"DATA PROTECTION BILL AND RIGHT TO PRIVACY: A DETAILED INTERPRETATION"

-Deeksha Shrivastava

ABSTRACT

Personal and Non-personal data are the two forms of data that can be broadly categorized. Personal data pertains to characteristics of identity which can be used to identify an individual. Non-personal data consists of aggregated data that cannot be used to classify individuals. Data protection refers to policies and procedures aimed at restricting interference into an individual's privacy as a result of the collection and use of their personal data. The Indian Supreme Court ruled in 2017 that the Indian constitution protects a person's right to privacy. There is no data security law in India. India has no data protection agency. India's Aadhaar biometric database, with over 1.3 billion records, is the largest in the world. In January 2018, it was revealed that access to the information of 1.3 billion records on the UIDAI database, including names, addresses, and images, was being sold for 500 rupees.

The Data Protection Bill, 2019 covers mechanisms for protection of personal data and proposes the setting up of a **Data Protection Authority of India.** The 2019 Bill has some important clauses that the 2018 draft Bill did not, such as the central government's ability to exclude any government agency from the Bill and the **Right to Be Forgotten**. The right to privacy has been recognized as a fundamental right emerging primarily from Article 21 of the Constitution, in ***Justice K.S. Puttaswamy (Retd.) v. Union of India***. To make this right effective, the State must create a data security system that serves the common good while protecting people from threats to their informational privacy posed by both state and non-state actors. The Committee must work with this awareness of the State's obligation as it establishes a data security policy.

I. INTRODUCTION

On July 31, 2017, the Indian government established a **Data Protection Committee**, which was lead by Justice B.N. Srikrishna, The report was submitted on July 27, 2018, and it looked at issues concerning data security in India. Later, the government made the Bill available to the public for comments and suggestions. On December 4th, 2019, the Union Cabinet adopted an updated **Personal Data Protection Bill, 2019** based on these recommendations. On December 11, 2019, the Bill was introduced in the Lok Sabha. It was then referred to a Joint parliamentary Committee of both the houses.

The 2019 Bill is broadly based on the principles of the General Data Protection Regulation, 2016 and the landmark judgment of the Supreme Court of India: ***Justice K.S. Puttaswamy (Retd.) & Anr v Union of India***[1] wherein right to privacy was upheld as a fundamental right under the Indian Constitution. The 2019 Bill aims to protect individuals' privacy rights in relation to their personal data while also governing and regulating the entities that handle such data.

- **Definition of Personal Data**

Section 3(28) of the Personal Data Protection Bill, 2019 states that "Personal data means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include inference drawn from such data for the purpose of [2]profiling."

- **Amended Definition of Sensitive Personal Data**

The word 'Passwords' from the 2018 bill has been removed under the 2019 Bill. This appears to be a government initiative to standardize the concept of confidential personal data in accordance with international standards and legislation. This was also a pressing need, as entities that were not processing sensitive personal data per se were required to comply with a higher level of compliance associated with such data simply by providing password-protected access to their services in order to provide enhanced data security to their users.

[1]W.P. (Civil) No. 494 of 2012

[2] Section 3 (32) of The Personal Data Protection Bill, 2019 defines 'profiling' as any form of processing of personal data that analyses or predicts aspects concerning the behavior, attributes or interests of a data principal.

The Central Government had exclusive and exclusive authority to classify such other forms of personal data as sensitive personal data under the 2018 Bill. The Central Government must now communicate with the Authority[3] before notifying any other forms of personal data as Sensitive Personal Data[4] under the 2019 Bill.

II. INDIAN PRIVACY LAWS

[5]In terms of implementation, it is clear that Privacy Laws protect the data-subject, i.e. an individual whose data is shielded from being accessed, used, or released without its permission. The real reason behind the need for triggering the Privacy Rules is collection, possession or transfer of 'personal' or 'private' information as given under **Rule 2(1)(i)** of the Privacy Rules. It is clear that in Indian privacy laws, the data subject is primarily an individual. It is clear that in Indian privacy laws, the data subject is primarily an entity. It is important to note that there is no meaningful legal distinction between a data controller and a data processor in terms of responsibilities, which, among other things, generates its own set of issues. According to the bill, the information covered does not include all personal information, but only "sensitive" personal details.

Data security regulations have been introduced in The Information Technology Act, 2000 with a particular emphasis on the protection and privacy of personal information. These privacy laws were not enacted with the purpose of restricting their application to the technology sector alone; rather, since data protection principles are a very universal and crucial issue, they can be applied fairly and with the same force and compliance to all sectors and operations. The concept of Right to privacy and data protection's impact in India is interwoven and interconnected to the concept of data protection and breach of personal data.

