**DATA PROTECTION**

Sonal Priya

Student, PSIT College of Law, Kanpur University

Kanpur, Uttar Pradesh, India

[psonal2626@gmail.com](mailto:psonal2626@gmail.com)

**ABSTRACT**

Whether the proposed Data Protection legislation in India maintains a balance between protecting people’s privacy, while ensuring innovation and state’s power to surveil? This paper examines the preventive and regulatory structure created in the form of Digital Personal Data Protection Bill of 2022, which aspires to establish the preliminary comprehensive legal legislation for protection of data in India. With the advancement in technology and internet usage, the entities which provide digital services often collect and store the personal data of a user with the objective of providing adequate services. However, in the recent years the instances of data breach has escalated and this facilitates unauthorized parties to use data to defraud, harass or to send unwanted adverts to an individual without the consent. The first part of the paper provides an introduction and emphasizes on the importance of data privacy of an individual. The second part of the paper highlights the need of data protection law to fortify the privacy, autonomy and security of an individual. The third and fourth part of the paper elaborates on the evolution of proposed data protection bill followed by the detailed description of its current status quo and the flaws which still persist to exist in the bill. Finally, the last part provides a series of suggestions before moving onto the conclusion.

**INTRODUCTION**

In the Era of Digitization as more and more data is becoming available on digital platforms, protecting people’s privacy and security has become a substantial issue. Every activity we perform online reveals real small piece of information about our existence, for example- our name, home address, telephone number, education background and employment etc. Moreover, we also search, share and shop online which means all websites get to know sufficient details about us. All of this data when put together, leads to a very detailed personal profile of an individual which can be used for personalized marketing, advertising and even also for political purpose. By keeping track of search history and list of cookies, combined with geographical location and other information, an individual will only be able to see the information which they want to see. At first instance, it seems very convenient but it is very alarming because our past interest will determine what we are exposed to in the future, leaving less space for the novelty that spark creativity, innovation and the democratic exchange of ideas. India’s privacy jurisprudence changed in the year 2017, when the Supreme Court in Justice K.S. Puttaswamy v. Union of India held that the Indian Constitution included a fundamental right to privacy. (Chandrachud) In the courts opinion, while deciding case the central deficiency was the lack of a ‘doctrinal formulation’ that could help decide whether privacy is constitutionally protected. (Chandrachud) With the proliferation of user-generated data, exponential industrial value of data and increase state surveillance, a data protection law must be regarded as a critical piece of legislation of our times.

1. **Need of Data Protection Law in India**

As we have observed through numerous centuries and civilizations that, development is intrinsically connected to the interchange of information and thoughts, which is why the open flow of data is vital and, as a result, oversight over it is inevitable. India has embarked on a rapid digitization path over the past few decades and its Digital India effort has further expanded the internet connectivity. Although the economy has been greatly benefitted from this shift towards digitization, but at the same time new security and privacy related issues have emerged. Data breaches are becoming more frequent in India's banking, healthcare, public sector, and private sector organizations as the percentage of smart phones in rural India increased from 9 to 25 percent by 2018, the number of Indians using social media increased from 142 to 326 million by the same year, and the average monthly data usage increased by 129 percent between 2015 and 2018 (assumed a compound annual growth rate). (Kantar). According to research findings of European Data Protection Supervisor (2019), Indian residents are becoming more susceptible to privacy invasions as a result of the insufficient steps made by the government to combat cybercrime (Supervisor). This all shows how urgently India needs a law on data protection.

In India, the 'Right to Privacy' and 'Right to Information' are Fundamental Rights enshrined in the Constitution, therefore there is a pressing need for legislation on data protection to balance and defend these rights, as well as other digital rights of an individual. The Data Protection Law will safeguard the confidentiality of individuals' personal data by further regulating data collection, usage, transfer, and disclosure. As data is borderless and accessible, the law will place accountability measures and supplement it by providing remedies for unauthorized and harmful processing of data. In India, there is no comprehensive legal framework for data privacy and Internet regulation; only appropriate options and preventive measures are stipulated under the Information Technology Act of 2000, the Information Technology Rules of 2021, the Indian Penal Code of 1860, the Indian Telegraph Act of 1885, the SEBI Data Sharing Policy of 2019 and the RBI Guidelines on Cyber Security Framework for Banks and Information Security, 2016. A fragmented and unorganized collection of rules, as well as their ambiguous grievance redressal procedures, further necessitates the development of a single piece of legislation on data protection. Moreover, present legislations merely regard privacy as a statutory right and not as a fundamental one, which clearly excludes regulation on state’s processing of individual data.

