Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

What the Personal Data Protection Bill brings to the Table

Abhishek Dagar[a]

[a]Law Centre II, University of Delhi, New Delhi, India

Received 20 May 2022; *Accepted* 09 June 2022; *Published* 12 June 2022

The Orwellian dystopia that looked too far-fetched to some in 1949 when he published his book 1984 is slowly beginning to take shape. The only difference is the "Big Brother" imagined by him has been replaced by "Big Data". The emergence of "Attention Economics", where human attention is a scarce resource, has led to unprecedented use of data analysis to not only understand human behaviour but predict it, thereby fueling the demand for data. Today, an unthinkable amount of data is being generated and processed by both state and non-state actors, which makes it imperative to have a piece of legislation that can protect the rights of the individual. To fulfill this objective and provide holistic legislation to govern the processing of personal data of individuals, the Indian government came up with The Personal Data Protection Bill 2019. This paper looks at the need for a data protection regime and its evolution around the world, but more importantly, it studies the provisions of the recently introduced bill and what impact it could have on the future of the digital economy.

Keywords: *PDP bill, big data, digital economy, data protection regime.*

INTRODUCTION

"Data is the new oil." This phrase has been used more times in the last decade than in the entirety of history. With the proliferation of companies like Facebook and Google, having billions of users, and the general digitalization of the world, people are leaving digital footprints all over the internet without knowing what these footprints could lead to. 94% of

businesses say that data and analytics are important for their business growth and digital transformation[1]. Companies have argued for 20 to 30 years to stop better regulation of the internet and data as the users have already agreed to their terms and conditions, making them billions of dollars along the way. This has been made possible by what is called big data.

BIG DATA

The origin of the term Big Data is not known, but John R. Mashey is credited with popularising the term in the 1990s. Oracle, one of the leading computer technology corporations, defines big data as "data that contains greater variety, arriving in increasing volumes and with more velocity. This is also known as the three vs "Big data" which is larger, more complex data sets, especially from new data sources. These data sets are so voluminous that traditional data processing software just can't manage them. But these massive volumes of data can be used to address business problems you wouldn't have been able to tackle before."[2] Organizations use the power of analytics to discern patterns of individual behaviour and market trends from the data to better predict future outcomes and prepare accordingly. Such processing of data has tremendous potential in fields like weather forecasting and medicine. However, it is increasingly being used to target advertisements of products to individuals who are more likely to purchase them. Continuing on this path of innovation, the potential of what can be harnessed from data would increase manifolds in the future.

WHY SHOULD YOU CARE ABOUT WHAT IS BEING DONE WITH YOUR DATA?

Imagine, you are looking for a health insurance policy. You consult one of your friends about what policy to take. He advises that his current policy is a nice and affordable plan that you can look at. Now you do your research and conclude that it is indeed a policy that fits your requirements. So you fill up the application form and wait for its approval only to find out that your insurance premium is 70% more than your friend's. You wonder what could cause such a difference as both of you are of the same age and have no previous medical history. What if I

[1] 'Global State of Enterprise Analytics report 2020' (*Microstrategy*) <https://www3.microstrategy.com/getmedia/db67a6c7-0bc5-41fa-82a9-bb14ec6868d6/2020-Global-State-of-Enterprise-Analytics.pdf> accessed 18 May 2022

[2] 'What is big data' (*OCI*) <https://www.oracle.com/in/big-data/what-is-big-data/> accessed 18 May 2022

