Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rishikesh Dave; Publisher – Ayush Pandey

Critical Analysis: Digital Personal Data Protection Bill 2022

Aditya Bashambu[a] & Lavanya Chetwani[b]

[a]National Law University, Odisha, India [b]National Law University, Odisha, India

Received 10 December 2022; *Accepted* 16 December 2022; *Published* 24 December 2022

Data Privacy has become a point for discussion post the digitization of the economy and surge in the utility of digital devices in one's daily life as lack of access control on crucial data of individuals can potentially expose them to fraud and identity theft. Governmental data breaches have the potential to put national security at risk. This topic needs a lot of deliberation as well as legislation that sets rules and regulations for preventing its misuse and maintaining "digital sovereignty." For these different countries implemented different regulations such as the California Consumer Privacy Act (CCPA), the General Data Protection Regulations (GDPR) of the European Union, and so on. Through this article we have made an effort to discuss the background of the Personal Data Protection Bill 2019 initiated in India to maintain the data privacy of Nagriks, further we dived down to why there was a need for new data protection legislation and discussed the newly introduced "Digital Personal Data Protection Bill 2022". The paper concludes with a critical analysis of the provisions of the above-mentioned bill discussing the welcomed changes that were the need of the hour as well as some provisions which need some overhauling as well as some finishing touches due to some lacunas spotted.

Keywords: *data principals, data fiduciaries, privacy, consent.*

INTRODUCTION

Nowadays the utility of digital devices and technology for executing various mundane activities has increased manifold. A new economy known as the "Digital Economy" has been carved out seeing the utility of digital technology in day-to-day activities. Digital Economy refers to the usage of information technology to carry out the creation, adaptation, market, or consumption of various goods and services. Indian Government, as well as the Reserve Bank of India, has launched numerous initiatives like Digital India, the launch of e-RUPI, and so on for enhancing the digitization of the Indian Economy. India has a gigantic consumer base as well as a producer base of data per capita among countries. Over the coming years, the amount of active internet users in India has been estimated to touch the figure of 120 crores (1.2 billion). It is quite evident on one hand that the utility of the internet and digital technology has enhanced efficiency as well as effectiveness in our economy but it is prone to various exploitation which may put the data of citizens in a vulnerable state.

This brings out the necessity of rules and laws for the internet to make it accountable as well as meet the belief of citizens who are trustworthy, accountable, and transparent. Digital data is the fundamental essential required in a fast-growing economy. This data is employed for usage by various intermediaries therefore it is quite essential to establish a framework of rules for data and personal data to prevent the misuse of personal data which can jeopardize the privacy of the citizen. So, it becomes quite onerous for the government to frame some rules and regulations to maintain digital sovereignty and ensure the privacy of personal data given by Nagriks to various platforms for the operation of a specific purpose. This eventually led to the creation of a bill by The Ministry of Electronics and Information Technology about the protection of the individual data of Nagriks to maintain 'digital sovereignty as well as the privacy of the Nagriks of the state.

BACKGROUND

The deliberation on the grave issue of privacy kicked off in 2012 when retired Justice AP Shah chaired the committee of the Planning Commission on issues related to privacy. Later, The

Ministry of Electronics and Information Technology established a committee to investigate the issues in connection to data protection in 2017 post the famous verdict of the Puttaswamy case. Justice B.N. Srikrishna, a renowned former Supreme Court justice, served as the committee's head. After much discussion, the committee presented the draft Personal Data Protection Bill, 2018 in the next coming year, which is 2018. Mr. Ravi Shankar Prasad, the Minister of Electronics and Information Technology, then presented the submitted draft as the Personal Data Protection Bill 2019 in the Indian Parliament. On August 4, 2022, the Government of India repealed the bill, claiming that it urgently needed a thorough legal framework, as suggested by the Joint Committee of Parliament (JCP), to regulate internet space. Laws on topics like cyber security, the Internet ecosystem, telecom rules, and data privacy also urgently needed to be introduced. The government received a lot of criticism for the current Data Protection Bill from a variety of stakeholders, including certain Big Tech firms like Google and Facebook and different privacy advocates. The previous bill was also opposed on the ground that it required a lot of compliance, which made it difficult for start-ups to comply with the listed provisions.[1]

DIGITAL PERSONAL DATA PROTECTION BILL 2022

The newly introduced Digital Personal Data Protection bill is legislation that outlined various rights as well as duties vested for citizens (Digital Nagrik) and also the obligations of the various data fiduciaries during the purpose of collection of data from Digital Nagriks. The objective of this bill is to establish regulations for the processing of digital personal data in a way that respects people's right to privacy, the necessity to process personal data for legal purposes, and any incidental uses. These incidental intents comprise the framework for abiding by Bill's provisions.

