Page 1856 - 1863

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 4

2020

The Personal Data Protection Bill, 2019: Boon or Bane

SAYANIKA DEY[1] AND SNEHA CHATTERJEE[2]

ABSTRACT

In the recent acquisition matters relating to cyberlaw has gained a wider approach. It is an important upcoming sensitive topic in the world that is to be dealt with. The advancement of scientific technology has paved the way for international law relating to data protection. The authors of the article have portrayed a comparative analysis of various countries in the context of The Personal Data Protection Bill, 2019. Main issues arising out of it has been discussed vividly. Critical analysis of cases in such light has been traced. The paper also focuses on data protection laws that are followed by United States of America putting forward its pros and cons.

The lacuna of the above-mentioned Bill that are prevalent in India has been mentioned in the paper. Suggestions and measures have also been observed in order to overcome such loopholes. Thereby a beneficial law relating to data protection at national level should grow which in turn will enhance the development of the country. The authors bring in forth the comparative analysis of different nations along with suggestions that are needed to be implemented in India on the ground of data protection so as to intensify the backdrop.

The methodology of our research is Doctrinal one.

Keywords: *Comparative analysis, loopholes, implementation, cyber laws, data protection laws.*

I. INTRODUCTION

'Cyberspace' a synonym for internet has become the heart and soul of a person's life so much so that, today, we cannot think of doing anything without the help of internet. From shopping to buying groceries, from booking train tickets to booking cabs for regular commute, from making hotel reservations to ordering food online, from searching a person in social media to researching for an article, from withdrawing money from atm to transferring money to another account through e-banking, from playing online games to doing business online, we cannot

[1] Author is a student at Amity University, Kolkata, India.
[2] Author is a student at Amity University, Kolkata, India.

 [ISSN 2581-5369]

think of doing anything without being hinged on internet aka cyberspace.[3]

However, one of the major backdrops for India's economic and social growth as a developed Nation State is the absence of a proper codified data protection law which could govern and penalize the transaction causing transgression to the society. It is quite disheartening to see that when every other developed Nation has already enacted a strong data protection law, India is still lagging behind and has just realized, after the leakage of data from WhatsApp and Facebook, the need for a strong enacted law for protecting sensitive information.

Every other day, we are falling prey to some kind of violation of our right to privacy, which has now been declared as our fundamental right. It is imperative for us to disclose our medical records to the doctor who stores that information in their software. Also, the operations and the pathology tests which are being conducted in the labs are being recorded. A leakage of those information would amount to gross violation of the basic human right. This has actually happened in Germany where millions of information of Indian patients including images have been leaked on the internet and are available for everyone to see, but there is no available amelioration for this leakage since India does not even have a data protection law to deal with these types of situations![4]

We have all been the eye witness as to how cyberstalking has taken lives of innocent girls. But to our utter dismay, there is no proper legislation to control cyberstalking except for the provision of Indian Penal Code defining as to which would amount to cyberstalking.[5] There are no remedy available to the victims of cyberstalking than to go for mutual determination.[6]

Every day, we get calls from different unknown numbers, basically fraudsters, asking for credit card or enquiring about our atm pin or frightening that our card is getting blocked. From where do they get the numbers? Quite expectedly from our telecom service providers. Here the question arises as to how could these telecommunication providers leak our personal information to a third party without getting penalized for their actions. The answer is that the sole reason for such violation, is we do not have a codified legislation to tackle the same.

Although, this has been dealt in detail in the later part of the article, it is needless to mention here that there is an impending need for rationalization of a general data protection laws which

[3] Dr. Sudhir Kumar Sharma, *Cyber Security: A Legal Perspective*, Volume 9 International Journal of Computer and Internet Security 1-11 (2017), https://www.ripublication.com/irph/ijcis17/ijcisv9n1_01.pdf (last visited Feb 18, 2020).
[4] Ibid.
[5] Abhimanyu Mathur, Cyberstalking Law: Ill-equipped to protect women, non-existent for men Times of India (2017), https://timesofindia.indiatimes.com/city/delhi/cyberstalking-law-ill-equipped-to-protect-women-non-existent-for-men/articleshow/59179132.cms (last visited Feb 18, 2020).
[6] Ibid.