tell you that the fitness band that you wear to track your daily activity sends your personal data to a server from where it is being sold to the insurance company in question, and based on the analysis of such data, the company has predicted that you are 50% more likely to avail the health insurance benefit than your friend and hence, a higher premium for you? This may sound like a scene from a dystopian novel, but today we are not far away from having such capabilities. Applied Artificial Intelligence, big data analytics, and modelling techniques have enabled organisations to harness the potential of data that is being provided to them knowingly or unknowingly by the people. While having an ad pop on your screen while browsing through a website may seem innocuous but the data processing required to put that ad on your screen can have the potential to affect your life in more ways than you can imagine. For instance, what price you pay for your car insurance premium could be made based on data given to third parties that you never intended to, or much worse, imagine a government-sponsored social credit system that determines the area of the city that you can live in or whether you are eligible to travel out of your state or country based on data collected by the government like the amount of tax you pay, your traffic violations, etc. Our digital footprints combined with the power of analytics make it impossible to be anonymous today. Besides this attack on individual privacy, these corporations are able to shape our world according to their needs. It is nothing short of manipulation of our behaviour without our knowledge

More harrowing use of data analytics was seen in the Cambridge Analytica Scandal[3] in which Cambridge Analytica, a British political consultancy firm, gained access to the information of millions of Facebook users, mostly Americans. Moreover, the company used cookies to track people around the web to understand their political beliefs, what motivates them, and how they feel about certain issues in general. The analysis of this data was used to target advertisements at them on Facebook to affect their voting behaviour in the United States Presidential elections. In 2018, Facebook admitted Cambridge Analytica may have accessed

[3] Kevin Granville, 'Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens' (*The New York Times*, 19 March 2018) <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html> accessed 18 May 2022

the data of more than 500 thousand Indians[4]Hence, it is important to understand the potential a seemingly worthless data set may possess. The misuse of such capabilities has not gone mainstream yet, but the threat is quite evident on the face of it. Such practices can not only mould the behaviour of the entire population subconsciously but can undermine the very institutions on which modern society stands. Historically, technological innovation has always outpaced its regulation. However, in this case, governments around the world have to be proactive in formulating regulations and creating a safer internet by ensuring the enforcement of such regulations.

HISTORICAL EVOLUTION

Global perspective

Privacy and data protection laws have witnessed a very noticeable evolution, especially during the last few decades all over the world. Historically, the concept of privacy can be traced as far back as 1890, when Samuel Warren and Louis Brandeis published an article titled "Right to Privacy"[5]It is one of the earliest writings that advocated the right to privacy in the United States of America. The writers, taking note of the technological advancements of the time that made it easier for the press to interfere in the private lives of individuals, noted that privacy should be protected by law as a value in and of itself. They defined privacy as the "right to be left alone". The United Nations General Assembly adopted the Universal Declaration of Human Rights, in 1948. Article 12 of the Declaration[6] was the first formal recognition of the Right to Privacy by the international community. The article prohibited arbitrary interference in privacy and attack on the reputation of an individual. It led to many nations taking steps toward inculcating the right to privacy in their domestic laws. In 1976, a multilateral treaty called the International Covenant on Civil and Political Rights came into

[4] 'Data breach: Government again sends notices to Cambridge Analytica, Facebook' (*The Times of India*, 25 April 2018) <https://timesofindia.indiatimes.com/business/india-business/data-breach-govt-again-sends-notices-to-ca-facebook/articleshow/63913964.cms> accessed 18 May 2022

[5] Warren and Brandeis, 'The Right to Privacy' (1890) 4 (5) Harvard Law Review <https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html> accessed 18 May 2022

[6] Universal Declaration of Human Rights, 1948, art.12

force. Article 17 of the covenant provides that every individual has a right to protection of the law against arbitrary and unlawful interference with his privacy, family, home, or correspondence[7]. By the 1980s, globalisation had a considerable foothold around the world. It led to an unprecedented cross-border movement of data. Many countries, therefore, passed legislation regulating such data transfers to stop what was then considered a violation of fundamental rights by unlawful processing of data. Hence, the OECD (Organisation for Economic Co-operation & Development) developed the **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980** to harmonise national privacy laws and prevent interruption in global trade. Soon after, in 1981, the Council of Europe adopted treaty no. 108, titled "**Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"**. The convention was the first binding international instrument that protects an individual from harm caused by unlawful processing of his personal data and regulated trans-border data transfer. The two documents, mentioned above, introduced principles to regulate the processing of personal data that are still relevant today and have served as guiding principles for contemporary privacy and data protection laws all around the world. These principles were as follows -