[1] Soumyarendra Barik, 'Explained: Why the Govt has withdrawn the Personal Data Protection Bill, and what happens now' (*The Indian Express*, 6 August 2022) <https://indianexpress.com/article/explained/explained-sci-tech/personal-data-protection-bill-withdrawal-reason-impact-explained-8070495/> accessed 06 December 2022

The bill is framed taking into account the following principles:

- The personal data of Nagriks employed to use by various fiduciaries as well as platforms must be done in a manner permissible in law. It should maintain fairness as well as transparency of the Nagrik connected.
- The principle of purpose limitation wherein the collected data must be used for the reason it was obtained for.
- The principle of data minimization wherein only that crux of personal data should be collected is essential for the fulfillment of a specific purpose.
- The principle of accurateness of personal data wherein effort should make to keep the personal data of Nagrik updated as well ensures the accuracy of the same.
- The principle of storage limitation wherein the personal data of Nagrik should not be stockpiled eternally by default. It should be limited to the time frame as is necessary for the operation of the specific purpose for which the data was collected.
- There should be no collection as well as the processing of personal data that is made illicit or unauthorized by the law. Reasonable safeguards should be undertaken for the fulfillment of the same.
- The principle of accountability wherein there should be the existence of accountability of the person who decided the purpose as well as the method of such processing of personal data.

All the processing of personal data that is carried out with digital means is under the ambit of DPBP Bill 2022. All personal data which is collected online as well as offline provided that the offline data collected is processed digitally will fall under the ambit of the aforementioned bill. This bill has completely excluded the manually processed data outside its ambit. The processing of personal data collected by data fiduciaries within the territory of India as well as which is used to provide goods and services within India fall under the territorial jurisdiction of the bill.[2]

[2] Trishee Goyal, 'A first look at the new data protection Bill' (*The Hindu*, 20 November 2022) <https://www.thehindu.com/sci-tech/technology/a-first-look-at-the-new-data-protection-bill/article66162209.ece> accessed 06 December 2022

WHY THERE WAS AN IMPERATIVE NEED FOR A REVAMPED DATA PROTECTION BILL?

1. Technology Advancement

There has been a manifold increment in the generation of personal data constantly by users (Data principals) due to an increase in the utility of digital devices in mundane day-to-day activities. This evident increment in the generation of personal data is accompanied by the technological advancement of companies (data fiduciaries). This collected data can be refined in a manner that can harm the autonomy, identity as well as prime privacy of the data principal. This brings out a need of a well up to dated data protection norms.

2. Ineffectiveness of Information Technology Rules, 2011 (IT Rules, 2011)

The presently enforced IT Rules, 2011 are ineffectual to prevent the misuse of personal data of data principals and curb the harm caused to them on many grounds. Firstly, the extant framework of the aforementioned rules depends upon the presumption that privacy is a statutory right instead of a fundamental right which is in direct contravention to the K.S. Puttaswamy v Union of India (2017) [3]verdict due to which processing of personal data by government institutions or organizations fall outside the ambit of these rules. Secondly, it is unable to comprehend different kinds of data that need to be protected.

Moreover, the obligation imposed on data fiduciaries is quite meagre which can be overpowered by any existence of a contract. Last but not least the consequences for any breach done by a data fiduciary are quite minimal and trifle. It is quite imperative to fix the obligations vested on data fiduciaries backed with any retributive action when they engage in any illicit practice which is forbidden under the law. [4]Apart from the above-mentioned reasons the joint parliamentary committee dealing with the PDP Bill also asserted the imperative need for various amendments and proposals that needs to be accommodated in the previously drafted bill related to data

[3] *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1
[4] Trishee Goyal, 'A first look at the new data protection Bill' (*The Hindu*, 20 November 2022) <https://www.thehindu.com/sci-tech/technology/a-first-look-at-the-new-data-protection-bill/article66162209.ece> accessed 06 December 2022

protection to make it more effectual and curb the menace of exploitation of personal data of data principals.

ANALYSIS OF DIGITAL PERSONAL DATA PROTECTION BILL 2022

The article aims to critically analyze the newly introduced Digital Personal Data Protection Bill 2022 reflecting some commendable changes made in the bill which were the need of the hour and were missing in the previously introduced bill about the protection of personal data of data principals accompanied with provisions which need some overhauls for finishing touches and the lacunas in the same.

