LEGISLATIVE COMMENT ON THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

Saurabh Bindal & Satyarth Kuhad *

I. Introduction

IT IS not a disputed fact that India is digitising at a massive rate.[1] India has surpassed China in terms of population and has become one of the largest data consumers and producers in the world.[2] The achievement which India has shown in the recent past, comes with a pinch of salt. It would not be wrong to state that technology has equal potential to harm as it has to protect.[3] This potential harm is equally placed for organisations as well individuals. Misappropriation of an individual's personal data amounts to breach of privacy which is essentially a violation of the right to life,[4] one of the fundamental rights granted to the citizens in the Constitution of India.[5] It is not uncommon to find news about data misappropriation across the world which has led all the powerful countries to make laws regarding this issue. Based on different principles, these major powers of the world have different laws regarding data protection. Currently, three approaches to data protection exist,[6] *laissez-faire,* the liberty approach of the United States, national security risk approach of China and the approach taken to hold individual dignity by the European Union (EU). GDPR, the data protection law of the EU seems to be a

---

* The first author is a Partner at the Fox Mandal & Associates. The second author is a Final Year LL.B. student at the Campus Law Centre, Faculty of Law, University of Delhi.

1 Presently, there are over 76 crore (760 million) active internet users (Digital Nagriks) and over the next coming years this is expected to touch 120 Crore (1.2 billion), Explanatory Note to Digital Data Protection Bill, 2022, Data protection Framework, *available at*: https://www.meity.gov.in/data-protection-framework (last visited on June 10, 2023).

2 *Ibid.*

3 Emily A. Vogels, Lee Rainie and Janna Anderson, "Tech causes more problems than it solves", *available at*: https://www.pewresearch.org/internet/2020/06/30/tech-causes-more-problems-than-it-solves/ (last visited on June 10, 2023).

4 The Constitution of India, art. 21.

5 *Justice K. S. Puttaswamy (Retd.)* v. *Union of India*, (2017) 10 SCC 1. The Supreme Court held that the right to privacy is a fundamental right flowing from the right to life and personal liberty as well as other fundamental rights securing individual liberty in the constitution. Chandrachud J. remarked about data protection, "Formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State."

6 *Supra* note 1 at 3.

composite and one of the most important regulations amongst them all.[7] The basic idea of all these approaches boils down to one belief that *it is the individual herself who decides in what manner her personal data is to be processed.* The approach taken by India seems inclusive of all these and focuses more on the individual's liberty and personal dignity.

The leitmotif of this article is to analyse the recent data protection Bill i.e., "The Digital Data Protection Bill, 2022 (hereinafter referred to as "the bill")"[8] drafted by the Government of India and suggest on how the shortcomings in the Bill can be rectified. The authors also discuss about the way forward.

II. History of the Data Protection Laws in India

The Government of India has been dedicated to make India a digital power for the last few years, but there have been very few measures undertaken to protect the digital systems as well as data stored by the government.[9] In the very first attempt, the Government of India provided for sections 43A and 72A in the Information Technology Act in 2000. These sections make provision for compensation to individuals whose personal data has been compromised and criminalising intentional data breach. Later in 2011, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 were framed under section 43A of the IT Act 2000. The protection and transfer of sensitive personal data or information are governed by these rules. These guidelines provide for procedures to be followed by the corporate bodies and persons collecting data on their behalf. These rules make up a major part of the data protection regime of the country.

In 2013, the Department of Electronics and Information Technology launched the National Cyber Security Policy which comprises advisory guidelines for preventing data breach. The Supreme Court of India in *Justice KS Puttaswamy* v. *Union of India,* pronounced the landmark judgement, unanimously recognising the right to privacy under Article 21, considering it intrinsic to an individual's life and liberty. Consequentially, the Government of India, in 2017, constituted an expert

7 The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organisations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros, *available at*: https://gdpr.eu/what-is-gdpr/ (last visited on June 10, 2023).

