INDIAN JOURNAL OF LAW, POLITY AND ADMINISTRATION

ISSN: 2582-7677

ANALYSIS OF DATA PROTECTION LAWS

MINI.S

Assistant Professor, Govt. Law College, Ernakulam

Abstract

During this pandemic time, there is a hike in the use of digital platforms and sharing of personal data in cyber space, resulting in exploitation of the same. As cyber space users are increasing there is huge data collected by many service providers, app developers etc. This data is being transmitted to many others without the consent of the subject. India has drafted Personal Data Protection Bill, which is yet to be passed in Loksabha. Data protection is a challenging area for many countries. In this paper, the sections of the Bill is analyzed and a comparison with General Data Protection Regulation is also effected. General Data Protection Regulation lays down rules relating to the protection of personal data in European Countries. Personal Data Protection Bill follows main features of GDP, but with more clarity and precision. This paper analyses the salient features of the Personal Data Protection Bill and had analysed the positive as well as the negative aspects of the Bill and had studied the historical aspects of data protection.

Keywords:- Data Protection, Privacy, Data Fiduciary, Data Principal

Analysis of Data Protection Laws

The pandemic Covid-19 had seen many changes in the world, both positive and negative. Many countries had resorted to new technologies for governance. The year 2020-21, due to pandemic, can be considered as the years in which works are digitalized and plethora of online platforms were exploited for academic as well as other purposes. Huge data was streamed and there is immense data flow in the cyber space. As cyber space users are increasing there is huge data collected by many service providers, app developers etc. The collected data includes financial details, bank details, health details etc. These data can be misused by the holders of this data. There are agencies which collect these data from these providers and they may sell it to other agencies.

Considering all these, Govt. took significant steps in tech policy and data regulation of non-personal health data, financial data etc. In India, we have IT Act 2000, to protect this data. But as it is not sufficient enough to meet the challenges, the Ministry of Information and Technology had constituted an expert committee, under the chairmanship of Retd. Supreme Court Judge, Justice.B.N. Srikrishna, for formulating a

ISSN: 2582-7677

legal framework relating to personal data that can work as a template for the developing world.[1]The Committee formulated the first draft of Personal Data Protection Bill in July, 2018. After much discussions and soliciting comments from public and key stake holders, Revised Personal Data Protection Bill was cleared by Union Cabinet on Dec 4 2019 and the government introduced Data Protection Bill in Loksabha on Dec 11, 2019. The same was referred to standing committee and the report of the committee was expected on the last week of Budget Session, 2020.

The bill intended to provide protection of the privacy of the individuals relating to their personal data.[2]The Bill tries to protect personal data as an essential facet of informational privacy. [3]Thus the sensitive personal data like health data, financial data, official identifier, sex life, biometric data, sex status, religious or political beliefs are protected by this bill. The bill prevents the Central Govt. from framing of any policy for the digital economy without governing personal data. [4]

Tracing the History of Data Protection Laws

The history of Data Protection can be traced back to the late 1960s, when the computers first started to collect and process personal data. The Younger Committee, in UK conducted a study and concluded that existing remedies, including privacy remedies under common law, were inadequate to address this new threat.[5]Its report identified the various existing data protection mechanisms.

In Germany, in the State of Hessen, adopted the world's first designed law for regulating automated data processing in public sector in 1970.[6] The foundation of data protection law was that the processing of personal data must be fair and to ensure that data is protected against the risk of intrusion in private life and the risk of unfair discrimination.

In 1973, the Council of Europe (CoE), also issued a resolution on the protection of individuals vis-a-vis electronic data processing banks. The data protection law had basically focused on providing reasons for enabling the person's privacy. CoE adopted Convention 108, which required states to enact additional legislation to enact additional legislation to ensure right to data protection. This Convention also laid down

[1] A Free and Fair digital Economy, Protecting Privacy, Empowering Indians, Chapter 1, Introduction, DPC Report,p.3,*available at* https://www.meity.gov.in/writereaddata/files/Dat_Protection_Committee_Report.pdf (last visited on 14/05/21)

[2] Objects of Data Protection Bill, 2019

[3] *Id*

[4] The Data Protection Bill,2019 ,s. 91(2)

[5] The history of Data Protection Law, Golden Data Law, Sep.20 , 2018,*available at* https://medium.com/golden-data/data-protection-law-how-it-all-got-started-df9b82ef555e (last visited on july 15,2021).