POSITIVE CHANGES IN DIGITAL PERSONAL DATA PROTECTION BILL 2022

1. Addition of Right to Post mortem privacy

The above-mentioned bill contains a set of rights provided to data principals accompanied by the obligations of the data fiduciaries handling the personal data of the data principal personal information. In the newly introduced bill, there has been an addition of one more right for data principals known as the Right to Post Mortem Privacy[5]. This right was endorsed by the Joint Parliamentary Committee related to data issues and was missing in the previously introduced PDP Bill 2019. The said right provides a means which allows the data principal to nominate another person in case of incapacity or death. Herein, "Incapacity" explicitly means the inability to exercise the vested rights due to the debilitation of the mind or body. On whole, it provided the power in the hands of the data principal to nominate another person so that the nominee may exercise the right of the data principal provided in the provisions of this bill.

2. Allowance of cross-border data flow

The previously introduced bill on data protection was condemned by various Big Tech Companies as it advocated the concept of data localization which made it tedious for the said companies to transfer the collected data of data principals outside India for the performance of

[5] *Ibid*

specific purposes. A big tech firm "Meta" condemned the provision of data localization as it increased the cost factor as well as made it difficult for the said companies to provide services in India. The PDP Bill 2019 laid down a three-tiered categorization based on which the transfer of personal data across the territory of India could be carried out. PDP Bill 2019 laid down that sensitive personal data ("SPDI") may be transferred provided such sensitive personal data continues to be stored in India whereas, in the case of critical personal data, it can only be processed in India, not outside India. [6]The bill provides the explicit right to the government to include all foreign and Indian Companies under the preview of data localization by citing reasons like national security, privacy, employment generation, and so on.

But the newly introduced Digital Personal Data Protection Bill 2022 has inducted a special provision for the transfer of personal data of data principals outside India under Chapter 4 named "Special Provisions". After taking into account several variables, a data fiduciary may now only communicate the personal data of data principals to countries or regions outside of India at the Central Government's discretion in line with the terms laid forth in the law. Overall, the new bill has permitted the transfer of personal data across international borders as long as it complies with its requirements.

3. Ease of compliance burden on Start-ups

The previously introduced PDP Bill 2019 was criticized by various start-ups as it was quite a compliance intensive which made it cumbersome for start-ups to provide services and obey the rules set out in the legislation. The provision of data localization outlined in the PDP Bill 2019 was the main point of disagreement for the start-ups. The start-ups asserted that their business included the operation of various digital tools and software based outside India which needed to access the core database to provide services. Another contention made by start-ups was

[6] Anind Thomas & Sherien Kaul, 'Data Localisation and the Personal Data Protection Bill, 2019' (*AZB & Partners*, 10 November 2022) <https://www.azbpartners.com/bank/data-localisation-and-the-personal-data-protection-bill-2019/> accessed 07 December 2022

regarding handling customers based outside India, they asserted that the data localization clause made it inconvenient for them to provide services to international customers. [7]

This was one of the prime reasons for the revoking of the PDP Bill 2019. Even the Minister of State of Electronics and Information Technology Rajeev Chandrasekhar argued that the burden of the data protection bill would have hurt start-ups. [8]The induction of the Digital Personal Data Protection Bill has lessened the compliance burden on start-ups.

4. Introduction of hefty penalties

The newly introduced Digital Personal Data Protection Bill has made some commendable changes in terms of penalties that can be levied in case of non-compliance of data fiduciaries observed by the data protection board. The quantum of penalties that can be imposed by the aforementioned board has been increased to Rs 500 crore which is of higher magnitude as compared to penalties imposed under PDP Bill 2019.[9]

In case of failure to observe reasonable safeguards to prevent the misuse of personal data of data principals by the data fiduciary, a penalty of Rs200 crore could be imposed on the same under the new draft. The earlier version of the bill provides a provision for the imposition of a penalty of 4 percent or Rs 15 crore of the company's annual turnover for the same offence. [10] On whole, the newly revised bill has increased the quantum of penalties that can be imposed on companies. This surge in penalties may make a deterrent effect on companies.