 [ISSN 2581-5369]

would be applicable to all kind of data transaction in India and which would apply to every individual and every person residing in India or doing business, at any point of time.

II. INDIAN OUTLOOK: METAMORPHOSING PHASE

The absence of a codified data protection legislation was not being felt in the yesteryears as is being vividly observed in the current scenario. Lately, the Apex Court has been of the opinion that right to privacy is a newer concept of fundamental right being achieved under Article 21 of the Constitution and as a part of the freedoms guaranteed under Part III of the Constitution[7] in the celebrated case of biometric identity scheme of Aadhar.[8] However, keeping in mind the dependency of the contemporary society over the cyberspace has constantly put forth indecision about the actual implementation and abidance of the judgment.

The claim for the recognition of the right to privacy as our fundamental right can be traced back to 1962 where the outnumbered judges were of the viewpoint that right to privacy is a fundamental right, however dissenting opinion surfaced the judiciary until 2017, when at last the Court decided to declare it as a fundamental right. Since 1995, after Videsh Sanchar Nigam Limited (VSNL) brought internet service to India, it never looked back to the orthodox method of communication and from then, every citizen of our country has become so hooked into internet that we cannot imagine one day without internet.

In the recent times, however, after the verdict of the Supreme Court in the case Justice K.S. Puttaswamy, a data protection bill named as "A Free and Fair Digital Economy: Protecting Privacy and Empowering Indians"[9] was tabled for the winter session of Parliament in order to carb the so-called 'data monopolism' and 'data imperialism'[10], to control the workings of the companies and corporate houses who, basically works with the data of public.[11]

III. THE PERSONAL DATA PROTECTION BILL, 2019: BREAKDOWN

The Data Protection Bill, 2019 preceded the Data Protection Bill the draft bill of Personal Data Protection, 2018. The Bill was constructed as a result of the verdict of the Hon'ble Apex Court

[7] Jyoti Panday, India's Supreme Court Upholds Right to Privacy as a Fundamental Right—and It's About Time Electronic Frontier Foundation (2017), https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time (last visited Feb 19, 2020).

[8] Justice K.S. Puttaswamy (Retd.) v. Union of India, WRIT PETITION (CIVIL) NO. 494 OF 2012 (2018).

[9] Arindrajit Basu & Justin Sherman, Key Global Takeaways From India's Revised Personal Data Protection Bill LAWFARE (2020), https://www.lawfareblog.com/key-global-takeaways-indias-revised-personal-data-protection-bill (last visited Feb 19, 2020).

[10] Ravi Shankar Prasad, India views its privacy seriously, data imperialism not acceptable Financial Express (2019), https://www.financialexpress.com/industry/technology/india-views-its-privacy-seriously-data-imperialism-not-accepta ble-ravi-shankar-prasad/1756321/ (last visited Feb 19, 2020).

[11] Amber Sinha & Arindrajit Basu, The Politics of India's Data Protection Ecosystem Engage EPW (2019), https://www.epw.in/engage/article/politics-indias-data-protection-ecosystem (last visited Feb 19, 2020).

 [ISSN 2581-5369]

where the Court held that privacy right is considered as the fundamental right under the Indian Constitution.[12] Clear guidelines have been laid in the Bill regarding its application where Personal Data being processed is focused on rather than the provincial frontier.[13] The Draft Bill of 2018 kept unacknowledged data ambit while in the Bill of 2019, an exclusion has been laid down in respect of anonymized data that should be communicated to the governing entity so as to provide with better services.[14] Modifications have been made in lieu of the definition of anonymization so as to comprise the data that satisfy the requisites of anonymization standards.[15] However few provisions that has been laid down in the Bill is not applicable to manual operations of small bodies and that comes under the purview of Data Protection Authority.[16] The Bill of 2019 also lays emphasis on the fact that it will have an over-ridding effect where the provisions are inconsistent in nature.[17]