[6] A guide for Policy Engagement on Data Protection, Part-1, Data Protection , P 09/98, *available at* https://privacy international.org/sites/default/files/2018-09,(last visited 10thmay 2021).

ISSN: 2582-7677

provisions for trans-border flows of personal information. Another important development was the Treaty of Lisbon, 2007. This Charter recognizes Privacy[7]and Data protection[8] as important fundamental right

Since 1960, when the IT sector developed, data is stored in virtual platform. Considering the concern of nettisons, new laws were introduced both nationally as well as internationally. Modern data protection law is the outcome of EU's approach to balancing the risks & benefits of automated data processing. [9] The new law ensures fairness.

The bill permits the processing of personal data, for the purposes of employment by data fiduciary [10]or by the data principal, who is an employee of data fiduciary. [11]The Bill also provides, the instances in which the personal data which are not sensitive personal data may be processed without obtaining the consent of the person[12] and enumerate the purposes for which data can be processed.[13]

So a question arises, if data can be protected as property right? Whether data can be considered as property?

Defining Data Protection

The main issue with respect to data protection is its definition. The issue of data protection is mainly connected with issue of right to privacy of other persons. The definition of privacy is to be precise and is defined as a part and parcel of a right to be let alone,[14]Treating Privacy as non interference in another's life. Privacy is a condition of "limited accessibility" consisting of 3 elements, secrecy (the extent to which we are known to others), solitude (the extent to which others have physical access to one self) and anonymity (the extent to which we are the subject of others attention).[15]

In modern technological period, we want privacy but at the same time, we are sharing many of our personal details in social media and for obtaining certain services, like health care, insurances, social benefit schemes etc. Thus with or without our knowledge, one's data is generated and transmitted to other companies. This will affect the confidence and faith of persons in the government and other sectors.

Comparative Analysis with GDPR

[7] Lisbon Treaty,art.7
[8] *Id*.,art.8
[9] *Id*
[10] The Data Protection Bill,2019.s. 3(13)
[11] Id.,s.13(1)
[12] *Id* .,s. 14 (1)
[13] *Id*., s. 14 (2)
[14] Warren S.D. Brandeis L.D, *The right to Privacy, Harvard Law Review*, 1890(4),P 193,205
[15] Gavison.R, *Privacy and Limits f Law, Yale Law Journal*, 1980 (89) P. 421, 428-436.

ISSN: 2582-7677

GDPR(General Data Protection Regulation), which came into force in May 2018, which is the law on personal data protection and privacy in European Union. This regulation lays down rules relating to the protection of personal data.[16]

GDPR contains 11 chapters and 91 articles. The word personal data is defined in Data Protection Bill, 2019[17] with more clarity than in GDPR.[18]On analysis it can be seen that the data in both GDPR and DPB are same but GDPR had included some additional grounds as legitimate interest[19] and performance of contract[20] in which such data can be processed. Sec. 12(a) of the Act, permits processing of personal data for performing any function authorized by law. This provision enables the data principal to process data regarding a person even without his consent. So this section had to be administered with much caution as it gives wide power on the state to process data of an individual. Thus the section 12 to 15 allows a data principal to process the data for public interest[21]or for the purpose of any medical emergency. [22]These Sections (Sec 12-15) can be considered as the crux of this Bill.

In GDPR, the personal anonymous data is out of scope.[23] The regulation clearly applies to information relating to an identified or identifiable person thereby anonymous data is ousted from the scope of GDPR

In Indian Bill, the central Govt. may direct organizations to disclose anonymised personal data.[24]As the definition clause in Indian Bill is very wider[25]it applies higher standards of data protection. Much caution has to be taken towards critical personal data about which, there is no reference in GDPR. Central Govt. is authorized to prescribe new categories of sensitive personal data. [26]

Right to Privacy

[16] General Data Protection Regulation ,art.1. 1) This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. 2) This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. 3) The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data

[17] *Supra note* 10,s. 3(29)

[18] *Supra note* 16, art. 4(1) personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[19] *Id*, art.6(1)(f)

[20] *Id,* art. 6(1) (b).