---

[7] Astha Oriel, 'Why Indian start-Ups Are Happy About Personal Data Protection Data Protection Bill Being Scrapped' (*Outlook India*, 7 August 2022) < https://www.outlookindia.com/business/data-protection-bill-withdrawn-why-indian-start-ups-are-happy-about-personal-data-protection-bill-being-scrapped-news-214620> accessed 07 December 2022

[8] Hemant Kashyap, 'Burden of Data Protection Bill would have Hurt Start-ups: Rajeev Chandrashekhar' (*Inc 42*, 4 August 2022) <https://inc42.com/buzz/burden-of-data-protection-bill-would-have-hurt-startups-rajeev-chandrasekhar/> accessed 07 December 2022

[9] Trishee Goyal, 'How different is the new data protection bill?' (The Hindu, 21 November 2022) <https://www.thehindu.com/sci-tech/technology/how-different-is-the-new-data-protection-bill/article66166438.ece> accessed 06 December 2022

[10] 'Personal Data Protection Bill: What's New in the Revised Draft and What It Means for You?' (*Outlook India*, 17 November 2022) <https://www.outlookindia.com/business/what-is-personal-data-protection-bill-what-s-new-in-the-revised-draft-of-data-protection-bill-and-what-it-means-for-you--news-238163> accessed 06 December 2022

MAJOR FLAWS IN THE BILL

No framework for the protection of 'sensitive personal data: The data protection bill that existed before, that is 'The Personal Data Protection Bill, 2019' categorized certain personal information as sensitive personal data or critical personal data. Chapter I Clause 3(36) of the bill defined what constitutes sensitive personal data. It includes that data which may relate to the Data Principal's financial data, sexual orientation, biometrics, genetic data, health data, intersex status, political and religious affiliations, etc. This differentiation between the two is dropped in the draft of the new bill. This suggests that all types of data are included under the "Personal Data" umbrella only. It highlights the lack of higher standards of guidelines and regulations for the protection of sensitive and critical personal data.

The issue of 'Deemed Consent": Chapter II Clause 8 of the draft of the Digital Personal Data Protection Bill, 2022 explains the theory of 'deemed consent'. It gives certain grounds where consent of the Data Principal is an assumed one and not explicit. It includes where the Data Principal voluntarily gives his data for the performance of any function under the provisions of any law, for compliance with any judgment or order issued under the law, for taking measures to provide medical treatment to himself or another individual, for purposes related to employment and also for purposes in the public interest. As a result, the measure makes it equally convenient for state agencies and private businesses to acquire personal information on the premise of implied consent. As a result, it makes it more likely that data may be used for improper reasons. The law is unclear as to whether the Data Principal can cancel such implied consent, in which case the Data Fiduciary must cease processing the personal data. Additionally, the measure says nothing about how this permission may be withdrawn.

Removal of the 'Data Localization' mandate: The new bill has not only removed the previous categorization of personal data but has also not mentioned the concept of data localization which existed in the previous bill. The previous bill provided for a three-tier classification system for moving personal data across borders. The aim of the government in limiting the flow of sensitive

or critical personal data was to maintain "digital sovereignty". [11]The new bill would allow data transfer and storage only to "trusted geographies" which means cross-border data sharing would be allowed only to the countries and territories notified by the Union government. This would be a positive change for big-tech companies, suggesting the direction of the bill to be pro-business. But which countries will be included in this remains unclear along with the grounds on which this selection will be based. Therefore, providing wide-ranging powers to the government. Additionally, the bill does not provide any framework for such data transfers.

Composition and Powers of the Data Protection Board: Chapter 5 Clause 19 of the bill makes 'The Data Protection Board of India' responsible for enforcing the provisions of this bill. The bill stays silent on the composition of this Board. The members of the Board and the Chairperson will be nominated by the Central Government. Hence, the Ministry of Electronics and Information technology will have direct supervision over the Board. This raises concern about the independence of the Board. One of the biggest data fiduciaries in the nation is the government. It handles the personal information of millions of Indians to provide services and benefits, issue licenses, permits, and official identification, as well as for general law enforcement purposes. As a result, it is crucial that the institution responsible for creating the regulations be independent of the government to guarantee the fair protection of data principals' interests. Additionally, the Board lacks Suo moto authority and may only rule on a breach of data privacy if it receives a complaint. Some other powers of the Board might be overlapping with the CERT (Computer Emergency Response Team) which is responsible for protection against cybersecurity incidents.

Offline and non-automated Personal Data not included in the Bill: Clause 4 (3) states that the provisions of this Act will not pertain to offline personal data, non-automated personal data, personal data processed by an individual for domestic purposes, etc. Because of this, a lot of important personal data remains unregulated. Not including offline and non-automated data may result in the breach of privacy of a customer. For example, citizens' personal information is also being collected in restaurants and shopping centres, including vital details like contact

[11] Trishee Goyal (n 12)

information, name, and age. The railway employee who is asking for the review of the food may also ask for a contact number, and email id in the feedback form. In the above daily examples, it is important to note that the entity collecting such personal data in an offline mode has no use for it. Excluding such data from the provisions of the bill may result in the unlawful use of the personal data of a citizen.