8 The Digital Data Protection Bill, 2022.

9 *Supra* note 1 at 6. Currently, the law does little to protect individuals against such harms in India.

committee under the Chairmanship of Justice B.N. Srikrishna to examine the data privacy concerns. The committee prepared a report: "A Free and Fair Digital Economy Protecting Privacy, Empowering Indians (hereinafter referred to as, "committee report")"[10] Along with the committee report, a draft bill was also submitted in 2018 which was modified and later introduced as the Personal Data Protection Bill, 2019 (hereinafter referred to as, "the 2019 Bill") in the Lok Sabha. The Bill was referred to the Joint Parliamentary Committee which submitted its report in December, 2021. However, the Bill could not be passed and was withdrawn in August, 2022.

Later, the Ministry of Electronics & Information Technology had introduced another draft Bill titled, the Digital Personal Data Protection Bill 2022. In a series of attempts to create a legislation for protecting personal data of the citizens, the Government of India has drafted a second bill specifically for data protection, after the Government had withdrawn the 2019 Bill, from the Lok Sabha in August, 2022. Presently, the bill has been passed by both the houses of the Parliament of India awaiting the consent to be given by the President of India.

III. The Digital Personal Data Protection Bill, 2022

The Ministry of Electronics and Information Technology, along with the Bill, had also issued an explanatory note to the Bill[11]. The note mentions the following seven fundamental principles on which the Bill is based: -

1) **Manner**- The usage of personal data must be done in a lawful, fair, and transparent manner by the organisations.
2) **Purpose Limitation**- The personal data must be only used for the purposes for which it is collected.
3) **Data Minimisation**- Only specific personal data which is required for a specific purpose must be collected.
4) **Accuracy**- To ensure that the personal data of the individual is accurate and up to date.
5) **Storage Limitation**- The personal data should be stored for such duration as is necessary for the stated purpose for which personal data is collected.
6) **Data breach prevention**- To ensure that there is no unauthorised collection or processing of personal data.

10 Government of India, "A Free and Fair Digital Economy, Committee of Experts under the Chairmanship of Justice B.N. Srikrishna" (2018).

11 *Supra* note 1.

7) **Accountability**- The person who decides the purpose and means of processing of personal data should be accountable for such processing.

These principles essentially carry their lineage from various provisions of the IT Act, 2000 and the committee report. While most of the fundamental rights are enforceable only against the State, this Bill, if enacted, would make up for a rare case where the fundamental right of privacy would be applied horizontally. Another fact that makes this Bill unique is that it is India's first legislative document to use the pronouns "her" and "she" to refer to persons irrespective of gender.

Analysis of Key Provisions of the Bill

Definitions

The Bill defines "child" as "an individual who has not completed eighteen years of age".[12] It seems from the provisions of the bill that emphasis has been laid on protection of data related to children.[13] The regulations worldwide have considered the children of age as low as 13 years to provide consent.[14] This Bill defines child as a person less than 18 years to keep it compatible with other legislations like Indian Contract Act, Juvenile Justice Act, and POCSO Act. This threshold has been criticized for not being in line with global standards as it is too high.[15] Although the committee report recognizes that "from the perspective of the full, autonomous development of the child, the age of 18 may appear too high" and suggested to determine the cut-off age anywhere between 13 to 18 years.[16]

The terminologies, "Data Principal" and "Data Fiduciary", are in consonance with the suggestions made in the committee report.[17] In other regulations the individual whose data is collected is referred to as "data subject" and the entity that collects the data is referred to as "data controller".[18] This terminology clearly gives a hint that the "controller" "controls" the "subject", which places the interest of the individual whose data is collected secondary to the entity that collects the data. And when the regulations are weak and the interests are discriminated against, data misappropriation takes place. The belief behind using a new terminology can

12 *Supra* note 8, s. 2(3).

13 The Bill also prohibits profiling of children which includes "behavioural monitoring" and "targeted advertising" to children. However, it can be exempted by the Government through a notification.

