

A Key Analysis on Data Protection Bill and Its Impact in India

Shiwani Anand*

Abstract

The goal of this research work is to assess and thoroughly investigate the data protection bill. India has become a huge market of data, post digitalization. Every day, tons of data are created and circulated. This data is a very powerful tool in this data-driven world. It has the power to create something as well as has the power to destroy something. The world is witnessing an increasing number of cybercrimes nowadays. However, the issue was that India lacked adequate data protection regulations. For around the past 3 to 4 years, debates were going on about the need for such a law. And for the first time in India, law is brought for data protection. It is named as data protection bill. In the year 2019, it was introduced. This research work tries to throw light and have a detailed discussion on the data protection bill. It further talks about the contents and features of the Data protection bill. It also talks about the advantages and some concerns regarding the data protection bill. Moreover, it talks about the recent WhatsApp privacy policy which was violating the data protection bill.

Keywords: Data protection bill, data post digitalization, cybercrimes, data protection regulations, WhatsApp privacy policy

INTRODUCTION

In the era of digitalization and where the internet is ruling the world, we or the people knowingly or unknowingly create a lot of data which generally consist of information about us or about the user [1]. Now you must be wondering what will be there in this information? This information can be anything like your address, pin code, bank details, dislike, etc. This data is a powerful tool in this data-driven world in many ways. The epidemic that altered our way of life made 2020 the year the globe became more digital than ever before. One of the year's silver linings was the increased emphasis on data and data flow value. Many times, we hear in the news that data was leaked by this company or data got stolen from this company. Data that got stolen can be used for illegal activities also. So, it was the need for an hour to bring a law that will bind or that will make companies responsible to protect their customer's data. And for this purpose, India brought a data protection law known as the data protection bill. In this research work is an in-depth study of the data protection bill and its impact on India. Today's global negotiations centred around deliberations about data transmission and security. In this regard, the Personal Data Protection (PDP) Bill, 2019, is India's first effort to internally legislate on data protection. The Bill is based on a previous Draft version prepared by a committee chaired by retired Justice BN Srikrishna. The current Draft, however, departs from the recommendations made by the Justice BN Srikrishna committee.

*Author for Correspondence

Shiwani Anand
E-mail: shiwanianand7@gmail.com

Student, Faculty of Law, Amity Law School, Noida, Uttar Pradesh, India

Received Date: February 21, 2023

Accepted Date: March 17, 2023

Published Date: March 23, 2023

Citation: Shiwani Anand. A Key Analysis on Data Protection Bill and Its Impact in India. Journal of Corporate Governance & International Business Law. 2022; 5(2): 31–35p.

What is Data?

You must be wondering what is this data all about? So, before moving further with our topic we

should understand what is this data all about [2]. The term "data" refers to a large acquisition of information stored on a desktop or a network. Personal and non-personal data are the two forms of data that can be generically categorized. Personal information is anything that can be used to identify a person, such as characteristics, traits, or attributes. Aggregated data that cannot be used to identify specific people make up non-personal data. Whereas an individual's location would be considered personal data, information obtained from the locations of many drivers, which is frequently used to inspect traffic flow, is considered non-personal data. Data protection pertains to rules and processes aimed at reducing invasion into a person's privacy as a result of the gathering and use of their private details. Data is divided into two categories: collection and processing. The data is collected and handled by fiduciaries, but processing might also be done by third parties [3]. For example, Facebook is fiduciary, whereas Cambridge Analytica was the data processor that drew relevant inferences from the data. For new generation sectors like advertising, machine learning, and artificial intelligence, data is the new oil. While Japan, the United States, and many other industrialized countries desire open data flow, India is leaning toward data localization to protect its domestic industry and residents.

USES OF SOLD OR STOLEN DATA

Every year, data breaches result in the theft of billions of personal documents. But, once the data has been stolen, what do the thieves do with it? Data breaches are, in fact, a lucrative business for thieves. Identity fraud is a cybercrime in which a person's private details are used to obtain benefits as a result of the victim. Many internet services collect personal information such as complete name, home address, and credit card details. This information is taken from online accounts by identity thieves with the goal to perpetrate fraud, such as using the victim's credit card or accumulating debt in their name. The exploitation of stolen personal data by fraudsters to initiate phishing attacks on their targets is possible. By seeming as something respectable, hacking scams entice victims to readily provide criminals private information like credit card details. If they have access to private information, criminals may attempt to blackmail the victim. Aside from the emotional issues that stolen data might create, it can also harm businesses. Criminals can use stolen data to target company employees to obtain confidential material or to deceive them into making payments. One person is the target of a specific kind of phishing attack called spear-phishing. Criminals can also attempt to hack into enterprise networks to snoop on them as well corrupt them with malware. Because of all this, there was always a debate that India needs a data protection law to protect data from all these frauds. After reviewing the situation, government decided to bring a data protection bill. A country needs to have a data protection law in this data-driven world.

