must be done for the particular purpose only for which the data principal has provided the details.[33]
- In the case where the data is to be processed for the state or any of its instrumentalities for the purpose relating to grant or issue of subsidy, service, certificate, license, etc., by the

[23]Section 3 of the bill
[24]Section 4(1)(a) of the bill
[25]Section 6(1) of the bill
[26]Section 6(3) of the bill
[27]Section 6(7) of the bill
[28]Section 5(1) of the bill
[29]Section 5(1)(i) of the bill
[30]Section 6(7) of the bill
[31]Section 6(6) of the bill
[32]Section 4(1)(a) of the bill
[33]Section 7(a) of the bill

state or any of its instrumentalities AND the data principal has previously consented for avail of such grant or issue, in such a scenario, no consent of data principal is required. [34]

- In the case where the data is processed for the state or its instrumentalities about the sovereignty and integrity of the nation, in such a scenario, no consent of the data principal is required.[35]
- In case the data is processed for fulfilling any obligation under any law in India, in such a scenario, consent of the data principal is unnecessary. [36]
- In case the data fiduciary needs to process the data to comply with any judgment, decree, or order of any court or tribunal in India or outside India. In such a scenario, consent of the data principal is not required.[37]
- In a scenario where it becomes necessary for the data fiduciary to process the personal digital data of the data principal because of a threat to the life or health of the data principal or any other individual, in such a scenario, the data fiduciary is not obliged to request for consent of the data principal[38]
- In cases where the processing of personal digital data relates to providing medical treatment in times of epidemic, outbreak of disease, or any threat to public health, in such situations, the consent of the data principal is not essential.[39]
- In situations where it is necessary to process personal digital data to ensure the safety of individuals in case of disaster or public outbreak, in such scenarios, the consent of the data principal is immaterial.[40]
- In case it is necessary to process the personal digital data of the data principal to safeguard the employer from any loss or liability, in such scenarios, consent of the data principal is immaterial. For example, the processing of data to prevent unpublished price-sensitive information/UPSI.[41]

**E. RIGHTS OF DATA PRINCIPAL:** The data principal has various rights. The data principal has the right to ask for the details and summary of data that the data fiduciary is processing. Data fiduciaries may have shared the personal digital data of the

[34]Section 7(b)(i) of the bill
[35]Section 7(c) of the bill
[36]Section 7(d) of the bill
[37]Section 7(e) of the bill
[38]Section 7(f) of the bill
[39]Section 7(g) of the bill
[40]Section 7(h) of the bill
[41]Section 7(i) of the bill

principal with other data fiduciaries. The data principal has the right to know the details of other data fiduciaries with whom the data fiduciary has shared his data.[42] The data principal can modify, erase, correct, or complete her digital data.[43] In case the data principal has any grievance, it is the right and duty of the data fiduciary or consent manager to provide a readily available grievance mechanism. [44] The data principal has the right to appoint any individual as his nominee to exercise the rights of the data principle in case of failure to exercise such freedom due to death or incapacity.[45]

**F. EXEMPTIONS:** The provisions mentioned above do not apply in specific scenarios. These situations are:

- A court tribunal processes the data or quasi-judicial authority, and such processing of personal digital data is necessary to function such organs.[46]
- The data is processed to prevent, detect, or investigate any crime. [47]
- In case there has been a default on the part of a person on account of a loan or advance he has taken from a financial institution, in such a scenario, determine the financial information, such as assets and liabilities of the defaulter.[48]
- In case the personal data of an individual is processed by instrumentalities of the state which are authorized for such processing in the interest of sovereignty and integrity of India, to maintain friendly relations with foreign states and to maintain public order and peace, in such scenarios the provisions mentioned above would not apply.[49]

**G. DATA PROTECTION BOARD OF INDIA:** The act provides for establishing a board called the Data Protection Board of India to perform various functions enshrined and provided in the front.[50] The board is empowered to proceed with any inquiry if a complaint is made.[51] The board can inquire into any complaint received by the data principal regarding the data fiduciary's breach of personal digital data and

[42]Section 11(1)(b) of the bill
[43]Section 12(1) of the bill
[44]Section 13(1) of the bill
[45]Section 14(1) of the bill
[46]Section 17(1)(b) of the bill
[47]Section 17(1)(c) of the bill
[48]Section 17(1)(f) of the bill
[49]Section 17(2)(a) of the bill
[50]Section 18(1) of the bill
[51]Section 28(5) of the bill

can impose penalties too.[52] In situations where the data fiduciary possesses the personal digital data of the data principal and a violation of data is made during the possession of the data fiduciary, the board can direct urgent measures to safeguard the rights of the data principal and impose penalties as provided in the act.[53]