14 *Supra* note 10 at 43.

15 *Ibid*.

16 *Supra* note 10 at 48.

17 *Id.* at 49.

18 *Id.* at 53.

possibly be to place the interests of Data Principals at par with the interests of Fiduciaries. The Government of India has adopted these terms since the inception of this legislation in 2018. The prejudicial terminology is however still used in other important regulations like General Data Protection Regulation (GDPR).

"Harm" has been defined as "(a) any bodily harm; or (b) distortion or theft of identity; or (c) harassment; or (d) prevention of lawful gain or causation of significant loss"[19]. This definition misses out some other important possible forms of "harm" and is not exhaustive. The 2019 Bill provided a more detailed list which included: (i) mental injury, (ii) loss of reputation or humiliation, (iii) discriminatory treatment, (iv) blackmail or extortion, (v) any observation or surveillance not reasonably expected by the data principal, and (vi) restriction of speech, movement, or any other action arising out of fear of being observed or surveilled. The Joint Parliamentary Committee recommended adding to the list of harms one another form i.e., 'psychological manipulation that impairs the autonomy of the individual', but it is not included in the bill.[20]

Section 2(13) defines "personal data" as "any data about an individual who is identifiable by or in relation to such data". The issues mentioned in above definitions regarding ambiguity persist in this definition also. Also, the definition is narrow. The definition used earlier i.e., the one given in the IT Rules 2011 was more expansive and clearer than this.[21] The committee report differentiated between "personal data" and "sensitive personal data" and provided for categories.[22] It defined "sensitive personal data" and provided for several heads which gave enough guidance to frame the definition, such as, passwords, financial data, health data, official identifiers which would include government issued identity cards, sex life and sexual orientation; biometric and genetic data; transgender status or intersex status, caste or tribe and, religious or political beliefs or affiliations. This bill however does not differentiate and places all kinds of data on equal footing which makes all kinds of data equally protectable.

Interpretation

This Bill is regarding protection of personal data of individuals, the collection of which is now part of almost every individual's regular life. The Bill provisions for

19 *Supra* note 8, s. 2(10).

20 Legislative Brief, The Draft Digital Personal Data Protection Bill, 2022, PRS; available at: https://prsindia.org/billtrack/prs-products/prs-legislative-brief-4053#_ednref7 (last visited: 15th August 2023)

21 For definition of "data", See, S. 2(e), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, and S. 2(1)(o), The Information Technology Act, 2000.

22 *Supra* note 10 at 30.

opting from the languages mentioned in the eighth schedule only.[23] This bill, if enacted, would affect all types of individuals including illiterates and people from uneducated strata of the society. For a clear understanding of the notice, consent and other procedures regarding the data processing, language in which the individual is most comfortable must be used. India being a highly diversified country boasts a large number of languages. The exact number of languages although cannot be stated but the numbers range from around 300 to 1500 according to different sources. In such a country where the language changes within a few hundred kilometres, provision for only 22 languages in the legislation concerning such a sensitive issue is highly unjustified.

Applicability

The protections available in the Bill only applies to the digital personal data and ignores the misappropriation of data in the offline mode. Misappropriating any data in offline mode is easy to do and there are no other laws or rules available for data protection which can possibly deal with the protection of personal data in the offline mode. This defeats the very purpose of the legislation.

A unique feature of the Bill is that along with its application in the territory of India, the bill has extraterritorial applicability also when "processing is in connection with any profiling of, or activity of offering goods or services to Data Principals within the territory of India" where "profiling" means, "any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a Data Principal"[24]. However, the Bill does not provide a mechanism to protect the data from getting exported outside India. The Bill confers wide discretionary powers to the Central Government to notify countries and permit data exportation to those countries.[25] This clearly amounts to excessive delegated legislation, as the factors under which such notification be made are not provided in the Bill.