III. EMERGENCE OF RIGHT TO PRIVACY AND BECOMING FUNDAMENTAL RIGHT

[3] Section 3 (5) defines 'Authority' to mean the Data Protection Authority of India established under section 4(1) of The Personal Data Protection Bill, 2019.

[4] Section 15 (1) of The Personal Data Protection Bill, 2019.

[5] Deepanwita Sengupta, The interrelationship between Data Protection Bill, 2019 and Right to privacy (Apr. 06,2021, 20:10) https://blog.ipleaders.in/the-interrelationship-between-data-protection-bill-2019-and-right-to-privacy/

Ancient India: In ancient Hindu scriptures, the idea of privacy may also be realistic. In light of the Hito-padesh, this stipulates that such things, such as worship and family matters, should be kept private. Although the term is not unfamiliar to Indian culture, some jurists, such as Sheetal Asrani-Dann, have reservations about the right to privacy in India. Even in ancient times, privacy was linked to Positive principles. Despite this, the ancient Indian text's right to privacy was ambiguous.

Modern India: The existence of a right to privacy was first rejected by the Supreme Court in the year 1954 by an eight-judge bench in the ***M.P. Sharma v. Satish Chandra***[6] case, while dealing with the power to search and seize documents from the Dalmia Group, while dealing with the power to search and seize documents from the Dalmia Group, dismissed the existence of a right to privacy on the basis that the creators of the Constitution. In ***Kharak Singh v. State of Uttar Pradesh***[7]**,** the Supreme Court held that there is no fundamental Right to Privacy. The Supreme Court in ***Gobind v. State of Madhya Pradesh***[8] cleared that Article 21 of the Constitution recognized the existence of a constitutional right to privacy. In the case of ***K.S. Puttaswamy v. Union of India***[9]**,** a nine-judge bench overturned the judgments of M.P. Sharma and Kharak Singh. After this decision, it is clear that the right to privacy is a constitutional right, and it will retain its place among the Golden Theology of Articles 14, 19, and 21.

In India, the Right to Privacy is a Fundamental Right: Right to privacy is a fundamental right under Article 21 of the Constitution of India affirmed in Justice K.S. Puttaswamy v. Union of India dated 24th August 2017 where they proclaimed that "Right to Privacy" is an integral part of Part III of the Indian Constitution. In 2017, a Supreme Court bench of five judges hearing the case on the Aadhaar Card and the right to privacy demanded that a nine-judge bench first determine if privacy is a fundamental right before ruling on the main Aadhaar case. In the Aadhaar case, the Attorney General argued that while many Supreme Court decisions had accepted the right to privacy, the Kharak Singh and M P Sharma decisions had refused to agree that the right to privacy was a fundamental right. It was therefore necessary to constitute a nine-judge bench to decide whether or not right to privacy

[6] AIR 1954 SCR 1077

[7] AIR 1964(1) SCR 332

[8] 1975 (2) SCC 14

[9] 2010 10 SCC 1

is a fundamental right. The Supreme Court's extensive interpretation prompted a series of government policies aimed at enacting Personal Data Protection laws.

IV. PRIVACY AND DATA PROTECTION

[10]The PDP Bill, which was inspired by the GDPR, was introduced to overhaul India's new data protection regime, which is currently regulated by the Information Technology Act, 2000. The latest draft of the PDP Bill establishes compliance standards for all types of personal data, expands individual rights, establishes a central data security authority, and mandates data localization for some types of sensitive data. If such nexus conditions are met, the PDP Bill extends extra territorially to non-Indian entities and imposes hefty financial penalties in the event of non-compliance.

Projected Non-Personal Data Framework:- The Ministry of Electronics and Information Technology, Government of India constituted a **NPD Committee** to explore the governance of non-personal data (**NPD).** The NPD Committee's report on the Non-Personal Data Governance System was released on July 12, 2020. According to the report, a separate NPD governance structure should be created. However, the study lacked clarity in terms of definitions, suggested provisions, and the goal that the proposal was supposed to accomplish. The NPD Committee then released an updated version of their report in January 2021, clarifying several issues. The updated report clarifies how the PDP Bill and the recommended NPD system would work together, stating that the NPD framework will only cover datasets. The updated report outlines the types of NPD that can be obtained, delves into the public and private rights that may exist in such data, and contains a comprehensive data exchange process that excludes transfers between private entities. The report provides separate guidelines for 'Data Businesses', or data collecting entities and also calls for the creation of a separate regulator that would function independently.

V. THE PERSONAL DATA PROTECTION BILL, 2019

A data principal is an entity whose personal data is being processed under the Bill. Data fiduciary refers to the agency or individual who decides on the means and purposes of data processing. The Bill controls how the government and companies incorporated in India

[10] The National Law Review, Volume XI, Number 96 (Last visited April 6, 2021)

process personal data. It also refers to international companies that deal with personal data of Indian people.

