VOLUME 1 ISSUE 1

"Personal Data Protection Bill, 2019 vis-à-vis Right to Privacy"

V. Krishna Laasya

Tamil Nadu Dr. Ambedkar Law University, Tamil Nadu.

vklaasya@gmail.com

----------***----------

ABSTRACT

The Paper drafted on Personal Data Protection Bill, 2019 seeks to enforce the adjudicatory aspect and the measures taken by the Legislature in order to ensure safe protection and preservation of an individual's current important asset- Data Privacy and Confidentiality. It is to be analysed that though it is a positive step towards achieving fulfilment of goals of an individual's privacy, it is also integral that the guidelines issued be rigid and that the authorities appointed, adhere to them.

Privacy has been highlighted in a different perspective post Justice K. S Puttaswamy judgement. It is thus essential that the concept of Data Protection be understood through the context of privacy.

Key Words: *Data Protection, Data Fiduciaries, Committee Report, Advancement, Privacy.*

1. INTRODUCTION

The Ministry of Law and Justice have envisioned personal Data Protection Bill, 2019. The Personal Data Protection Bill has been introduced in the Lok Sabha on 11 December 2019, referred to the Standing committee on 11 December 2019 whose report of extension was granted to the second week of the Monsoon session of the Parliament.

It has been put forth by the Indian Parliament[1] with the objective of Data Protection granted to every individual, and the authority in control of the same is the Data Protection Authority (DPA). The Personal Data Protection Bill, 2019, keeps data access granted at the disposal of the Indian Government, Indian established companies in check.

2. FEATURES ADOPTED IN THE BILL[2]

The concept of consent being a major contributing factor to collection and analysis of an individual's data is also subject to the exception of no express consent necessary if the data is being utilised for emergency medical purposes, institution through legal proceedings or when a State is fulfilling its duty in providing amenities.

Data Fiduciaries have been bestowed with the following functions, namely undertaking of corrupt-free measures, adoption of measures like encryption to safeguard and protect personal data and establish their own feedback measures by making sure that the concerns and disputes of the individuals are addressed.

An important aspect of the Bill includes the usage of the data available on social networking sites which provide for information and utilise it in a reasonable manner.
Central Government is said to gain access of data from the Data Fiduciaries, provided it is non-personal data. This Bill has amended and revised the Information Technology Act, 2000 and deleted the failure of companies data protection provision.

3. JUSTICE SRI KRISHNA REPORT[3]

The Report has been prepared with the perspective of fusing modern practices with the traditional frameworks by incorporation of essential viewpoints addressing fears and opinions of Indians

[1] For the Bill by the Parliament, see <https://www.prsindia.org/billtrack/personal-data-protection-bill-2019>. Last accessed- 09 May 2020.
[2] Personal Data Protection Bill, 2019 as introduced in Lok Sabha- Bill No. 373 of 2019. See <https://www.prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf>. Last accessed 09 May 2020.
[3] For detailed Report of Data protection Bill, Justice Sri Krishna, see <https://www.prsindia.org/sites/default/files/bill_files/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill%2C%202018_0.pdf>. Last accessed 09 May 2020.

regarding personal data. In today's Digital Era, Data advancement has paved way for more streamlined researches, quicker access to information and for better prospects[4]. It is said that the Data Protection Bill is set to create not only internal but also a cross-border legal structure for data protection[5].

3.1 Data Fiduciaries

Any data that is sought to be protected ought to be to subserve for common good and in public interest. The Individual who is the owner of his/her personal data is to be the "Data Principal" as the concept of protection of personal data revolves around him/her. It must be brought forth that it is not only the individuals but also entities who are entitled to receive personal data, who must exercise reasonable care and act in conformation with the principles laid. These entities are thus called "Data Fiduciaries"[6]-Data Shared on the basis of Trust.

Ensuring that data is protected, there is a requirement for fulfilling goals, namely Power given to the Individual must be complete and not merely ostentatious. The growth of an economy is not merely fair minded but also must be empowering to the citizens.

In *Pico v. United States*[7], the US Supreme Court decided that banning access of certain books from the Library on grounds of being Anti- American was held to be not justified. It was not just for protection of individual's right to information but also for the sake of protection of State's Interest in promoting education. This envisages a policy where Individual is able to decide what to do with personal data and the entities requirement to carefully provide Data Protection and this in turn promotes the society's welfare.

---

[4] See Rohan George, Predictive Policing: Legal Implications, The Centre for Internet and Society, 24 November 2015. <https://cis-india.org/internet-governance/blog/predictive-policing-what-is-it-how-it-works-and-it-legal-implications>. Last accessed 03 May 2020.
Detection of Data Analysis in the case of money laundering. Business Today, 12 October 2016, Srinivas Tadigadapa Last updated 15 July 2019 16:45 IST. <https://www.businesstoday.in/current/economy-politics/how-big-data-and-analytics-can-help-india-fight-against-money-laundering/story/238397.html> Last accessed 03 May 2020.

[5] For Data Protection Bill and its Analysis, see will India's Proposed Data Protection Law protect privacy and Promote Growth by Anirudh Burman on 09 March 2020, <https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217 >. Last accessed 09 May 2020.