Notice

The format of the notice is not provided in the bill. The provision prescribes for a clear notice in plain language mentioning the data required and the purpose. But there is no provision that provides for the notice to possess details of how the data will be processed and who would be able to possess and access the data. The provision does not specify whether the notice should be in written form or not. It mentions "itemised notice"[26] which must be just a list.

23 *Supra* note 8, s. 32.

24 *Supra* note 8, s. 4(2).

25 *Id.,* s. 17.

26 *Id.,* s. 6.

Even in cases where there are grounds for processing that are not consensual, the concept of notice must be made necessary. Any exemption from the requirement of notice must only apply in extreme cases or when giving notice renders the lawful processing purpose impossible to achieve. Additionally, the details offered at the time of notice must be increased. The law must also include provisions for proactive disclosure of a privacy policy and the common terms of data processing.[27]

The retrospective provision[28] is highly unreasonable and impractical for the Fiduciaries to comply with. An individual might have given her consent a thousand times over the internet. It is not practicable and traceable. This can possibly lead to a large number of false and frivolous litigations.

Consent

Section 7 deals of the bill with the consent to be given by Data Principals while providing the personal data to Data Fiduciaries. Although, the section provides enough safeguards about the consent which has to be received before processing the personal data, there remains a fundamental issue. Similar to the provision for notice, there is no specified form prescribed for the consent. Just an "affirmative action" would be considered as a consent. Leaving ambiguity in such a critical part of the law to be made, can be tricky for the Data Fiduciaries to follow and implement.

The clause discussing withdrawal of consent provides that the consequences of such withdrawal should be borne out by the withdrawing Data Principal.[29] However, such consequences should only be restricted to consent for processing personal data necessary for the execution of a contract.[30] The clause also mandates that the ease of such withdrawal shall be comparable to the ease with which consent may be given.

Deemed Consent

The personal data of an individual might also be processed without a consent in a number of situations where the consent is deemed to be given by the Data Principal. Although the provided situations seem to be just and equitable, there is a scope of misuse. E.g., the bill authorises the State and its instrumentalities to use an individual's personal data for providing her benefit through different schemes.[31] This might be

27 Page 8, Comments on Draft Digital Personal Data Protection Bill, 2022, VIDHI Centre for Legal Policy.

28 *Supra* note 8, s. 6(2).

29 *Id.*, s. 7(4).

30 *Supra* note 27.

31 *Id.*, s. 8(2).

considered as valid ground for assuming a deemed consent but the provision does not supply with a mechanism which ensures that only the data necessary for that purpose would be shared, that too with the concerned department only.

Also, it seems unclear whether private entities would be authorised to avail these grounds, given that the processing needs to be "in public interest". Section 11(1) can be read as a similar provision where only the Central Government has been authorised to notify a Significant Data Fiduciary.[32] There is also the ground of "fair and reasonable purpose", but in this case, it would have to be notified by the Government as to what amounts to a "fair and reasonable purpose". In doing so, the Government can also consider the Data Fiduciary's legitimate interests.[33]

Obligations on Data Fiduciary

Section 9 relates to obligations on Data Fiduciary however it does not provide any mechanism to fulfil those obligations. The provision mandates the Data Fiduciary to make reasonable efforts to ensure data accuracy, storage and deletion etc. but no fool proof mechanism is provided which can guide the subjects of this bill to make rules and regulations regarding the "reasonable efforts". A Data Fiduciary is required to "implement appropriate technical and organisational measures"[34], for which a Data Fiduciary must be at a high-powered position in the organisation she is working with. In an organisation where there are no minimum necessary technical and organisational facilities, the obligations on the employee who would be a Data Fiduciary would be unfair. In case of any data breach, the Data Fiduciary or Data Processor would have to inform the Data Principals affected, but the Data Fiduciary is not obliged to mitigate and prevent further data breach at the earliest.[35]

The Bill specifies two classifications of Data Fiduciary namely, Data Fiduciary and "Significant Data Fiduciary". While a Data Fiduciary can be appointed by any organisation (private and government), a Data Fiduciary can be notified as a "Significant Data Fiduciary" only by the Central Government, based on the factors mentioned in section 11(1). The most important issue that arises here is that only the Central Government can notify a "Significant Data Fiduciary" and no other Government, state instrumentality or private entity is authorised to perform this function. Since the factors on the basis of which the Central Government may

32 *Supra* note 8, s. 11.