[21] *Supra note* 10,s.14©

[22]*Id*.,s. 12 (d).

[23] *Supra note* 16, art. 1

[24] *Supra note* 17, Clause 91.

[25] *Id*.,Sec 3(29)

[26] *Id*.,Sec3(36)

ISSN: 2582-7677

The milestone decision of Supreme Court on right to Privacy [27]reaffirmed that this is a fundamental right guaranteed under the Constitution of India. It had acknowledged that right to privacy was integral to freedoms guaranteed and was an intrinsic aspect of dignity, autonomy and liberty. The case was regarding the legal validity of Aadhar database. This case overruled the earlier decisions[28] of Supreme Court on the right to Privacy. In these cases, State argued that right to Privacy is not a fundamental right as specifically ported by Constitution. In the present case, Chandrachud.J, observed the dangers in data mining and the necessity of a data protection law to protect the privacy of the individuals. Accordingly such a law is necessary for the protection of personal data of citizens from exploitation.[29]Aadhar had complied with the Triple test [30] which states that any law can interfere with the personal liberty of an individual satisfies- legality, need & proportionality)

Right to Delete

After processing data, the same shall be deleted from public domain. If the processed data has to be retained for a longer period, the express consent of the concerned person should be obtained.[31]But the period which will be considered for applying the provision to apply is not specified in the section. A very wide authority is given to the data Principals to seek information from data fiduciaries about their individual data. [32]Similarly, data Principal can erase any immaterial information of a data fiduciary without any formality.[33]So the Sections 17 and 18 points to the necessity of a control over the data principal, as the authority is vested with wide powers.

Rights of Data Principal

The data principal has a right to confirm from the data fiduciary, whether the personal data collected has been processed.[34]The data principal has the right to correction and erasure of personal data being processed if found incorrect.[35]If the data principal feel necessary that, his personal data which is being processed or ought to be corrected or to add more information or to erase some data, he can make a request to the data fiduciary for the same. After receiving such a request, [36]if data fiduciary feels that such amendment,

[27] *Justice.K.SPuttuswamy (Retd) v Union of India*, (2017)10SCC 1, AIR 2017 SC 4161
[28] *M.P.Sharma v Satish Chandra, District Magistrate, Delhi*(1954)SCR 1077 : *Kharak Singh v State of Utter Pradesh*(1964)1 SCR 332
[29] *Supra note* 27.
[30] *Maneka Gandhi v Union of India*, (1978)AIR 597
[31] Supra note 26, s.9(2)
[32] *Id*., s.17(1)
[33] *Id.,* s.18.
[34]*Id.,* s.17(1)(a)
[35] *Id.,* s.18(1)
[36] *Id*

ISSN: 2582-7677

correction or addition is not required, he may intimate the same to the data principal by stating the objections. If the data principal is not satisfied with the justification provided, he may require the data fiduciary to mention alongside the personal data to which the amendment or deletion is sought, to the effect that the same data is disputed by the data principal.[37]

As per this section, an objection is raised by the data principal and same is rejected, he is not left with any other option to restrict the publication of the data. Only by endorsing that the processing of that data is objected, the data principal's grievance can't be redressed and the bill is silent regarding the scope of appeal. If the objection is rejected without justification, the data fiduciary can be penalized with a fine of 5000/- [38] The processing of data cannot be prevented by the data principal. So much power is cornered on the data fiduciary. This section vests wide power on the data fiduciary to reject the application submitted by the data principal and to publish the same. But the data fiduciary is to pay a penalty of Rs.5000/- per day & up to 10 lakh rupees in case of significant data fiduciary.[39]

If the request of the data principal under section 18 is accepted by the data fiduciary, amendment to that effect has to be carried out and to be notified to concerned authorities and stake holders.[40]

Processing data without consent

The bill lays down situations in which data can be processed without obtaining consent from data principal. The state is entitled to process data of a data principal for executing the functions of the state authorized by law.[41]Such processing is necessary, for rendering any service to data principal or for providing authorization for doing any activity or if such data is processed as authorized by any central or state law or for the compliance of any order of a judicial or quasi judicial authority or in life saving situations or medical aid in pandemic situation or in any emergency or disaster. In all such situations, state can process data without the consent of the data principal.