Age of consent still 18: Additional obligation has been imposed by the bill on the Data Fiduciaries for processing the personal data of children. It includes taking the verifiable consent of the child's parents or legal guardians before the processing of the data. The purpose for which the data is used should also be known to the parents or legal guardians. It is undeniable that the proposed provisions would have a significant impact on data fiduciaries given that a significant portion of internet users in India are under the age of 18. This threshold has been criticized for not being in line with global standards as it is too high. It is noteworthy that the bill recognizes the personal data of children as a special category and holds data fiduciaries accountable for how it is processed. This will also affect the gaming industry because the bill simply prohibits processing personal data in a way that is 'likely to harm' children without actually defining what constitutes a way that is likely to harm or damage the children. This vague provision raises questions on how the intended outcome is supposed to be achieved.

Ignorance of the Puttaswamy judgment (wide exemptions provided to the Government): The Supreme Court in Justice K.S. Puttaswamy (Retd) v Union of India[12] laid down a triple test system to ensure the right to privacy of citizens. It says that any invasion of privacy by state or non-state actors must necessarily pass the test. It includes 'necessity', 'reasonability', and 'proportionality'. The bill ignores the judgment. This can be noticed in Clause 18 of the draft. By its terms, the central government may exempt any government authority from its application by issuing a simple statement declaring that it was done for reasons such as public order, national security, etc. The bill has also not defined these terms clearly. This standard is lower than the one established by the privacy judgment. In addition, by evaluating the quantity and type of personal data, the government can now even exempt entities from the private sector,

[12] *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1

such as specific businesses or a class of them. Clause 18(4) further exempts any state authority from the requirement to delete data after use, allowing them to effectively hold personal data indefinitely in violation of the idea of purpose limitation and storage limitation. On top of this, the government is also given automated exemption in cases of prevention, investigation, etc. of crime where it can process personal data without even notifying. This provision is thus faulty because it would allow—nay, encourage—the administration to act arbitrarily and violate the fundamental right to the privacy of personal information.

Amendment to the RTI Act: The draft bill aims to amend Section 8.1(j) of the Right to Information Act, 2005 so that an RTI applicant's request for the disclosure of personal information may be rejected (irrespective of it being in the larger public interest). [13]Since the majority of the information that may be requested in an RTI application can be outright rejected because it falls under "personal information," such an absolute taking away of reasonable caveats permitted under the RTI Act has the potential to be misused and weaken the significance of RTI. This clause raises the risk of abuse by the government as it can deny revealing important information to the public.

No defined timelines: The bill imposes few obligations on the Data Fiduciaries but has not mentioned any timeframe within which the data fiduciary has to perform such obligation. According to the bill, The Data Principal's permission to the processing of personal data cannot be irrevocable or permanent. She can withdraw consent anytime and the Data Fiduciary will be obligated to delete the data once the consent has been withdrawn. But there is a lack of a deadline for such deletion[14]. Similarly, there is no deadline as to when the Data Fiduciary has to delete the personal data after its purpose has been served. Additionally, no time limit has been prescribed in Chapter 5 of the draft for the Data Protection Board to adjudicate on a matter.

---

[13] Manu Sebastian, 'Digital Personal Data Protection Bill Proposes to Amend RTI Act to Completely bar disclosure of Personal Information' (*Live Law*, 20 November 2022) <https://www.livelaw.in/news-updates/digital-personal-data-protection-bill-proposes-to-amend-rti-act-to-completely-bar-disclosure-of-personal-information-214573> accessed 07 December 2022

[14] Rohan Krishna Seth, 'Analysis of the Draft Digital Personal Data Protection Bill, 2022' (*Bar and Bench*, 26 November 2022) < https://www.barandbench.com/columns/analysis-of-the-draft-digital-personal-data-protection-bill-2022 > accessed 5 December 2022

Broad definition of public interest: The wide definition of "public interest" used in the draft bill to recognize "deemed consent" is one of the main issues in the bill. Clause 8(8) of the draft mentions that public interest includes: prevention and detection of fraud, credit scoring, search engine optimization, etc. Such a wide and vague definition of this important term may prove to be a disadvantage for the Data Principals as it gives a wide gamut of rights to the Data Fiduciaries wherein, they can assume consent.