WHAT IS A DATA PROTECTION BILL? ITS CONTENT AND FEATURES

Mr. Ravi Shankar Prasad, Minister of Electronics and Information Technology, introduced the Personal Data Protection Bill, 2019 in the Lok Sabha on December 11, 2019 [4]. The bill aims to ensure that the personal data of persons are protected, and it proposes a Law to do so. This data protection Bill oversees the handling of personal information by the following entities: the government, (ii) Indian companies, and (iii) international firms dealing with the private data of Indian residents. Personal information is collected about an individual's qualities, traits, or identification attributes that could be used to recognize them. Certain types of personal data are classified as sensitive in the bill. Financial information, biometric data, caste, religion or political opinions, or any other type of data established by the government in collaboration with the Agency and the relevant sectoral regulator are examples of this. An information custodian is an institution or person who chooses how and why personal data is processed. Personal data, for example, can only be processed for particular, unambiguous, specified, and lawful purposes. Furthermore, all data fiduciaries must take specific transparency and accountability steps, including implementing security protections and (ii) establishing grievance redressal systems to handle individual concerns. When managing sensitive personal information of children, they must additionally have measures for proof of age and parental consent. This bill has given rights to its citizen. Individual rights are outlined in the bill (or data principal). These rights include the ability to: acquire proof from the fiduciary that their personal information has been produced, (ii)

request revision of incorrect, insufficient personal data, (iii) possess personal information transmitted to any other data controller in certain conditions, and (iv) limit the continued release of information of their private information by a fiduciary if it is no longer appropriate or permission has been revoked [5]. This bill provides certain grounds or circumstances in which personal data can be processed. These grounds are for the benefit of the citizen. The bill only permits fiduciaries to process data with the agreement of the individual. Personal data can, however, be filtered without permission in certain circumstances. These include: (i) if the state requires it for the individual to receive benefits, (ii) judicial proceedings, and (iii) responding to a medical crisis. Without these grounds, no one has permission to process personal data and if someone tries to get personal data without these grounds then it would be considered unlawful. This data protection bill forbids the exchange and processing of sensitive personal data outside of India's borders. It restricts the exchange and use of sensitive data, and it can only be performed with an individual's permission. Clause 41(1) of the Bill also proposes the establishment of a Data Protection Authority, which would guarantee that Bill's requirements are implemented and followed. The bill also permits data principals or those who are linked to the data, to alter or delete their personal information. It also establishes exceptions to the consent rules. That is, in medical situations, when filing a lawsuit, and when providing state services.

CONCERNS ABOUT THE DATA PROTECTION BILL

1. Exemptions for the government: Section 35 of the bill would allow the National Government to prohibit any government agency from the law's obligations.
2. There are no legitimate exclusions: There is no compelling justification for government entities to be exempt from Bill's core requirements.
3. Though the government would specify protocols, safeguards, and control measures, this would be a simple breach.
4. Executive hegemony: The executive's discretion to make such an order is not subject to oversight.
5. Arbitrary and intrusive: The current procedures for safeguarding civilians from unjustified and intrusive State action, as revealed by the Pegasus case, are ineffective.

Once implemented, the Personal Data Protection Bill, 2019, will be the first law in India to acknowledge the right to be forgotten. However, it is worth noting that the bill does not specify any remedies for limiting or prohibiting publication. It could be a total removal or simply changes in the underlying or deindexing of the data to make access more difficult. Deindexing is the process of deleting a data link from a search engine's results page, although it does not remove the material from the website where it was originally published. There are no criteria for the Grievance redressal Officer to use in determining which remedy is appropriate. Everything is up to the Adjudication Officer's discretion. The Bill's censoring component is also a source of worry [6]. The fact that the Adjudicatory Officers are selected by the Government and then have the authority to restrict internet data is considered a threat to the division of powers and fair trials. Although Chapter II of the Bill has measures for limiting personal data processing, the right to be forgotten must be expanded to encompass the ability to object to processing, not simply disclosure.