[6] For Analysis of Data Fiduciaries, Data Principle and Accountability, See Protection of Personal Data Bill, 2018 by DSCI and NASSCOM.
<https://www.dsci.in/sites/default/files/Protection%20of%20Personal%20Data%20Bill%2C%202018.pdf> Last accessed- 03 May 2020.

[7] For Argument placed by R. Pildes on Individuals Rights against State provided Rights, see Pico v. United States, 60 U.S. 279 (1864)

3.2 Jurisdictional Aspect

It has been recommended by the Committee that the objectives which will sort out the jurisdictional aspect include the need to protect the data, and to institutionalise a mechanism to conform that the data fiduciaries are operational.

The base forms through the objective territoriality where the acts have though been committed outside the territory, they should have caused a major effect on the jurisdiction[8].

The Nationality principle is sought to be adopted whereby the Data must be protected irrespective of the place of its process. Majority agree that the most important pre-requisite for Data Protection is the power granted by the Individual who is the owner of that information. This grants the benefit of user autonomy and consent gives a clear way of overcoming liability.

3.3 Building Blocks in Data Protection Regard

- *Data Personal in Nature*: Determination of Personal Data has undergone many changes and been fixed on the lines of relation to identified individual[9]. However, in the current decade it has borne to be difficult to come to a conclusion and thus data is now longer classified into identified or identifiable, it is rather being identified on the basis of degree of IP address. Thus a definition that can cater to all types of people must be developed. Another mechanism to achieve the same is de-identification which is a topic still in development.
- Another part to be analysed is the concept of sensitive personal data which is an iota of personal data and is categorised according to the circumstances. It is that data which is classified as such owing to the fact that it might cause more harm to the owner of the data and greater amount of confidentiality is required. Some examples include Passwords, Genetic Data, Finger Prints, Religious Data.
- *Consent*: This is the foundation of all data plans of the Government or any Data fiduciary. Consent is required to be express and the individual ought to be in a completely conscious state of mind. Generally, the consent forms are complex and require that the individual be thorough

[8] For the aspect of Jurisdiction, Christopher Kuner, Data Protection Law, 18(2) International Journal of Law and Information Technology 2010 and see Banyan Tree Holding v. Murali Krishna 2010 (42) PTC 361.
[9]For the relation of Data being ether identified or identifiable, See OECD Guidelines on Protection of Privacy 2013 <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm >. Last accessed 06 May 2020.

of the whole document which is not the current scenario as the Individual might not read or understand the form[10]. Thus, there is a need for greater protection in terms of orality and important parts must be made understood to the individual.

- *Enforcement Mechanism*: There can be a possibility of model forms drawn to adhere to the framework and annexures, schedules attached to provide for better data protection. Non-compliance is to raise the penalty thus enabling for more compliance in data protection.
- The structure is said to influence the data fiduciaries on the lines of consent of the individuals with emphasis on the obligations.
- If the purpose of the consent obtained changes or differs from the original consent, then consent for the same must be obtained from the individuals.

3.4 Recommendations in the Report

The committee has raised the following recommendations namely:

a. Personal Data obligations shall be both by private and public entities[11].
b. Even if the data has been wrapped in anonymity, the regulations set by the Data Protection authority ought to be followed[12].
c. Sensitive personal Data like passwords, fingerprints, must be in accordance with law and must remain in careful custody of the Data Fiduciaries or Government authorities[13].
d. Individuals who are below 18 years of age, are to be considered children and separate guidelines are to be adopted for same, which requires constant check by the Government[14].
e. Data Fiduciaries and the relationship with the individuals should be of a trust-based nature and though, a level of flexibility is allowed they should be careful and cautious.

3.5 Personal Data Breach

The principles that underline the definition of personal data Breach include integrity, which is to prevent unauthorised release of data, confidentiality that is to prevent the involuntary disclosure

[10] See B. W. Schermer et Al, The crisis of Consent and stronger legal protection, Ethics and Information Technology 2014.
[11] See Section 3(3) and 3(15) of the Personal Data Protection Bill, 2019
[12] See sections 3(3), 3(16) and 61 (6)(m) of the Personal Data Protection Bill, 2019.
[13] See Sections 3(35) and 22 of the Personal Data Protection Bill, 2019.
[14] See Section 23 of the Personal Data Protection Bill, 2019.

of data and availability, which leads to destruction or loss of data[15]. Thus, it has established the concept that a breach that has affected the integrity, confidentiality and availability is only the breach that forms a part of the personal data breach under the Personal Data Protection Bill, 2019.

Based on the degree of severity, the case is to be notified to the Data Protection Authority. A harmful effect to the rights of Individuals require the immediate intervention of the Data Protection Authority who will offer advice on how to curb the breach.

If the breach is considered relevant to the Authority, then only it is to be made aware to the individual. It is required to inform the individuals, not only if the breach pertains to him/her, but also so that the individual may take appropriate steps on his part to safeguard from the breach.