1. **India’s Data Protection Bill**

Even after deliberation for more than a half decade, India’s Data Protection Law is still in the form of a bill (draft of a proposed law that is under discussion in the parliament). In the year 2017, Supreme Coiurt through Justice K.S. Puttaswamy verdict declared Right to Privacy as a fundamental right, and also stressed upon the significance of data privacy in digital era. This landmark judgement gave impetus to the development of much-awaited data protection legislation in India, and Justice Shree Krishna Committee, under the Ministry of Electronics and Information Technology was formulated in the same year. The committee proposed (Technology, Draft Personal Data Protection Bill, 2018) However, the draft was withdrawn and amended to become ‘ (Justice)

For further deliberation, the bill was referred to Joint Parliamentary Committee, which with its report suggested 81 amendments (modifications) to the 2019 bill and renamed it to ‘Data Protection Bill, 2021’. The title was amended to drop the term ‘personal’, as ‘non-personal’ data was also suggested to be included under the ambit of data protection bill. Moreover, the bill also made certain recommendations like, the data fiduciary in case of data breach must report within 72 hours to the Data Protection Authority; the power of central government to exempt certain agencies from obliging to the bill in the interest of the sovereignty and integrity of India, security of the state, friendly relations with foreign states or public order; and now the selection committee for appointment of chairperson and members of Data Protection Authority would include the Attorney General of India, an Independent Expert of Data Protection and Directors of any IITs and IIMs. However, the bill was withdrawn owing to the widespread criticism with regard to the wider powers vested upon the Central Government, increased regulatory compliance, and compulsory data localization (mandatory for a company to store a copy of personal data within India).

In India, the Union Government has lately introduced a modified version of a bill, now known as ‘The Digital Personal Data Protection Bill, 2022’ (Technology), which is a comprehensive legal framework on data protection and the main provisions of a bill are mentioned as follows:

* **Applicability**
* The current version of the bill mainly restricts itself to the processing of digital personal data no matter it is collected online or offline, within India.
* The processing of data located outside India, will only be done in cases where data is collected for creating individuals digital profile or for offering goods or services.
* **Data Principal and Data Fiduciary**
* A data principle is a person whose data is being gathered. In the case of minors, their data principals will be their parents or legal guardians (guardians appointed by the court).
* The entity (human, corporation, firm, state, etc.) that determines the purpose and means of processing an individual's personal data is known as a data fiduciary.
* **Rights of Data Principal**
* The current version of the bill assures that individual will have access to fundamental information regarding the collection, processing, and treatment of their personal data in the languages designated in the Indian Constitution's eighth schedule. This right allows an individual to request information about the exact personal data being gathered, as well as the name of the data fiduciaries who have access to it.
* Data principal need **to give consent** before their data is processed and they also have right **to know the purpose** of such data collection. Moreover, they also have a **right to postmortem privacy** (to withdraw consent) and get personal data deleted within a reasonable period of time.
* Consent shall be assumed to be given if processing is required for the execution of any statutory duty, the provision of a State service, a medical emergency, employment reasons, and defined public interest objectives such as security of a nation, prevention of fraud, and ensuring security of information.
* When data gathered by the data fiduciary is no longer relevant for the purpose for which it was collected, the data principal will have the right to seek its deletion or rectification.
* The data principle will have the right to choose someone to act on his or her behalf in the event of the data principal's death or incapacity.
* **Obligation of Data Fiduciaries**
* Data fiduciaries must take reasonable measures to verify the accuracy and completeness of data, as well as construct appropriate security controls to avoid a data breach, and must also notify the Data Protection Board of India and impacted individuals in the case of a breach.
* Data fiduciaries shall stop retaining personal data after the purpose has been accomplished and keeping is no longer required for legal or commercial reasons (limitation on their storage). The storage limits rule, however, will not apply in the event of processing by government bodies.
* It is mandatory requirement for data fiduciaries **to appoint a Data Protection Officer (DPO)** to oversee their data protection practices, and address inquiries or apprehensions that may arise from data principals.
* **Data Protection Board**
* To guarantee compliance and effective redressal of complaints, the draft proposes for the establishment of an autonomous Data Protection Board, where the data principal can register a complaint against the data fiduciary. Furthermore, the board will have the authority to investigate and sanction companies for noncompliance with the bill, as well as cancel or suspend their licenses.
* **Cross-Border Data Transfer**
* The bill permits for limited cross-border data storage and transmission to specific recognized countries and territories if they have an appropriate security landscape and the government can examine data of Indians located there.
* **Financial Penalties**
* If data principal, submits forge documents while signing up or files false grievance complaints, fine upto Rs. 10,000 can be imposed.
* If a data fiduciary commits a data breach and fails to inform the data principal, a punishment ranging from Rs. 50 crores to Rs. 500 crores may be applied.
* **Exemptions**
* The government has the authority to exclude some enterprises from complying with the bill based on the number of users and volume of personal data collected by the firm.
* However, National-Security prohibitions have been preserved, as in the 2019 version of the law.