33 What's In India's New Data Protection Bill?; *available at*: https://www.mondaq.com/india/privacy-protection/1258868/whats-in-indias-new-data-protectionbill#:~:text=On%2018 %20November%202022%2C%20the,Bill%20by%2017%20December%202022 (last visited on June 15, 2023).

34 *Supra* note 8, s. 9(3).

35 *Id.,* s. 9(5).

perform this function are of national importance, such duty must be bestowed upon all significant stakeholders and accountable entities (including private organisations) of the country.

Section 12 is a praiseworthy provision which empowers the Data Principal to obtain information regarding processing of her personal data by keeping it under the ambit of the "right to information". The access to the information seems easy too, as it makes it mandatory for the Data Fiduciary to maintain a summary of the processing of personal data. This Section along with other sections furnish wide significant rights for Data Principals including, "Right to correction and erasure of personal data", "Right of grievance redressal" and "Right to nominate".[36]

Duties of Data Principals

Interestingly, the Bill does not only protect the personal data of the Data Principals unidirectionally, by providing them rights, but also provides with duties to be performed by the Data Principals. In case any Data Principle fails to abide by duty prescribed in section 16(2), there is a provision for imposition of costs as the penalty.[37]

Exemptions

The Bill confers broad powers on the Central Government without any checks and balances provided. Under the exemptions provided therein Data Principals are left with no rights in those cases which defeats the very purpose of this Bill.[38] This provision would empower the Central Government to obtain and possess personal data of any individual for an indefinite period of time and no procedure has been prescribed in this section which is a violation of the fundamental right of "right to freedom". Article 21 of the Constitution of India states, "Protection of life and personal liberty —No person shall be deprived of his life or personal liberty except according to procedure established by law". Since protection of privacy and personal data of an individual comes within the ambit of article 21, accessing personal data without establishing a fair procedure would be a violation of article 21.

In *Maneka Gandhi* v. *Union of India*,[39] the Supreme Court laid down the triple test to be passed before making any law interfering with personal liberty:[40]

36 *Id.,* ss. 14 and 15.

37 *Id.,* s. 21(12).

38 *Id.*, s. 18.

39 (1978) 1 SCC 248.

40 *Ibid.*

(1) It must prescribe a procedure;

(2) the procedure must withstand the test of one or more of the fundamental rights conferred under Article 19 which may be applicable in a given situation; and

(3) It must withstand the test of article 14.

Another issue is violation of the principle of proportionality. The powers intended to be given to the Central Government are absolute. The Central Government can possess an individual's personal data indefinitely. Using these exemptions, based on several grounds, a government agency would be able to create a 360-degree profile for surveilling individuals.[41] This can be done by utilising the data retained by various government departments for other lawful purposes. This raises the question whether these exemptions will meet the proportionality test. The Supreme Court in *Justice KS Puttaswamy* v. *Union of India*,[42] held that any infringement of the right to privacy should be proportionate to the need for such interference. Any restriction must be proportionate and narrowly tailored to the stated purpose.[43] One of the grounds on which the Central Government can exempt any government department from receiving consent before processing personal data, is "security of the State".[44] The Supreme Court in *People's Union for Civil Liberties* v. *Union of India*,[45] had laid several guidelines regarding interception of communication between individuals, on grounds of national security:[46]

The authority issuing the interception order must maintain records of: (i) the intercepted communications; (ii) the extent to which material is disclosed; (iii) the number of persons to whom the material is disclosed and their identity; (iv) the extent to which the material is copied; and (v) the number of copies made (each of which must be destroyed as soon as its retention is no longer necessary).