4. PRIVACY IN LIGHT OF *PUTTASWAMY*[16] JUDGEMENT

The Supreme Court formulated that the Right to Privacy flows from Right to Life and Personal liberty, thus emphasising on the level of privacy of an individual's data and the need to retain it for himself. The aim of such a privacy is that every person should have complete power and self-determination[17]. In order to preserve the right to privacy there is a requirement to fulfil the pre-requisites of an authorised interest of the State, structure to proportionate the interest and the restriction placed must be legal. It is noteworthy that freedom is one of the touchstone of constitution and is the raison d'etre of our independence.

This concept of Privacy has paved way for many data legislations, judgements and the Data Protection Bill, 2019. Privacy and Data Protection is inter-related and data protection can be considered as the legal structure that fits privacy within it.

[15] Analysed and embodied in the White Paper of Committee Experts on the Data Protection. See <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf >. Last accessed 09 May 2020.
[16] Justice K. S. Puttaswamy v. Union of India, 2017 (10) SCALE 1, 2017 10 SCC 1, WP (C) 494/2012. Coram- Justice DY Chandrachud, Justice Jagdish Singh Khehar, Justice Abdul Nazeer, Justice S. Bobde, Justice Jasti Chelameswar, Justice Rohinton Nariman, Justice Abhay Sapre, Justice Sanjay Kishan Kaul.
[17] Bert- Jaap Koops et Al., A Typology of Privacy, Pennsylvania University Journal of International Law (2017) p. 566 and cited by J. Chandrachud in the Puttaswamy Judgement, *supra* 4

5. SPD RULES AND SECTION 43A OF THE INFORMATION TECHNOLOGY ACT, 2000

The OECD principles provide that the security undertaken to protect data include physical, organisational and informational measures[18] and has stated that the Fundamental Principles of Data include Free flow and implications include that of processing of data domestically.

Under Section 43A of the Information Technology Act, 2000 SPDI Rules have been formulated with emphasis on protection of data[19]. These Rules analyse implementation of the policies that conform with control mechanisms to protect the nature of data. They have categorised Passwords, fingerprints, medical records as part of Sensitive Personal Data and any company incorporated as a body corporate is to obtain consent to use the sensitive personal data.

CONCLUSION

It has been analysed that the Bill does not give as much rights to the individuals as it does to the Government. It over bears the government with extension in duties and rights and provides a troubling relationship between the concept of privacy and data protection. It does not address the actual concerns of the data privacy and provides an eyewash by way of committee report on data privacy headed by Justice Sri Krishna.

It has been an existent hope for many that after the Justice Puttaswamy judgement that changed the perspective of privacy in the Indian minds, the current Data Protection Bill will strive and bring out a better analysis of the same, which was not met adequately.

[18] OECD Guidelines on Protection of Privacy and Transborder flows of Personal Data (2013) at <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm >. Last accessed on 09 May 2020.

[19] On 13 April 2011, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 have been issued under Section 43 -A read with Section 87 (2) of the Information Technology Act, 2000.

REFERENCES

Websites

1. For the Bill by the Parliament, see <https://www.prsindia.org/billtrack/personal-data-protection-bill-2019>. Last accessed- 09 May 2020.
2. Personal Data Protection Bill, 2019 as introduced in Lok Sabha- Bill No. 373 of 2019. See <https://www.prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf>. Last accessed 09 May 2020.
3. Detailed Report of Data protection Bill, Justice Sri Krishna, see <https://www.prsindia.org/sites/default/files/bill_files/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill%2C%202018_0.pdf>. Last accessed 09 May 2020.
4. For the relation of Data being ether identified or identifiable, See OECD Guidelines on Protection of Privacy 2013 <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm >. Last accessed 06 May 2020.
5. Analysed and embodied in the White Paper of Committee Experts on the Data Protection. See <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf >. Last accessed 09 May 2020.
6. OECD Guidelines on Protection of Privacy and Transborder flows of Personal Data (2013) at <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm >. Last accessed on 09 May 2020.

Papers and Research Articles

1. Rohan George, Predictive Policing: Legal Implications, The Centre for Internet and Society, 24 November 2015.
2. Srinivas Tadigadapa, Detection of Data Analysis in the case of money laundering. Business Today, 12 October 2016, Last updated 15 July 2019 16:45 IST.

3. Anirudh Burman- For Data Protection Bill and its Analysis, see will India's Proposed Data Protection Law protect privacy and Promote Growth on 09 March 2020.
4. B. W. Schermer et Al, The crisis of Consent and stronger legal protection, Ethics and Information Technology 2014.
5. Bert- Jaap Koops et Al., A Typology of Privacy, Pennsylvania University Journal of International Law (2017) p. 566 and cited by J. Chandrachud in the Puttaswamy Judgement, *supra* 4.

Research reports

1. For Analysis of Data Fiduciaries, Data Principle and Accountability, See Protection of Personal Data Bill, 2018 by DSCI and NASSCOM.
2. For the aspect of Jurisdiction, Christopher Kuner, Data Protection Law, 18(2) International Journal of Law and Information Technology 2010 and see Banyan Tree Holding v. Murali Krishna 2010 (42) PTC 361.