1. **Flaws in Digital Personal Data protection Bill, 2022**

The latest draft of the bill although introduces some significant changes but also carries with itself certain shortcomings. For a start, the proposed bill restricts itself to the processing of only digital personal data and excludes non-personal data (data that does not contain any information that can be used to identify a natural person) (Non-personal Data). This narrows down the ambit of the bill because anonymous data after compilation can make a very detailed profile of an individual, and it is very difficult to differentiate between personal and non-personal data. Second, the proposed bill assigns a lot of power to the state to exempt itself as well as its agencies, and private entities from any or all the provisions of the bill. As a result of which, a lot of personal data can be processed and collected by the state or agencies without obtaining the consent from an individual. Also, the bill fails to provide a robust framework for wrongful and illegal surveillance done by the state which not only results in breach of privacy but is also against the democratic fabric of the Constitution of India. Third, the current version of the proposed bill suggests that the scope of authority and tenure of members of Data Protection Authority will be prescribed later and would depend on the discretion of the central government, which reflects ambiguity and does not inspire confidence. Also, the authority does not possess any suo moto powers to initiate investigations on its own accord and solely functions on complaints by the data principals.

Fourth, the proposed bill does not provide any regulation regarding data localization rules (transfer of data beyond country’s borders by data fiduciaries) and it can cause serious consequences like spying and misuse of personal data which as a result might have negative impact on economy (Abbey). Rather, as compared to previous versions of data protection bill, in the current draft the data localization rules have been relaxed owing to the pressure from big social platforms. Fifth, the proposed bill is in direct conflict with the Right to Information (RTI) Act, 2005 (which has empowered citizens to access information and hold governments accountable), and seeks to amend RTI to expand its purview and exempt all personal information from its ambit (The Right To Information Act, 2005). Sixth, the bill only provides for a hefty pecuniary penalty up to Rs.500 Crores, and does not provides for punishment unlike the 2019 version of the bill. This does not creates a deterrence on data fiduciary, because even after committing grave data breach if they do not hold enough assets to match the penalty, they would be exempted as proceedings would become futile. Seventh, the proposed bill does not provides any specified timeline for the Data Protection Officer (DPO) to revert to apprehensions and inquiries raised by data principals which is a noticeable limitation of the bill. In the cases like these where bill is silent about a certain procedure a significant discretion will automatically vest with the data fiduciaries in responding to the request made by data principals. Lastly, the proposed bill has diluted the data principals ‘right to be forgotten’ (right to get data permanently deleted), and rather provides a limited right to correction and erasure of personal data.

1. **SUGGESTIONS**

After an examination of the Personal Data Protection Bills of 2018 and 2019, and the Digital Data Protection Bill of 2022, the following suggestions are made to make the proposed draft bill more rights-respecting and in accordance with the rules set forth by the Supreme Court in the landmark ruling of K.S. Puttaswamy v. Union of India. Above, each provision of the bill has been comprehensively described along with the flaws which bill continues to possess. Now, the following suggestions are advised to make the proposed bill more precise and multidimensional.