The bill aims to protect individuals' privacy in relation to their personal data, establish a trust relationship between persons and entities processing personal data, and more. Protecting the human rights of individuals whose personal data is processed, creating a system for organizational and technological measures in data processing, laying down norms for social media intermediaries, cross-border transfer, accountability of entities processing personal data, remedies for unauthorized and harmful processing, and establishing an Indian Data Protection Authority.

Processing of personal data is exempt from the provisions of the Bill in some cases. For example, in the interests of state security, public order, India's sovereignty and independence, and friendly ties with foreign states, the central government may exempt any of its agencies. The exemption for certain other purposes such as prevention, investigation, or prosecution of any offence, or research and journalistic purposes is made. Individuals' personal data may also be processed without their permission under such cases, (i) when the state is forced to provide benefits to the individual, (ii) during legal proceedings, and (iii) in the event of a medical emergency.

VI. KEY PROVISIONS OF THE BILL

Individuals' personal data is governed by these provisions. They are as follows –

i. **Data Fiduciary:** Data fiduciary[11] means any entity or any individual which determines the purpose and means of processing personal data. The bill enumerates certain obligations relating to the Data fiduciary, such as- Personal Data should be processed only for clear and lawful purposes, The privacy of the person to whom the data belongs, should be ensured, etc.

ii. **Data processing without consent:** The bill provides provisions for processing of data after consent is obtained from the Data Principal.

[11] Clause 2(13) of the Bill

iii. **Rights of the Data Principal:** The bill also provides for rights[12] that can be exercised by a data principal such as the right to seek information regarding the manner or the data fiduciary's processing practices with respect to the personal data.

iv. **Data Protection Authority:** The bill provides for the establishment of a Data Protection Authority[13] to protect the interest of data principal, prevent misuse of personal data, ensure compliance and promote awareness regarding data protection.

v. **Regulatory Sandbox:** The data protection authority must develop a sandbox to facilitate and enable the use of artificial intelligence, machine learning, and other emerging technologies. The organizations that will be included in the sandbox will not be needed to comply with the Bill's provisions.

VII. RIGHT TO BE FORGOTTEN

The right to be forgotten is a legal right that requires people to get their personal details deleted from the internet, which is a public space. However, by exercising this right, one is restricting the public's right to information, which is protected under the Freedom of Expression. Person data is often generated by both public and private bodies, rather than by the people themselves. It is also possible to look up and obtain details about someone who does not have an online account. The right to be forgotten pertains to the right of individuals to erase, restrict, delete or correct deceptive, humiliating personal information on the Internet.

This right was founded by a ruling by the **Court of Justice of the European Union (CJEU)** in the well-known ***Google Spain Case***, in which the court ordered Google to delete online links relating to a Spanish individual's debt collection proceedings. The individual's right to have incorrect or inaccurate data from search engines rectified, erased, or blocked was upheld by the court.

There is confusion as to whether or not this right exists in India. In a case, the Karnataka High Court claimed that the right to be forgotten, which is common in Western countries, can be used in sensitive cases involving women in general and extremely sensitive cases

[12] Chapter V of the Bill

[13] Clause 41 of the Bill

involving rape or affecting the modesty and integrity of the individual concerned. This decision has been criticized as controversial because it is founded on a concept of women's modesty and dignity rather than the constitutional right to privacy.

Case Law- The Odisha High Court in the case ***Subhranshu Rout @ Gugul v. State of Odisha***[14] observed the importance of the right to be forgotten of an individual and how it remains unaddressed in legislation. The case concerned content online that was deemed offensive to a woman. The court noted that recognizing such a right by law would help in safeguarding woman's rights online, thus highlight the importance of strong individual privacy rights. The court was aware that, if enacted into law, the current draft of the PDP Bill would provide a right to be forgotten in India.

VIII. ANALYSIS OF THE BILL

- **The Advantages of the Bill are-**

i. Localization of data will aid law enforcement authorities in gaining access to information for investigations and enforcement.
ii. Instances of cyber attacks and surveillance will be checked.
iii. Social media is being used to spread fake news, which has resulted in lynchings, national security threats, which can now be monitored, checked and prevented in time.
iv. Data localization will also increase the ability of the Indian government to tax Internet giants.

- **The Disadvantages of the Bill are-**

i. Many contend that the physical location of the data is not relevant in the cyber world. Even if the data is stored inside the country, national authorities may not have access to the encryption keys.
ii. National security or reasonable purposes are an open-ended terms, this may lead to intrusion of state into the private lives of citizens.