Although the Bill does not specifically mention interception of communication in the Bill, the above safeguards could be used as guiding principles for making a framework of processing data under special circumstances. The Committee Report also recommends expeditiously bringing in a law for the oversight of intelligence gathering activities.[47]

---

41 Report on Draft Digital Personal Data Protection Bill 2022, PRS; *available at*: https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022 (last visited 15 June 2023).

42 *Supra* note 5.

43 *Ibid.*

44 *Supra* note 8, s. 18(2).

45 (1997) 1 SCC 301.

46 Chaitanya Ramchandran, "PUCL v. Union of India Revisited: Why India's Surveillance Law Must Be Redesigned for The Digital Age" 7 *NUJS Law Review* 105 (2014).

47 *Supra* note 10.

Compliance Framework

Chapter five of the Bill provides the compliance framework of personal data protection. The compliance shall be managed by a board, namely, "Data Protection Board of India" (hereinafter referred to as "the Board") which would be constituted by the Central Government. The chapter lays out the details of composition, functions and procedures to be followed by the Board.

The Bill however intends to keep the functioning of the Board independent,[48] but even a simple reading of the provisions related to the Board would make it sound dubious. The Bill delegates all responsibilities regarding composition, strength of the Board, removal of the Chairman, and terms and conditions of the services of the members, to the Central Government. This empowers the Central Government to change the structure as well as the terms and conditions at any moment of time. This can lead the Central Government to use the Board for various unlawful benefits including political benefits. The Board has been mandated to discharge functions as assigned by the Central Government along with its main function of determining non-compliance of the Act.[49] Under this provision, the Central Government can certainly influence the functioning of the Board making it act like its agent. The Central Government is going to become an organisation with the largest number of Data Fiduciaries in the country. It processes the personal data of millions of people for the services and benefits, granting of permits, licenses, and official IDs. This fact makes it necessary for the regulatory body to develop the rules and regulations to be independent of the government's influence in order to ensure fair protection of data principal's interests.[50]

The 2019 Bill sought to provide for an independent Data Protection Authority and the necessary details such as composition, manner and terms of appointment were specified in the Bill itself.[51] The committee report also supplies with sufficient details regarding composition and functioning of the Board (therein named as "Data Protection Authority") including detailed obligations and enforcement tools at the disposal of the Board.[52]

Section 21(8) of the Bill mandates the Board to complete the enquiry at the earliest. However, there is no specific time period prescribed to dispose of the complaints received by the Board. At the level of Data Fiduciary, there is a prescribed time

48 *Supra* note 8, s. 19.

49 *Id.*, s. 20(1).

50 PRS Legislative Brief, *available at*: https://prsindia.org/billtrack/prs-products/prs-legislative-brief-4053#_edn23 (last visited on June 12, 2023).

51 *Ibid.*

52 *Supra* note 10.

period of seven days to deal with the grievance of Data Principals but the purpose for an early redressal is defeated when the Board has discretion with respect to time period to hold the inquiry and close the complaint.

The Bill empowers the Board to review its orders by an adjudicating group larger than which passed the concerned order.[53] There is no provision of any appellate body in the Bill. The aggrieved party would be able to appeal directly to the High Court. This can possibly lead to unjustified harassment of the victim of data breach until the High Court decides on the matter. However, there were provisions for an Appellate Tribunal in the 2019 Bill.[54]

Section 25 provides for penalty in cases where the non-compliance is "significant". However, disappointingly only financial penalty is the only form of punishment prescribed in the Bill. Data breach can significantly harm an individual's life. Along with it, non-compliance to any provision of this bill would amount to the violation of a Fundamental Right of the affected individual. Other than this, data breach can in many ways prejudice our nation's security and integrity. No criminal liability has been set out for such violations.