**H. APPEAL AND ALTERNATE DISPUTE RESOLUTION:** The act provides a mechanism for an appeal if a person is aggrieved by an order made by the Data Protection Board of India. The request can be filed in the Telecom Disputes Settlement and Appellate Tribunal. [54] It is necessary on the part of the aggrieved party that the appeal must be filed within sixty days from the date on which the board made the order.[55] It is the discretion of the appellate authority that it can allow an appeal even after the expiry of the mandated sixty-day period if the source is satisfied that the applicant or the appellant had sufficient reasons for not being able to appeal within the stipulated period of sixty days.[56] It is necessary on the part of the tribunal to hear both parties before making any order. [57] The order passed by the appellate tribunal is executable as a decree of the civil court. [58] The court is at its discretion to recommend parties to solve the disputes through mediation, wherever possible.[59]

**I. PENALTIES:** The act provides various penalties for the breach of provisions of the show or rules made under the authority of the action. The penalty ranges from 10,000 to 250 crores. [60] It is pertinent to note that the act provides for only penalties in terms of monetary value[61]. It is obligatory on the part of the authority to consider specific matters such as the nature of the breach, the heart of the data that has been breached, the loss incurred due to the violation of personal data, and any other considerations which the board authority deems necessary and proper[62]. All the penalties collected under the act will be deposited into the Consolidated Fund of India.[63]

[52]Section 27(1)(b) of the bill
[53]Section 27 (1)(a) of the bill
[54]Sections 2(a) and 29(1) of the bill
[55]Section 29(2) of the bill
[56]Section 29(3) of the bill
[57]Section 29(4) of the bill
[58]Section 30(1) of the bill
[59]Section 31 of the bill
[60]Schedule of the bill
[61]Section 33(1) of the bill
[62]Section 33(2) of the bill
[63]Section 34 of the bill

J. **VIEWS OF THE AUTHOR:** The very basis for protecting personal digital data was emphasized in Justice KS Puttaswamy's case. [64] In this case, much emphasis was given to the term **informational privacy**. Defining informational privacy and terming it as a part of the right to privacy, Justice Nariman wrote

*"521. In the Indian context, a fundamental right to privacy would cover at least the following three aspects: • Privacy that involves the person,i.e., when there is some invasion by the State of a person's rights relatable to his physical body, such as the right to move freely; • Informational privacy which does not deal with a person's body but deals with a person's mind, and therefore recognizes that an individual may have control over the dissemination of material that is personal to him. Unauthorized use of such information may, therefore, lead to infringement of this right; and • The privacy of choice, which protects an individual's autonomy over fundamental personal choices."*

However, the newly passed bill has no mention or regard for informational privacy.

The second observation of the author is that the central government and instrumentalities of the central government are fettered with excessive powers and control over the processing of digital personal data. In certain situations, such as maintaining the sovereignty and integrity of the country and maintaining friendly relations with other nations, the central government is exempted. It can exempt any instrumentalities belonging to it about specific provisions, such as the consent of the data principal before processing the data. In the past few years, there has been an extraordinary allegation against central agencies such as CBI, ED, and NIA for using excessive powers and undermining the rights of persons. So, to provide exemptions to these instruments of the central government creates a trust deficit between the people and society at large, and the very intention behind the bill is liable to be defeated.

The third observation of the author is related to the hefty amount of penalties. The bill provides for a significant amount of fines ranging from 250 crores. Unlike the personal data protection bill of 2019, the bill offers no criminal liability, which provides for imprisonment of a term not exceeding three years. [65] However, if the data fiduciary commits a grave breach but is not in a financial position to pay the fine, the purpose of imposing fines would be defeated. Also, the fear of criminal liability plays a significant role in deterring the offense.

The fourth and final observation of the author relates to the cross-border transfer of data. This current era is an era of a globalizing world. It is impossible to restrict the data within the

[64] K.S. Puttaswamy and Anr. vs. Union of India 2017 10 SCC 1

[65] Section 82(1)(b) of the personal data protection bill 2019

jurisdictional limit of a particular nation. It is a click away to transfer data around the globe. It is sad to know that the bill is silent about cross-border transfers. The Digital Personal Data Protection Bill 2019 had relevant provisions regulating cross-border data transfer. In the 2019 bill, the data protection authority could manage cross-border data transfer.[66]

**H. CONCLUSION:** The necessity to have a comprehensive law on the safety and security of personal data protection bills has finally been achieved. The bill comprehensively defines all the terms and is not restricted to natural persons only. The statement is clear on how the data has to be processed and the obligations attached to the data fiduciaries relating to the data it holds. The act equally imposes certain obligations upon the data principal. The show's highlight is the establishment of the Data Protection Board of India. To read the bill by its judgment, it nevertheless is a bill that serves the need and essential purpose for which the bill is introduced. But the only trust deficit lies in the contention of powers fettered upon the central government and its agencies. It is necessary on the part of them to apply the bill fairly and reasonably. The statement shall be used to them in letter and spirit of the law to fulfil the cause of the bill for which it was introduced,i.e., personal data protection.

[66]Section 49(2)(g) of the personal data protection bill 2019