First and foremost, the Principle of data minimization should be incorporated in the bill which will restrict the amount of data collected or stored at the outset of data collection. Secondarily, it is highly recommended that the legislative scrutiny of the definitions which are to be notified later by the Executive through rules, be necessarily done to make certain that the ambiguity do not get in the way of citizens accessing their rights. Also, the bill must explicitly identify surveillance as a harm and ensure that governmental surveillance is kept to a bare minimum, through suitable procedural checks, as it is critical to gain citizens' trust and faith in the confidentiality and safety of their personal data. Furthermore, the Government's monitoring of data held in India must be firmly based on necessity, as defined by statute, and must be integrated into the Bill. Furthermore, the inclusion of the right to rectification of data principals is strongly advised as it would ensure that the data is accurate and not misleading. In the current version of the bill multiple issues regarding the composition of the Data Protection Authority have stir up and it is suggested that a Quasi-judicial body consisting of technical experts must be appointed, as it will inspire public participation and trust in the complaint redressal mechanism. Another important insertion should be the right to data portability of data principals, which will help them to freely operate and transfer their data among multiple data fiduciaries. Next, the data localization rules must make clear that what type of data can or cannot be transferred outside India and the same must be mandated in the bill. Also, the exemptions given to the government should not be overbroad unlike the current version of the bill, and rather should be limited in its approach so that it does not results in the abuse of power. At last, the scope of deemed consent must be narrowed down, as widening its scope would substantially affect the privacy and security of individuals data. The above laid down recommendations will ensure that the object of the bill is fulfilled, and there is protection from violation of long- standing rights of privacy and autonomy.

1. **CONCLUSION**

Despite long-term attempts aiming to solve the problem, India still continues to struggle in establishing sustainable data protection laws which would safeguard the security of citizens' personal data and control the usage, acquisition, transfer, and disclosure of data. However, while framing legislation, lawmakers with due caution must strike a balance between an individual, the entities that retain and manage our data, as well as the state. The incidents like Cambridge Analytica where one company misused personal Facebook data to target and manipulate voters in US election, and Pegasus Spyware which is designed to infiltrate iOS and Android devices secretly to collect information reflects the alarming rate of data breach. With the advancement in technology and growth of society, the recognition of privacy as a legal right has also changed and now it is recognized as a fundamental right. Accordingly, it is the indispensable duty of the state to protect privacy of an individual. As India is gradually evolving into a more empowered and knowledge-based economy, it must have legislations which aspire to protect individual autonomy of citizens. It is considerable need of the moment that the proper data protection law be made, so that the citizens are not under a persistent fear of their personal data getting leaked and misused. Additionally, it is also necessary for a developing country like India to ensure that the foreign companies are not afraid to enter the domestic market as no company would be willing to invest its time and money on a country which is delicate on its privacy and data protection. However, the evolution and subsequent extension of the scope of the bill symbolizes significant efforts towards fortifying the privacy of an individual, but still there is a need to formulate more pragmatic framework which can only be done after realizing the cost-benefits of data protection.

**REFERENCES**

Abbey, N. (n.d.). *What is data localization?* Retrieved from stl.tech: https://stl.tech/blog/why-data-localization-is-essential/

Chandrachud, D. Y. (n.d.). *Justice K.S.Puttaswamy(Retd) ... vs Union Of India And Ors. on 24 August, 2017*. Retrieved from indiankanoon: https://indiankanoon.org/doc/91938676/?type=print

Justice, M. o. (n.d.). *The Personal Data Protection Bill, 2019*. Retrieved from prsindia.org: https://prsindia.org/billtrack/the-personal-data-protection-bill-2019

Kantar. (n.d.). *Internet Adoption in India: ICUBE 2020*. Retrieved from assettype.com: https://images.assettype.com/afaqs/2021-06/b9a3220f-ae2f-43db-a0b4-36a372b243c4/

*Non-personal Data*. (n.d.). Retrieved from Wikipedia, the free encyclopedia: https://en.wikipedia.org/wiki/Non-personal\_data

Supervisor, E. D. (n.d.). *Government access to data in third countries: Final report*. Retrieved from edpb.europa.eu: https://edpb.europa.eu/system/files/2022-01/legalstudy\_on\_government\_access\_0.pdf

Technology, M. o. (n.d.). *Draft Personal Data Protection Bill, 2018*. Retrieved from prsindia.org: https://prsindia.org/billtrack/draft-personal-data-protection-bill-2018#:~:text=Under%20the%20Bill%2C%20data%20fiduciaries,of%20certification%2C%20licences%20and%20permits.

Technology, M. o. (n.d.). *prsindia*. Retrieved from https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022

*The Right To Information Act, 2005*. (n.d.). Retrieved from Indiankanoon.org: https://indiankanoon.org/doc/671631/