DATA IS THE NEW OIL

Abstract

Whether the recently passed 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 Act of 2023, 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.

Keywords: Data protection, consent, right to privacy, right to information, data breach.

Author

Sonal Priya
Student
PSIT College of Law
Kanpur University
Kanpur, Uttar Pradesh, India
psonal2626@gmail.com

I. 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.

II. REVIEW OF LITERATURE

1. **The Digital Personal Data Protection Act, 2023[1]:** The Digital Personal Data Protection Act, 2023- This legislation aims to standardize India's data privacy regime. At the outset, the Act applies to the processing of digital personal data on Indian territory, where the personal data has been acquired in digital form and personal data is gathered in non-digital form and then digitized. Second, processing of digital personal data outside of India if such processing is in connection to any activity linked to supplying goods or services to data principals inside India. The Act accords equal protection to all digital personal data and makes no distinction between sensitive personal data and crucial data.

2. **Privacy and Data Protection in India: An Analysis[2]-** The article examines how privacy is crucial for a tranquil existence of dignity and liberty, as well as for human rights. Data protection and privacy have become a national concern and requirement as a result of increased digitization and usage of social networking sites and the internet. In the legal realm, data protection and privacy are synonymous and critical.

3. **Privacy and Data Protection in India: A Critical Assessment[3]-** The article discusses the issue in India between the right to privacy and data protection and argues that the present Information Technology (Amendment) Act, 2008 is insufficient for data

[1] https://www.pwc.in/assets/pdfs/consulting/risk-consulting/the-digital-personal-data-protection-act-india 2023.pdf
[2] Yashraj Bais, Privacy and Data Protection in India: An Analysis, International Journal of law and Management and Humanities, Volume 4 issue 5, 2021
[3] Shiv Shankar Singh, Privacy and Data Protection in India: A Critical Assessment, JSTOR, Volume 53 no. 4, 2011

protection. The author proposed separate legislation to safeguard data and privacy and hopes to spark a debate on the subject which is utilized in the study of the IT provision and amendment legislation of 2008.

4. **Navigating Data Protection in India: Key Laws and Regulations for Protecting Personal Information[4]-** The article examines data security and privacy in India. With the emergence of computerized systems capable of storing and spreading vast quantities of information in the 1970s, issues about privacy and data protection gained importance. Although the Indian Constitution does not directly guarantee the right to privacy, courts have read it alongside other rights guaranteed by the constitution, such as the right to life and liberty, to include a limited right to private. As a signatory to many international treaties, India recognizes the privacy rights stated in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

5. **A Soft Tone with a Tiger Claw a Critical Commentary on the Digital Personal Data Protection Bill, 2022[5]:** The discussion on the Digital Personal Data Protection Bill, 2022, gives useful insights into the bill's progression from the long Personal Data Protection Bill, 2019, to the more compact version. The article delves into numerous critical components of the bill, such as digital citizens' rights and obligations, children's privacy rights, and the redressal process for data fiduciaries. Furthermore, the commentary carefully examines unclear phrases about deemed consent, which have been a source of contention.

6. **Twelve Major Concerns with India's Data Protection Bill, 2022[6]:** This article highlights the 12 significant issues concerning the digital data protection law 2022 that are useful to scholars who want to evaluate these issues broadly and assess their significance to the bill's provisions.

7. **India's Digital Personal Data Protection Bill, 2022: How Practical is Consent?[7]-**The article presents a brief examination of the idea of consent in connection to the Digital Personal Data Protection law, outlining the significant issues related to consent in the law.

8. **Comments on the Draft Digital Personal Data Protection Bill, 2022 Submissions to the Ministry of Electronics and Information Technology[8]:** The VDIHI Centre submitted suggestions in this study that include key clauses and critical definitions of the Digital Personal Data Protection Bill. The paper carefully examines the law and key issues such as data principles definition, presumed consent, and act application. This report is necessary for research purposes in order to comprehend the present state of the legislation and the suggestions offered by the VDIHI Centre.

[4] Shanaz, Asifullah Samim and Mohammad Edris Abdurahim Zai, Navigating Data Protection in India: Key Laws and Regulations for Protecting Personal Information, Trinity Law Review, Volume-3, Issue-2, 2023
[5] https://www.epw.in/journal/2023/6/commentary/soft-tone-tiger-claw.html#:~:text=The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022%20is%20contrary%20to,them%20in%20the%20draft%20bill
[6] https://www.medianama.com/2022/11/223-twelve-major-issues-data-protection-bill-2022/
[7] https://jolt.richmond.edu/2023/01/19/indias-digital-personal-data-protection-bill-2022-how-practical-is-
[8] https://vidhilegalpolicy.in/research/comments-on-the-draft-digital-personal-data-protection-bill-2022/

III. SCOPE AND LIMITATIONS

1. Scope

- This research focuses on privacy and data protection legislation in India and their efficacy in protecting individuals' rights to privacy.
- To gain a better understanding, the research identifies the strengths and implications of statutes in data protection principles, mechanisms for enforcement, rights for data subjects, penalties for data processors, cross-border transmission of data provisions, and remedies for individuals in the event of a data protection breach.