- **Collection limitation Principle** - Data should be collected lawfully and fairly after obtaining the consent of the data subjects.
- **Data quality Principle** - data collected relevant to the purpose of collection should be accurate and complete.
- **Purpose specification Principle** - The purpose for which personal data is collected should be clearly specified at the time of data collection to the data subject
- **Use limitation Principle** - Data collected has to be used for a specified purpose only, except with the consent of the data subject or by authority of law.
- **Security safeguard Principle** - Reasonable security measures have to be taken to keep the data secure.
- **Openness Principle** - Transparency should be adopted in relation to the use of personal data by the data controller.

[7] International Covenant on Civil and Political Rights, 1996, art.17

- **Individual Participation Principle** - Data subjects should have the right to access, confirm or rectify their personal data.
- **Accountability Principle** - Data controllers have to demonstrate compliance to regulators.

However, the biggest landmark in the field of data privacy and protection came when the European Union adopted the **General Data Protection Regulation (GDPR).** The law came into force on 25 May 2018 in all member states to harmonise data privacy laws across Europe. It is the culmination of decades of work done in the field and imbibes the above-mentioned principles to provide unprecedented control to citizens over their data and prevent misuse of the data by controllers and processors.

Indian Scenario

The Indian Legislature has scantly paid heed to the domain of privacy and data protection in India. There wasn't any single law governing the processing of data. However, a few sector-specific rules have been formulated to regulate the use of personal data such as the Aadhaar (Targeted Delivery of Financial and Other Subsidiaries, Benefits, and Services) Act 2016, as amended by the Aadhaar and Other Laws (Amendment) Bill, 2019, which permits financial institutions to use biometric information to verify individuals' identities when opening bank accounts. Information technology act 2000 is the only act that explicitly aims to regulate the processing of Sensitive Personal Data and Information (SPDI). Section 43A of the act provides for compensation for failure to protect data[8]. The provision makes a body corporate, including any company, a firm, sole proprietorship, or other association of individuals engaged in commercial or professional activities, liable to pay damages in case of negligence in maintaining reasonable security practices and procedures to safeguard any sensitive personal data and information which it owns, controls, or operates. Moreover, Section 72 of the IT Act penalizes disclosure of any information procured in pursuance of any of the powers conferred under this Act to a third person[9] while Section 72A penalises disclosure of any information

[8] Information Technology Act, 2000, s 43A
[9] Information Technology Act, 2000, s 72

collected under a contractual relationship with the intention or knowledge that such disclosure would likely cause wrongful loss or wrongful gain[10].

Although the legislature was hesitant to delve into the area of privacy and data protection, the Supreme Court of India has explored the contours at regular intervals. M.P. Sharma vs Satish Chandra, District Magistrate[11] was one of the first judgments wherein the Supreme Court considered reading the Right to Privacy in the provisions of the Constitution of India. An eight-judge bench of the court, while discussing the provisions of search and seizure in the CrPC concluded that the Right to Privacy was not a fundamental right under the Indian Constitution. A similar notion was upheld in other cases like Kharak Singh vs the State of UP[12]. However, with the passage of time and growing global consensus on the issue of privacy and data protection, the Supreme Court also changed its stance on the issue, which culminated in the landmark judgement of ***Justice K.S. Puttaswamy (Retd) v Union of India***[13] wherein a nine-judge bench of the court acknowledged that the Right to Privacy is an intrinsic part of the fundamental right to life and personal liberty as enshrined by Article 21 of the Constitution of India. It was a historic judgement in the domain of privacy with far-reaching effects on individual bodily autonomy and protection of personal data. However, like any other fundamental right, privacy, too, could be restricted under certain circumstances. The court observed, "*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*."

