DE JURE NEXUS LAW JOURNAL

Author:

Siddhant Khare

Symbiosis Law School, Noida

1st Year, BA LL.B.

DATA PROTECTION BILL AND RIGHT TO PRIVACY – A CRITICAL ANALYSIS

ABSTRACT

Ravi Shankar Prasad, Minister of Electronics and Information Technology, introduced "The Personal Data Protection Bill" in the lower house on December 11, 2019. The bill seeks to ensure, among other things, the safeguards of individuals' privacy in relation to their personal data, the transparency of organizations and institutions processing personal data, and the establishment of a Data Protection Authority (abbreviated "DPA") for the various purposes that the Bill seeks to fulfil. The Bill is the Government of India's reaction to the long-standing demand for a "data protection framework" to secure individuals' personal data that they contribute to various internet services, deliberately or unwittingly.

Keywords – Privacy, Data Protection, Bill, Union Cabinet.

INTRODUCTION-

In this research paper, we will focus on a critical analysis of the data protection bill and right to privacy. It involves the starting scenario of the data protection bill and its major key factors. Also we will be analyzing the right to privacy and the collaboration among the same. There would also be various case laws reflecting the situation based on the topic and tell us about what exactly happened in the past related to it.

DATA PROTECTION BILL-

On July 31, 2017, the Government of India established a Committee of Experts on Data Protection, chaired by **Justice B. N. Srikrishna**, to investigate concerns relevant to Data Protection in India, and the report of this Committee was submitted on July 27, 2018. Later, the government made the Bill available to the public in order to solicit feedback and suggestions from various stakeholders, ministries, and consultants. On December 4th, 2019, the Union Cabinet approved a revised Personal Data Protection Bill, 2019, based on these suggestions. Later, on December 11, 2019, the Bill was introduced in the Lok Sabha and referred to a Joint Select Committee of both houses.

In **Justice K.S. Puttaswamy (Retd.) v. Union of India,**[1] the right to privacy was recently recognised as a basic right arising principally from Article 21 of the Constitution. To make this right meaningful, it is the responsibility of the State to put in place a data protection framework that promotes the common good while protecting citizens from threats to informational privacy posed by both State and non-State actors. The Commission must work with this notion of the State's obligation when developing a data protection framework.

MAJOR FEATURES OF THE BILL-

The Bill governs the processing of personal data by Indian states, firms incorporated in India, and international companies dealing with personal data of Indian citizens. The Bill establishes fiduciary data duties (i.e., the body deciding the goal and means of processing personal data) and requires that certain accountability and transparency actions be taken when discovering data. The Bill requires data fiduciaries to handle personal data only if the data principal (the person to whom the data relates) has given his authorization.

In addition, the Bill establishes a legal framework for the acquisition and use of personal information. The Bill proposes the creation of a DPA to control and execute the legal structure while offering a collection of rights and obligations for the processing of personal data. The Bill also gives the Central Government significant standard-setting powers, which the DPA is tasked with carrying out. The Bill's broad area of implementation is an essential feature. If enacted, it would apply to all corporations in India save those expressly exempted. Any organisation

[1] K.S. Puttaswamy and Ors. V.Union of India and Ors [W.P.(C). No.494/20121

that collects data through automatic techniques would be affected. The DPA has the authority to classify small companies based on turnover, data volume handled, and data collection reasons.

Furthermore, the Bill emphasises the importance of consent in the proposed data protection framework. The Bill also recommends that individuals' personal data be accessed only with their free, informed, and detailed consent, with provisions allowing such permission to be revoked. Any processing of data without such authorisation would be considered a violation, and fines might be imposed under Sections 11 and 57 of the Personal Data Protection Bill, 2019. Section 11 of the Bill creates a new category of' sensitive personal data,' which can only be treated with 'explicit consent.'

Section 12 of the Bill specifies the circumstances under which personal data can be treated without consent. If personal data is required for the benefit of primary data, legal procedures, medical emergencies, or the maintenance of law and order, the grounds are as follows. The Bill also empowers the Central Government to direct data fiduciaries to include confidential personal data or non-personal data in order for the Central Government to better plan service delivery or establish evidence-based regulations. Section 16 of the Bill requires data fiduciaries to provide methods for age verification and parental consent when processing sensitive personal data of minors. Furthermore, under Chapter V of the Bill, some rights are granted, such as the right to get certification as to whether or not data has been accessed, the right to correct inaccurate personal data, and the right to be forgotten.