The Bill has stressed on the fact that after the completion of the purpose or the process the data obtained should be deleted.[18] If the data is kept for a longer period, then there should be the consent of the individual or the party regarding the same and the consent should not be implied one it should be expressive.[19] The Bill however, does not talk about the time period as to how long over rule the provision of Section 4 of the Bill. The Bill also deals brings into effect about the procedure to certify the minor person's age and that it specified in the systematization of the Bill.[20] The Data Fiduciaries does not incline into it.[21] Similar in case of Privacy by Design Policies will be verified by the competent authorization which were earlier chosen by the Data Fiduciaries and was mandatory to put it forth in the official website of the same.[22] The tenure to scrutinize the same is provided in the bill in the regulations. In the Bill, there has been favored expulsion of search engines. There should be a justifiable reasons that will allow the action of the search engines.[23]

The Bill does not contain in the ambit of Sensitive Personal Data definition the word passwords.[24] The Draft Bill of 2018 needed the sanction to continue the process of Sensitive

[12] *"The Personal Data Protection Bill, 2018: A Summary" dated July 30, 2018 Available at:* http://www.cyrilshroff.com/wp-content/uploads/2018/07/Personal-Data-Protection-Bill-2018.pdf *(last visited Feb 20,2020).*
[13] *Section 2 of* the Personal Data Protection Bill, 2019.
[14] *Section 91(2) of* the Personal Data Protection Bill, 2019.
[15] *Section 3(2) of* the Personal Data Protection Bill, 2019.
[16] *Section 39 of* the Personal Data Protection Bill, 2019.
[17] *Section 96* of the Personal Data Protection Bill, 2019.
[18] *Section 9(1) of* the Personal Data Protection Bill, 2019.
[19] *Section 9(2) of* the Personal Data Protection Bill, 2019.
[20] *Section 3(33) of* the Personal Data Protection Bill, 2019.
[21] *Section 16(3) of* the Personal Data Protection Bill, 2019.
[22] *Section 22 of* the Personal Data Protection Bill, 2019.
[23] *Section 14(2)(h) of* the Personal Data Protection Bill, 2019.
[24] *Section 3(36) of* the Personal Data Protection Bill, 2019.

 [ISSN 2581-5369]

Personal Data when there was observance of the important effects.[25] The trustees should only fulfill the requisite to make the Data Principal[26] aware of serious damage.[27] A broadened right is given in the hands of Data Principals where they have the right to seek from the Data Fiduciaries there individual data.[28] The right also includes an approach to have a view on the entities of the Data Fiduciaries about the type of personal information communicated and the entities that have assessed the personal information.[29] The Bill of 2019 has entrusted in it the right to remove immaterial information of the individual.[30] The Principals of Data possesses the capacity to erase such immaterial information straight away and even there is no need of adjudication.[31] A modern division has been implemented in the class of Data Fiduciaries known as the consent managers and it has been mentioned in the Bill.[32] In the Bill of 2019, the principals of data can put forth or eliminate their consent through the consent managers or by their own.[33] However these managers should register with the competent body mentioned in the provisions of the Bill.

The Bill of 2019 has paved the way for Social Media Intermediaries.[34] It falls under the division of Data Fiduciaries. These entities link with the users for creating, modifying, uploading, sharing or accessing data. The action of these entities have effect on the integrity and sovereignty of the nation as it involves a huge involvement of the users and it is apprised by the Government of India.[35] These apprised entities need to enable the users that register for it or to practice the services from sitting in India to verify the accounts voluntarily.[36] The Bill of 2019 has narrowed down the drafted bill of 2018 with regards to localization and Cross Border Data Transfers. There is no need for localization and it shall be only followed for personal information. However, there is a need for storing Sensitive Personal Data in the country of India and it can be send abroad for processing.[37] Personal information that are critical in nature should be processed in the country of India itself, however certain exceptions do exist.[38] The evolvement of advanced technologies in machine learning and artificial intelligence has been