ADVANTAGES OF DATA PROTECTION BILL

1. Localization of data can aid security agencies in gaining access to information for examinations and prosecution.
2. Currently, a large portion of the inter-data transfer is managed by bilateral "mutual legal assistance treaties". This method of accessing data is possible, but it takes time.
3. Cybercrimes and monitoring will be investigated.
4. Pegasus, an Israeli software, has hacked a huge proportion of WhatsApp accounts.
5. Fake news is being propagated on social media, resulting in mob violence and national security risks that can now be tracked, checked, and prevented in real-time time.
6. The power of an Indian government can charge Online behemoths would also improve as a result of data localization.
7. Data sovereignty can also be enforced with the support of strong data protection regulations.

WHY DOES INDIA NEED A DATA PROTECTION BILL?

India is developing as a digital world, and it requires strong legislation to preserve its inhabitants' privacy. It is difficult to identify what rights people have because there is not a strong data protection policy in place, which makes the fundamental privacy rights practically meaningless. A data protection law will give citizens a legal basis for their rights by specifying the scope of the fundamental right to privacy, and what data custodians who collect personal data may and cannot do with it. Personal data also contains highly sensitive data such as contact information, locations, religious beliefs, political beliefs, and so on. There are currently no rules prohibiting corporations from keeping these data. Firms are also not liable if sensitive data such as surfing patterns and online activities is disclosed, which is frequently stored without the consumers' agreement. This bill will therefore have provisions to stop the usage of such data. It is becoming more crucial for governmental organisations to defend citizens' data rights as consumer data usage grows and data's industrial value rises. Data protection laws, which control the gathering, use, transmission, and disclosure of that data, provide protection for people's personal information. Additionally, they provide individuals with access to their data, establish rules on businesses collecting personal data, and provide remedies for unauthorised or harmful exploitation.

WHATSAPP CONTROVERSY IN CONTEXT OF DATA PROTECTION BILL

WhatsApp's new data privacy policies for India were revealed on January 4, 2021. As a consequence of this privacy improvement, WhatsApp shall be ready to share user metadata and chats with business accounts with Facebook. Because India lacks comprehensive data protection legislation, WhatsApp may take these steps in India rather than in the European Union. The Ministry of Information Technology, on the other hand, presented the Proposed Personal Data Protection Bill to Parliament in 2019. Data owners must give express consent, according to clause 11(2)(c) of this bill. Clauses 5 and 6 stipulate that the data custodian may only acquire data with the approval of the data owner. WhatsApp, on the other hand, can easily get over these restrictions. It can claim that users have expressly agreed to have their metadata used and shared with Facebook to operate the messaging service. As a result, WhatsApp's defence may be that this was not withholding information from the user. The problem with this privacy upgrade was that it does not provide the customer or the data owner with many options. A user can either accept or refuse the terms of service, in which scenario they will be unable to send WhatsApp messages. Alternatively, a user must agree for their information to be used for both reasons. Clause 11(3)(c) enables the data custodian to get consent for each purpose of handling sensitive personal data separately. So, because information and conversations with a business bank account that WhatsApp would have been open to sharing with Facebook could expose sensitive personal information like patient data, sexual preference, and so on; this requirement could have avoided WhatsApp from taking approval for both purposes at the same time [7]. However, to secure a watertight process against cyber behemoths like WhatsApp, it would be preferable to broaden the scope of the service beyond sensitive personal information to encompass all personal data. As a result, a provision in the PDP bill that is analogous to Article 7(2) plus Recital 32 of the European Union's General Data Protection Regulation is required. It would necessitate the data custodian to obtain authorization for the collection and processing of all personal data for each unconnected purpose separately. It would allow the data principal more control over their data. Clause 11(4) forbids the data custodian from refusing data principals products or services if they decline to consent to the processing of data that is not essential to supply such goods or services. As a result, WhatsApp would not have denied its users messaging services simply since they declined to agree to the gathering and analysis of their metadata, which is not required to provide a chat feature. The lack of data security does not mean that WhatsApp's privacy policy will be ignored. Because consumers do not have enough ability to sort out the terms and conditions, the privacy policy change can also be viewed as a conventional contract. Users must either agree to the terms in their entirety or reject them entirely. Even though the fact that the Indian Contract Act of 1872 does not distinguish between such forms of contract and a normal contract, the court has developed guidelines that must be followed due to the parties' unequal negotiating power [8]. When a person "has no option or rather have no meaningful choice" but to sign the contract and accept the contract's unjust conditions, the contract must be deemed irrational and unconscionable. "It is not

required to install WhatsApp on your cell phone and it is voluntary", the court noted, implying that users' privacy concerns were underplayed. You have the option of not installing WhatsApp [9]. As a result, the rights to privacy of data principals require a comprehensive and explicit statutory foundation. By enhancing permission specific and purpose limitations in India's data protection legislation, the PDP bill seeks to limit the responsibilities of the data fiduciary.