2. Limitations

- This study is confined to the provisions and a critical examination of India's right to privacy and data protection law.
- The research is contingent on the accessibility of relevant information and data, and any barriers to obtaining such information and data may have an influence on the research's conclusions, which will be reliant on secondary sources.

IV. RESEARCH OBJECTIVES

The following are the research objectives:

- To comprehend India's data protection and privacy legislation framework.
- To get a comprehensive grasp of the right to privacy, data regulation, and its significance in the digital age.

V. RESEARCH QUESTION

- Whether India possess any enforcement regulations in place in the event of a violation of the right to privacy?
- Whether the current Indian legislation is effective in resolving the legal issue of data breaches by the entities?

VI. RESEARCH METHODOLOGY

The Doctrinal Research Framework Method was used by the author for this study. This approach entails a critical examination of legal documents and literature, such as legislation, case law, and scholarly papers. The author incorporates both primary and secondary sources. Relevant Indian regulations, such as the Information Technology Act of 2000, the Indian Penal Code of 1860, the Personal Data Protection Bill of 2019, the Data Protection Bill of 2021, the Digital Personal Data Protection Act of 2023, and others, are primary sources. Secondary sources include scholarly publications, books, and studies from relevant organizations and data protection professionals. A Descriptive Study approach is also used to describe data protection, privacy, and compliance as they currently operate. This enables for a thorough examination of India's legal framework's strengths and flaws, as well as the possible ramifications of the data privacy law.

1. **Need for 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 important and urgent it was for India to formulate a law on data protection.

In India, the 'Right to Privacy' and 'Right to Information' are Fundamental Rights enshrined in the Constitution, and a legislation on data protection balances and defend these rights, as well as other digital rights of an individual. The Data Protection Law further safeguards the confidentiality of individuals' personal data by regulating data collection, its usage, transfer, and disclosure. As we know that 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, when there was no comprehensive legal framework for data privacy and Internet regulation; only appropriate options and preventive measures 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 inefficiently sufficed the issues regarding data protection. A fragmented and unorganized collection of rules, as well as their ambiguous grievance redressal procedures, further necessitated the development of a single piece of legislation on data protection, and finally on 11 th August 2023 the bill after receiving assent from President of India came into existence in the form of an act.

2. **India’s Legislation on Data Protection:** After deliberation for more than a half decade, India’s Data Protection Law bill (draft of a proposed law that is under discussion in the parliament), on 11th August, 2023 was finally enacted. In the year 2017, Supreme Court 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 ‘Personal Data Protection Bill, 2019‘ (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 passed a modified version of a bill, now known as 'The Digital Personal Data Protection Act, 2023' (JUSTICE), which is a comprehensive legal framework on data protection and the main provisions of a bill are mentioned as follows:

- **Applicability**
  - The act 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 act 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 act provides 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 act, as well as cancel or suspend their licenses.

- **Cross-Border Data Transfer**
  - The act 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 act based on the number of users and volume of personal data collected by the firm.
  - However, National-Security prohibitions have been preserved in the present legilation, as in the 2019 version of the law.

3. **Concerns Revolving Around Data Protection Legislation:** The Personal Digital Data Protection Act, 2023 although introduces some significant changes but also carries with itself certain shortcomings. For a start, the act 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). This narrows down the ambit of the act 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 act 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 act. 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 act 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, as the act 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 act 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 recently passed enactment the data localization rules have been relaxed owing to the pressure from big social platforms. Fifth, the act 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 act 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 act 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 act 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 act 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.

VII. SUGGESTIONS

After an examination of the Personal Data Protection Bills of 2018 and 2019, and the Digital Data Protection Act of 2023, the following suggestions are made to make the act 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 act has been comprehensively described along with the limitations which act continues to possess. Now, the following suggestions are advised to make the act more precise and multidimensional.

First and foremost, the Principle of data minimization should be incorporated in the act 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 act 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 Act. 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 enactment 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 act. Also, the exemptions given to the government should not be overbroad unlike the current enactment, 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 act is fulfilled, and there is protection from violation of long- standing rights of privacy and autonomy.

VIII. 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

[1] Abbey, N. (n.d.). What is data localization? Retrieved from stl.tech: https://stl.tech/blog/why-data-localization-is-essential/
[2] 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
[3] 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
[4] 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/
[5] 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
[6] 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.
[7] Technology, M. o. (n.d.). prsindia. Retrieved from https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022
[8] The Right To Information Act, 2005. (n.d.). Retrieved from Indiankanoon.org: https://indiankanoon.org/doc/671631/