[25] Anon, (2018). *THE PERSONAL DATA PROTECTION BILL, 2018*. [online] Available at: https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf [Accessed 21 Feb. 2020].
[26] Section 2(14) of the Personal Data Protection Bill, 2019.
[27] *Section 18(2), Draft Bill of 2018*
[28] *Section 17(1) of* the Personal Data Protection Bill, 2019.
[29] *Section 17(3) of* the Personal Data Protection Bill, 2019.
[30] *Section 18 of* the Personal Data Protection Bill, 2019.
[31] Ibid
[32] *Section 23(5) of* the Personal Data Protection Bill, 2019.
[33] *Section 23(3), (4), and (5)* of the Personal Data Protection Bill, 2019.
[34] Explanation to *Section 26 (4)* of the Personal Data Protection Bill, 2019.
[35] Ibid
[36] *Section 28 (3) and 28(4) of* the Personal Data Protection Bill, 2019.
[37] *Section 33(1) of* the Personal Data Protection Bill, 2019.
[38] *Section 34(2) of* the Personal Data Protection Bill, 2019.

 [ISSN 2581-5369]

excluded for purpose, storage and requirement for consent in the Bill of 2019 as per the provisions guiding Regulatory Sandbox.[39] abiding by the Aadhaar case.[40]

IV. COMPARATIVE ANALYSIS:

To ascertain India's perspective towards data protection laws, it would be pedagogic to analyze the laws pertaining to other Nation States, especially those which are being implemented in the recent past. A scrutiny of the international legislations illustrates dyad manifested versions of data protection laws. The US version is based on cross-sectoral laws whereas the UK model is based on a central federal policy.

The US data protection law is not concentrated to a single fundamental legislation but has a diverse field of legislations monitoring the accumulation and utilization of personal data.[41]

However, the laws are being amended or a constant change is proposed to be brought into action at each senatorial session to systematize the legislations at the central level. Instead, the US constitution comprises of a hodgepodge structure of central and state laws and regulations which could sometimes overlay, interlock and refute one another. On top of that, there are many regulations, developed by federal bureau and the companies operating in that country that are not having any binding force of law but is a chunk of automated suggestions and instructions that are regarded as 'best practices.[42] These advisory regulations have administrative and responsibility regime, whose use has taken a toll in the recent years.[43]

The US privacy protection can be equated with Article 21 of Indian Constitution, i.e., to secure personal liberty and to protect one's personal space from the strict regulations of the government. As far as data protection laws are concerned, America follows the principle of 'right to be let alone' which implies that there should be as little intervention as possible in its citizen's personal life and liberty in order to provide due respect to each one of their rights and duties. Although the US Constitution, does not provide a straightforward blanket protection on right to privacy, the same right is granted in a slender form in the Fourth Amendment to the US Constitution, basically in the form of right against unaccommodating search and seizure. As a result, the data privacy laws of US varies greatly with the European Union Model, from which the Indian data protection regime has evolved. Firstly, as already discussed, in contrary

[39] *Section 40 of* the Personal Data Protection Bill, 2019.
[40] Justice K.S. Puttaswamy (Retd.) v. Union of India, WRIT PETITION (CIVIL) NO. 494 OF 2012 (2018).
[41] Sheshadri Chatterjee, *Issues of personal data protection and privacy policy: A comparative analysis for different countries*, Volume 4 International Journal of Law 01-08 (2018), http://file:///C:/Users/hp/Downloads/4-1-62-810.pdf (last visited Feb 20, 2020).
[42] Ibid.
[43] Jeffrey Rosen, The Unwanted Gaze, The Destruction of Privacy in America Random House, 2000.

to the EU model, there is no definite group of data protection principles to control the dissemination of personal information in US. Secondly and lastly, the data protection laws provide separate set of rules and regulations for private and public entity. The laws governing the government agencies and the individual person is given under varied provisions of different legislations. In addition to that, every state has their independent data protection regime.[44]

V. THE LACUNA OF DATA PROTECTION STILL PREVAILS?

The Bill of 2019 does not bring into its ambit that a parliamentary law is to be brought in forth for the needs and proportionality to the aim that is to be looked into when the privacy is hampered.[45] Section 35 of the Bill of 2019 does put any check on the power of Government of India. It makes the Government superior on its own and in turn is contradictory to the objective of the Bill of 2019.[46] The Government can process the personal data of the citizens in cases of when the security of the nation is questioned and thereby opening the door to know the personal information of the public thereby lacking to maintain the privacy and that the personal information is accessed by the Government.