CONCLUSION

The right to privacy is a fundamental human right, as per the Apex Court in the Puttaswamy decision (2017), and it is needed to safeguard personal information as a vital facet of informational privacy, while the growth in digital is also good to expand new vistas of socio-economic growth. In light of recent incidents of data theft and exploitation by foreign influences and organizations, India urgently needs reforms and legislation in the area of citizen data protection. Nevertheless, the Bill must strike a balance between government action and a sufficient balance of powers to ensure that everyone is held accountable. It is also worth noting that it is the legislation's implementation, not the legislation itself, that ensures that it accomplishes its goals. Consumers should have greater ownership over personal data and a larger portion of the value it provides, as Satya Nadella stated in his speech at the Economic Forum on "Data Dignity" [10]. It is past time to grant the Data Principal complete control of his data. In this context, the government's data protection policy should not prevent any policy for the digital economy's growth from being framed, as long as it does not compromise personal data privacy.

REFERENCES

1. Garg R. (2022 Mar 11). Personal Data Protection Bill, 2019 and the right to be forgotten. [Online]. iPleaders. [cited 2023 Mar 17]. Available from: <https://blog.ipleaders.in/personal-data-protection-bill-2019-and-the-right-to-be-forgotten/>
2. Wikipedia Contributors. (2023). Data. [Online]. Wikipedia. [cited 2023 Mar 17]. Available from: <https://en.wikipedia.org/wiki/Data>.
3. Simplilearn. (2023 Mar 23). What Is Data: Types of Data, and How to Analyze Data? [Online]. Simplilearn. [cited 2023 Mar 17]. Available from: <https://www.simplilearn.com/what-is-data-article>.
4. Insights Editor. (2022 Mar 5). Data protection Bill. [Online]. INSIGHTSIAS. [cited 2023 Mar 17]. Available from: <https://www.insightsonindia.com/2022/03/05/data-protection-bill-2/>
5. Admin. (2019). Personal Data Protection Bill, 2019 withdrawn on August 3, 2022: Know latest updates [Online]. BYJUS. [cited 2023 Mar 17]. Available from: <https://byjus.com/free-ias-prep/personal-data-protection-bill-2019/>
6. Personal Data Protection Bill 2019. [Online]. Drishti IAS. 2019 [cited 2023 Mar 17]. Available from: <https://www.drishtiias.com/daily-updates/daily-news-editorials/personal-data-protection-bill-2019>
7. Bhalla V, Dave P. (2021 May 21). WhatsApp Privacy Policy applies only to India due to weak data regulations. [Online]. The Leaflet – An independent platform for cutting-edge, progressive, legal, and political opinion. [cited 2023 Mar 17]. Available from: <https://theleaflet.in/whatsapp-privacy-policy-applies-only-to-india-due-to-weak-data-regulations/>
8. Diganth Raj Sehgal. (2021 Feb 1). The Personal Data Protection Bill, 2019 - making right to privacy fundamental. [Online]. iPleaders. [cited 2023 Mar 17]. Available from: <https://blog.ipleaders.in/personal-data-protection-bill-2019-making-right-privacy-fundamental/>
9. Dhavate N, Mohapatra R. (2022 Jan 5). A look at proposed changes to India's (Personal) Data Protection Bill. [Online]. Iapp.org. International Association of Privacy Professionals. [cited 2023 Mar 17]. Available from: <https://iapp.org/news/a/a-look-at-proposed-changes-to-indias-personal-data-protection-bill/>.
10. Agarwal S. (2022 Feb 17). Fresh legislation may replace Data Protection Bill. [Online]. The Economic Times. [cited 2023 Mar 17]. Available from: <https://economictimes.indiatimes.com/tech/technology/fresh-legislation-may-replace-data-protection-bill/articleshow/89624369.cms>