This provision will enable the state to process the data of any person when the situation demands. There is possibility of misuse this section as it is possible to process the data for political gain. The government can process the data of opposition and can retain the data or publish the same without entertaining the objection raised by the data principal.

---

[37] *Id.,*s.18(3)
[38] *Id.,*s.58
[39] *Id.,* ss. 57 -66, Chapter 10 , 'Penalties and Compensations'
[40] *Id.,* s.19
[41] *Id.,* s. 12

ISSN: 2582-7677

Duration of Retention

The processed data has to be deleted from public domain once its purpose is fulfilled. And if any data is to be retained further, express consent of data principal is necessary.[42] This provision is framed loosely as it does not specify the time limit within which the data has been deleted. This section also provides excessive power on the data fiduciary. If the processed data is not deleted even after its purpose, the remedy available to the data principal is not at all addressed in the Bill. The Bill does not explain the term, "purpose for which it is processed".

The data fiduciary need not intimate the source of personal data, if the same is obtained from any other source. Similarly the data fiduciary is to inform about the breach of any personal data processed by the data fiduciary to the authority.[43]

The duties of data fiduciary is vaguely stated in the Bill[44]. It lacks clarity and it does not lays down the extend of authority of the data fiduciary. Hence there is possibility to exert excessive power.

Transparency in Processing Data

The data collected by data fiduciary has to provide certain data available like details of the data collected, the nature of data collected, how they are protecting the data collected from data principal. The auditor appointed under this Bill has to provide data trust code to each data fiduciary that will help in assessing the credibility of each fiduciary.[45]The Bill empowers the data principal to withdraw the consent given through a data manger[46] which will be considered as a direct withdrawal of principal.[47]The Bill also restricts the transfer of sensitive personal data outside India. The Bill acknowledges the rights of children[48] just like in GDPR.[49]But the bill is silent as regards the subject of mentally disabled persons. The way in which the data relating to such a vulnerable group is to be processed has to be dealt with separately and elaborate provision has to be made for the collection and processing of data.

Analysis of the Bill

[42] *Id.*,s.9
[43] *Id.*,s.25
[44] *Id.*,s.10
[45] *Id.*,s.23(1)(f)
[46] *Id.*,s.23(3)
[47] *Id.*,s. 23(4)
[48] *Id.*,s.16
[49] Supra note 16. art.8

ISSN: 2582-7677

The Bill tends to protect the personal sensitive data of the data principal. The provisions are intended to provide safe utilization of virtual media. The provision of the duties of data fiduciary[50] has to be properly identified and the jurisdiction limits should be properly stated. The data principal should be able to approach the appropriate authority if his rights as provided in the Bill is denied. The powers of data manager[51] has to be identified properly. The Bill protects the data from being transmitted outside India. In this way , the data of a data principal can be kept in tact. The right to be forgotten, the right to erasure provided in the Bill helps the data principal in restricting his information from viewed by public for a limited period.

Conclusion

In the case of consent to be given by the data principal, many aspects have to be considered. India being a country with different languages, it is highly necessary that the written consent form should be provided both in English as well as in regional language. It should be ascertained that the person who gives consent had in fact consented to process his data. It must be ascertained that the person reads and understands the consent to process and only after that their data has to be processed.

The limits of the powers and duties of the data fiduciary have to be clearly recorded, so that the power is not misappropriated by the authority. By imposing heavy penalties on the data fiduciary, the Bill had tried to maintain equilibrium.

On an overall analysis of the Bill it can be seen that the Bill protects the data from misuse. The Bill is much more effective than its contemporary GDPR, which is discussed in this paper. By giving a wide definition for the term Data Protection, the ambit of the Bill is extended.

[50] *Supra note* 43
[51] *Supra note* 45