There has been suppression in the global market due to data localization and the emerging business aiming at worldwide expansion would have to suffer. The upcoming law has paved the way for the users to verify their accounts voluntarily which in turn is a serious threat in the field of data protection.[47] The Bill of 2019 mentions that the data fiduciaries should store minimum of one serving copy of the personal information in the server that is located in the country i.e. India. However, the critical personal information should only be stored in the country. According to the view of the authors of this paper it is an interference of the State in the personal information of the individual.

A regulatory framework has been formed in the Bill of 2019. The working of the regulatory framework is dependent to the Government of India. The Government of India has the power to designate the members of the competent data protection authority through suggestion of an outside committee.[48] Further, the members of the competent authority has a tenure of five years

[44] Daniel Solove. Conceptualizing Privacy, California Law Review 2002; 90(4):1088-89, 1100-02, 1112-13, 1130- 31.
[45] Business Today. (2019). *Personal Data Protection Bill 2019: Unrestrained power to central government may undermine privacy*. [online] Available at: https://www.businesstoday.in/current/policy/personal-data-protection-bill-2019-central-government-power-may-undermine-privacy-of-citizens-people/story/392186.html [Accessed 21 Feb. 2020].
[46] *Section 35 of* the Personal Data Protection Bill, 2019.
[47] De Du Express. (n.d.). *The Pros and Cons of The Data Protection Bill 2019*. [online] Available at: https://duexpress.in/the-pros-and-cons-of-the-data-protection-bill-2019/ [Accessed 24 Feb. 2020].
[48] Anon, (n.d.). [online] Available at: https://www.cfr.org/blog/three-problems-indias-draft-data-protection-bill [Accessed 24 Feb. 2020].

 [ISSN 2581-5369]

which is a small span of time to understand about the working of the body and thus coming to a suitable solutions for the problems that are to be addressed. Thereby, the authors of the paper is of the notion that the tenure of appointment should be extended so that the members become well aware of the functioning of the body and thereby aiding in providing a swift data protection.

The Bill of 2019 has proposed some terminologies without explaining or providing with a wider scope. It has come up with "social media intermediaries" without explaining the meaning of it.[49] If there is lacuna in the explanation of the terms used in the statute, then how will the problems arising out of it be addressed? This might result in wrong interpretation of the words which in turn can contradict with the objective of the legislation that is laid down.

VI. CONCLUSION AND SUGGESTION

After all these discussions, it is quite confusing as to what is the actual reason for the government to store these data and what would be its goal for the next years down the line and how would it seek to achieve the said goal. As far as data storing and maintaining is concerned, it is quite disheartening to find that although there has been the introduction of advanced technologies and varied gadgets in the country, people lack the basic knowledge as to the maintenance and handling of these data to avoid it being mishandled by hackers and spammers. Moreover, the proposed act does not clearly mention the compliance procedures for the storing and preservation of the sensitive information, therefore, this may create a miscommunication and misconception among the companies regarding the compliance of the provisions, which might hamper the innovative ideas and creativity of these companies, which would, in turn, might affect the economy of the country. Thereafter, it is advisable that before implementation of any act, it should be made clear as to the process of its compliance. These companies as well as individuals dealing with sensitive information should be provided with a clear set of rules and regulations in order to achieve the target object of the act and also to gain more power in the international boundaries.

*****

[49] Majumdar, R. (2019). *Data Protection Bill: Govt breaks silence but secrecy remains*. [online] Available at: https://www.indiatoday.in/india-today-insight/story/data-protection-bill-govt-breaks-silence-but-secrecy-remains-1627717-2019-12-12 [Accessed 24 Feb. 2020].

 [ISSN 2581-5369]