Miscellaneous

One of the major shortcomings of the Bill is absence of two significant rights of the Data Principals namely, "Right to data portability" and "Right to be forgotten". Both these rights were part of the 2019 Bill. The Committee report in its recommendations of Chapter V explicitly recommended for provision of these two rights.[55] According to the Committee report, "the right to data portability is critical in making the digital economy seamless."[56]

Right to data portability

"The right to data portability allows Data Principals to obtain and transfer their data from data fiduciary for their own use, in a structured, commonly used, and machine-readable format."[57] This right enables the Data Principals to have a better control over their data with respect to data migration between different Fiduciaries.

Right to be forgotten

The "Right to be forgotten" refers to the right to erase or limit the disclosure of an individual's personal data available on the internet. This right can prevent access

53 *Supra* note 8, s. 22.

54 The Personal Data Protection Bill, 2019, Ch. 12.

55 *Supra* note 10, Ch. 5.

56 *Id.* at 75.

57 *Supra* note 50.

to an individual's personal data by the public at large. Although this right has not been granted explicitly by any statute or judgement in India, the Supreme Court and High Courts have discussed and considered it to be a part of "Right to privacy". The Committee Report observed, "that the right to be forgotten is an idea that attempts to instil the limitations of memory into an otherwise limitless digital sphere."[58] In *Justice K.S.Puttaswamy (Retd)* v. *Union Of India*,[59] Sanjay Kishan J. observed that the "Right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the Internet"[60] While, the IT Rules, 2021 also do not include this right, they do however, lay down the procedure[61] for filing complaints with the designated Grievance Officer so as to have content exposing personal information about a complainant removed from the internet.[62]

IV. Conclusions and Suggestions

The issue of personal data protection is highly sensitive and affects every individual's life. The Bill if enacted, would be the first dedicated legislation for personal data protection in India. Considering the sensitivity of the issue as well as the number of people this legislation would affect, it is quite difficult to predict the success of the legislation. Its actual repercussions and shortcomings would be known only once it is implemented. However, the Bill is a mixed bag legislation. It contains certain praiseworthy provisions, some of them being the stronger and improved versions of the preceding drafts. Although the Bill has promising features, it needs to be refined in terms of definitions and clarity of language. The bill also grants arbitrary powers to the Central Government with respect to exemptions to its agencies from compliance. This can possibly prevent fair implementation of the law. Along with this, the Data Protection Board which is the regulatory authority needs to be more independent with statutory authorization for uninfluenced regulation of the compliance of the provisions.

The Digital Personal Data Protection Bill, 2022 deals with an issue which has never been strictly regulated by the State. Even after the declaration of right to privacy as a fundamental right by the Supreme Court of India, no dedicated law has been enacted by the Parliament yet. The Bill has been passed by both the houses of the Parliament. The effort of the Central Government is a necessary step in the right

58 *Supra* note 10, at 77.

59 *Supra* note 5.

60 *Supra* note 5, para 62 [Judgement of Sanjay Kishan J.].

61 Page 23, Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

62 *Ibid.*

direction. With this progress, the citizens of the country are waiting for this legislation to be enacted, with great expectations.

The Bill is undoubtedly drafted in simple language and an easy to understand, still there is a need to clarify the language in some provisions, such as the language surrounding the legitimate interest type of ground which we believe is at the heart of privacy legislation.[63]

The Bill certainly lacks of some important mechanisms. There should be some implicit mechanisms which could act as guidance for proper implementation of the law. E.g., There is no provision in the Bill which could suggest that even those handling the personal data would have limited or reasoned access to the personal data. There should be a mechanism to permit for access and record whenever given.

The provisions of deemed consent should include more stringent requirements like (a) the implied consent for processing personal data must be for a specific purpose; (b) the implied consent must be revocable; (c) it must be illegal to use implied consent to process sensitive personal data or to process any personal data in a way that poses a significant risk of harm; and (d) additional guidance may be provided on when consent may be given.[64]

63 *Supra* note 5, s. 8(9).

64 *Supra* note 27.