Delegated Legislation: Delegated legislation refers to the situation where the Parliament delegates its law-making powers to the Executive due to paucity of time and various other prominent reasons. This is one of the major problems with the bill. A large number of the provisions of the bill contain a clause that states "as may be recommended" or its equivalence[15]. This provides the government with the authority to impose rules and regulations in the future. The aforementioned structure provides absolute power to the Indian Executive organ to rule arbitrarily and to perform the law-making powers under the provisions of the bill without any guidance from the legislature. There is thus dependent on the Executive and it might start working capriciously and the objectives of the bill might not be achieved.

Significant Data Fiduciaries: The bill has also introduced the concept of 'significant data fiduciaries' in Clause 11 of the draft. It is defined as the entity that decides the purpose and means of the processing of the personal data of an individual[16]. She is further empowered to nominate a Data Protection Officer who shall act for him and an Independent Data Auditor whose duty is to evaluate the compliance of the Significant Data Fiduciary with the provisions of the bill. But the power to appoint the Significant Data Fiduciary is vested with the government. The basis for this appointment can be the volume and sensitivity of personal data processes, public order, security of the State, etc. Thus, the government is given wide powers of

[15] Sarvesh Mittal, 'Twelve major Concerns with India's Data Protection Bill, 2022' (*Medianama*, 19 November 2022) <https://www.medianama.com/2022/11/223-twelve-major-issues-data-protection-bill-2022/> accessed 6 December 2022

[16] Varsha Rajesh, Tanisha Khanna, Aparna Guar & Gowree Gokhale, 'Digital Personal Data Protection Bill, 2022: Analysis and potential impact on business' (*Nishith Desai Associates*, 24 November 2022) <https://www.nishithdesai.com/NewsDetails/8453> accessed 07 December 2022

appointment. Thus, the chances of the Significant Data Fiduciary and officers appointed by her, becoming the puppets of the government rise.

Missing rights of the Data Principal: The draft of the new bill has not mentioned two crucial rights which were provided to the Data Principals. The right to data portability is the first. This right allows the Data Principal to receive from the Data Fiduciary the data that she had provided along with the data that the Fiduciary had generated during the rendering of services. This increases the consumer welfare of the Data Principals as it enables them to choose the best platform among the available options. For example, the Data Principal can transport his data from one social media platform to another if she is unhappy with its services and she will not have to provide all the personal data again to the new platform. This user right has not been incorporated into the new bill.

The right to be forgotten is the second right that is forfeited. Although not a core right, the aforementioned right enables the data principal to request the data fiduciary to stop disclosing their personal information. This right is incorporated into the right to erasure by the bill. The freedom of speech and expression of other people is compromised by the confusion between the general right to erasure and the right to be forgotten, which is restricted to the revealing of personal data. The right to information for everyone else and the freedom of speech and expression must be balanced with this[17].

CONCLUSION

With the help of good policies and technological advancements, India's digital infrastructure is getting better day by day and is finally taking shape. With 760 million active internet users (Digital Nagriks), India is rapidly transitioning towards a "digital-first economy". In this highly digitalized environment, the personal data of millions of people is also stored online on various platforms. This can also include very crucial personal data like sexual orientation, bank details, financial data, etc. Thus, it becomes the paramount duty of the government to protect such data from misuse. To serve this purpose the Ministry of Electronic and Information Technology, on

[17] Trishee Goyal (n 12)

November 18, 2022, the new Digital Personal Data Protection Bill draught was published. This bill replaces the previous Personal Data Protection Bill 2019. After critically analyzing all the aspects of the aforementioned bill in the above article, we conclude that despite its promising features, it needs refinement.

The key highlights of the bill include the introduction of 'consent managers' who will act on behalf of the Data Principals, allowance of cross-border data flows, formation of the Data Protection Board of India, various rights provided to the Data Principals like the right of information, right to correction or erasure, etc. But there are also a lot of flaws that must be worked upon. These can be non-categorization of personal data, vague definitions, no proper composition of the Data Protection Board, too much power in hands of the Executive, etc.

The vague definitions of various words in the bill need to be defined more clearly as there can be many interpretations of the words leading to absurdity. The Data Protection Board should be made more powerful and independent and its reliance on the government should be reduced. Further, amendments should also be brought to bring back the categorization of personal data. As a result, while the revised bill makes several positive modifications, it also leaves several unresolved issues that need to be addressed in subsequent drafts.