"The right to be forgotten" encapsulates a significant portion of the legislation. Section 20 provides that the data principal has the right to prevent the continuous publication of his personal data if the purpose of the data has been served, the data principal's consent has been revoked, or the data has been unlawfully disseminated. The Bill also gives the DPA the authority to take actions to defend individual rights, prohibit abuse of personal data, and assure compliance with the law.

NEGATIVE ASPECTS OF THE BILL-

Although the Bill has many strong and progressive measures, there are some clauses and features that raise serious concerns about the Bill's efficacy in protecting people' data. They are addressed in the following paragraphs:

1. HARM AND DAMAGE TO PRIVACY:

The definition of 'damage' in the Bill looks to be troublesome for many stakeholders. According to the idea of damage, any discriminatory treatment, rejection, or removal of a service resulting from the assessment of the data principle would be protected under it. This Bill addresses discrimination in general, which imposes severe limits on business activities because many businesses must discriminate on many grounds in order to function properly. In truth, only certain sorts of discrimination are prohibited by the Indian Constitution. The Bill considers the likelihood of harm when considering what kind of protection and privacy safeguards should be incorporated into the design of business policies.

2. VOLUNTARY USER VERIFICATION:

Another concern levelled at the Bill is its provision allowing businesses to provide users the option to voluntarily verify their identity. If users do not verify their identity, they will be subject to government surveillance or analysis. This proposal will increase the danger of data breaches and entrench control in the hands of major social media corporations that can afford to establish and operate such verification systems. Furthermore, this increases the possibility of user privacy intrusions. It also ignores the fact that social media anonymity might have advantages such as whistleblowing and stalker protection.

3. NO CONSENT TRANSFER OF NON-PERSONAL DATA:

The Bill also requires businesses to share non-personal data with the government for public good and planning purposes. This will not only raise huge privacy concerns, but it will also have a terrible influence on businesses, since many corporations hold trade secrets in the form of non-personal data, which if revealed, may result in a setback.

RIGHT TO PRIVACY-

The right to privacy was established as a fundamental right by the Supreme Court of India on August 24, 2017. It was a widely celebrated decision that was regarded as one of the vanguards of human rights in the face of unprecedented technical breakthroughs. During the hearing, the Union Government informed the Bench that a committee was being formed to provide a framework for the preservation of the right to privacy and data protection regulations, chaired by **Justice B N Srikrishna,** a former Supreme Court judge. On the committee's advice, a bill was tabled in Lok Sabha on December 11, 2019. This also critically analyzes the law in the context of the right to privacy, writing a criticism of significant elements of the said bill and recommending essential

amendments to the bill before it is voted on. This paper does so by engaging in the contents of a webinar in which Justice Srikrishna provided some insights into the law and implies that some unfavourable alterations were made before it was tabled in Lok Sabha.

While hearing this case through a Bench of three erudite Judges, the Supreme Court remarked that there were decisions of Benches that were contradictory in their interpretation of the basic right to privacy. The learned Attorney General of India presented before the bench that in **M P Sharma v Satish Chandra**[2], District Magistrate, Delhi and **Kharak Singh v State of Uttar Pradesh**,[3] observations were made that the right to privacy is not particularly shielded in the Constitution, which were delivered by a Bench of eight and six learned Judges, respectively.

CONCLUSION-

The Personal Data Protection Bill is India's first step toward ensuring data privacy for its citizens and preventing data misuse. It emphasises the importance of obtaining the individual's consent before using his or her data for any reason. It also includes provisions for the establishment of an Indian Data Protection Authority to ensure that the proposed Bill is properly enforced. It is a long-awaited legislation since India lacked a comprehensive law to protect its residents' data, leaving citizens unprotected and vulnerable in a world rife with cybercrime.

While the Bill is impressive in some ways, it also has several shortcomings, such as a strong emphasis on harm without accurately characterizing it, and making it essential for businesses to exchange non-personal data. The fundamental flaw in the Bill, which has won it criticism from many lawyers, academics, and politicians, is the passages that offer exemptions to the government, allowing any government agency to avoid the proposed Act. This clause sparked serious and relevant concerns about the government's intentions, with Justice **BN Srikrishna,** whose committee developed the draft law in 2018, describing it as an attempt to convert India into an Orwellian state.

[2] M.P. Sharma v. Satish Chandra(AIR 1954 SC 300)

[3] Kharak Singh v. State of Uttar Pradesh (AIR 1963 SC 1295)