[14] BLAPL No. 4592 of 2020

IX. OFFENCES AND PENALTIES

Offence	Penalty
Violating of the Bill by collecting or transmitting personal data	Fine of ₹15 crore of 4% of annual turnover, whichever is higher
Failure to perform a data audit	Fine of ₹5 crore or 2% of annual turnover, whichever is higher
Re-identification and processing of de-identified data without consent	Imprisonment of up to three years, or fine, or both

X. THE CORRELATION BETWEEN THE DATA PROTECTION BILL, 2019 AND THE RIGHT TO PRIVACY

In the age of data-gathering and online companies, digital technology has made it possible to not only store personal information generated by customers, but also to monitor their decisions as they browse online sites, resulting in an increasing demand for data security. With the passing of time, it has become apparent that the specific aspect of common law allowed judges to grant the required protection, i.e. privacy, also known as the **"Right to Privacy"**. Tort law has grown to include privacy issues, demonstrating how developments in law enforcement are linked to modern data-driven initiatives, which have had a significant effect on constitutional law as well as we can see in the 'AADHAR' controversy. [15]In May 2017, The Economist called **Data** the most powerful resource even more valuable, which was a major realization as to how law enforcement has changed around the world and how much influence is now measured by how much data the government keeps and regulates, and how heavily it revolves around data hoarding, data mining, and monitoring of this data.

Private data collection is excluded from the Bill's rules for reasons such as the prevention, investigation, or prosecution of any crime, or for personal, domestic, or journalistic purposes which leave an individual's data open to abuse because it is still accessible to some industries without their permission.

XI. JUDGEMENTS RELATED TO BILL AND PRIVACY

[15] Supra Note 5

- **R. Rajagopal v. Union of India (1994)[16]:** The Supreme Court ruled that the right to privacy is a part of the constitutionally protected right to personal liberty. It was acknowledged that the right to privacy can be both a tort and a fundamental right. A citizen has a right to safeguard the privacy of his or her own family, marriage, child-bearing and education among other matters and nobody can publish anything regarding the same unless-
    (i) He/she knowingly or unconsciously enters into a conflict.
    (ii) The publication is based on information from public records (except for cases of rape, kidnapping and abduction).

- **Unique Identification Authority of India & Anr. v. Central Bureau of Investigation (2014)[17]:** In this case, the Central Bureau of Investigation sought access to the database of the Unique Identity Authority of India for the purposes of investigating a criminal offence. In an interim order, the Supreme Court ruled that the Unique Identity Authority of India could not share any biometric details about anyone who has been assigned an Aadhaar number with any other agency without their written consent.

- **Justice K.S. Puttuswamy (Retd.) & Anr. v. Union of India & Ors. (2015)[18]:** In this Supreme Court order, the issue of privacy was discussed in light of the Unique Identity Scheme. The court had to decide if such a right is covered by the Constitution. According to India's Attorney General, privacy is not a fundamental right granted to Indian people. As a result of the unresolved dispute, the Court decided to refer the case to a wider bench for resolution. This was settled in the 2017 decision that the constitution contained a fundamental right to privacy.

- **Balu Gopalakrishnan v. State of Kerala (2020)[19]:** The Kerala High Court in this case passed an interim order prohibiting the State Government of Kerala from exporting COVID-19-related data to Sprinklr, a data analytics firm based in the

[16] 1995 AIR 264 1994 SCC (6)

[17] SLP (CRL) 2524/2014

[18] WRIT PETITION (CIVIL) NO 494 OF 2012

[19] WP (C) 9498/2020

United States. The High Court ruled that the State Government must take certain steps before granting Sprinklr access to the data. Anonymizing the data, obtaining express consent from residents, and ensuring the return of data after contractual obligations have expired are all examples of these steps. This decision creates a high standard for all public-private partnerships in the post-COVID-19 period in the field of data security, stressing the government's role in managing citizens' data.

XII. CONCLUSION

The Right to privacy is a fundamental right, according to the SC in the **Puttaswamy decision (2017)**, and it is vital to protect personal data as an integral facet of informational privacy, while the growth of the digital economy is also necessary to open new vistas of socio-economic growth. Given the growing importance of the digital economy, establishing a regulatory sandbox may be necessary; however, giving the government unrestricted and extensive powers to exempt government agencies from the 2019 Bill's provisions in some situations may contradict the 2019 Bill's intent and jeopardize an individual's fundamental right to privacy. Although the 2019 Bill relaxes some of the more restrictive requirements of the 2018 Bill, such as the requirement for data localization, it also appears to dilute a few of the law's most important features, which seek to protect data principals' privacy rights.

XIII. SUGGESTIONS

It may be proposed, based on the above-mentioned detailed discussions:

- A separate law regarding the right to privacy should be enacted to protect citizens' identities from identity fraud.
- A Central Communication Interception Review Committee should be established to look at and review the interception orders issued by the relevant authority.
- A data protection authority should be created to protect data and keep track of how data processing evolves.
- Any individual who attempts to collect information from a government resource or an official should face a penalty.