Hence, over a period of time, the courts have developed a significant amount of jurisprudence on privacy in India. Moreover, the establishment of the digital economy and the sheer amount of data being generated today makes it imperative to develop a comprehensive data protection regime that is conducive to both economic growth and Individual's right to privacy and protection of personal data. The Union government constituted a committee led by Justice B.N. Srikrishna to study issues related to data protection in India. Based on the committee's report,

[10] Information Technology Act, 2000, s 72A
[11] *M.P.Sharma v Satish Chandra, District Magistrate* (1954), AIR 300
[12] *Kharak Singh v State of UP* (1963), AIR 1295
[13] *Justice K.S. Puttaswamy (Retd) v Union Of India* (2018) Writ Petition (Civil) No. 494/2012

Personal Data Protection Bill, 2019 was introduced in Lok Sabha on 11 December 2019. The bill aims to provide a legal framework to regulate the processing of personal data and mitigate the risks involved therein. The bill is currently pending parliamentary approval.

THE PERSONAL DATA PROTECTION BILL 2019

The Personal Data Protection Bill 2019 aims to be an all-encompassing piece of legislation concerning the privacy of individuals relating to their personal data. The bill tries to regulate entities involved in the processing of personal data of individuals to build a trustworthy relationship between such entities and individuals. The provisions of the bill apply to the processing of personal data within the territorial boundaries of the nation by any entity- public or private, a single person or body of persons incorporated under Indian law, and also by foreign entities operating within the territory of India. The provisions of the bill do not apply to anonymised data, i.e., data that has gone through such irreversible transformation that renders it impossible to decipher who it belongs to except in certain circumstances. The bill defines the natural person to whom a data set belongs as the "Data Principal" while the entity who determines the purpose and means of processing the personal data is defined as the "Data Fiduciary". Such nomenclature has been adopted to signify the expectation on the part of an individual that his personal data would be used fairly and any processing would be done keeping in mind his best interests by the data fiduciary. Another party involved in this relationship is the "Data Processor", i.e., the entity that processes the data on behalf of the data fiduciary. Since the bill aims to regulate the processing of personal data, it is necessary to understand what exactly is meant by personal data. The bill defines "personal data" as any piece of data that can directly or indirectly identify a natural person having regard to any characteristic, trait, attribute, or any other feature of the identity of such a natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling. "Processing" of personal data involves any operation performed on such data, like storage, collection, use, disclosure, and sharing in its broadest sense.

OBLIGATIONS OF DATA FIDUCIARY

A data protection regime cannot function effectively without putting certain obligations on the data fiduciaries given their dominant position in the relationship with data principals. The objective of such obligations is to limit the processing of personal data to the extent necessary for the fulfillment of the purpose of processing and to ensure that the processing of the data ultimately benefits society at large. The bill prohibits any processing of data except for a specific, clear, and lawful purpose[14]. It provides that personal data shall not be processed except with the consent of the data principal at the commencement of such processing[15]. Processing of personal data is allowed only for a purpose consented to by the data principal or any other purpose incidental thereto. Moreover, it is the duty of the data fiduciary that the processing is done in a fair and reasonable manner[16]. The data principal has to ensure that the processing is in the best interest of the principal and within his reasonable expectations. The bill also provides for a limitation on the collection of personal data by the data fiduciary. It allows for the collection of only that data that is necessary to fulfill the purpose of processing consented to by the data principal.[17] One of the most important facets of a data protection regime is to ensure that the data principal is provided with all the necessary information necessary to make an informed decision regarding the sharing of his personal data. The bill makes it a duty of a data fiduciary to provide the required information to the data principal in the form of a "notice" at the time of collection of the data or as soon as reasonably practicable. The notice shall comprise all the information like purpose of processing the personal data, nature of data being collected, rights of a data principal, whether any cross border of the acquired data is sought by the data fiduciary, the process for grievance redressal; and any other necessary information as specified by the regulations. The notice shall be clear, concise, and easily comprehensible. However, the bill does provide for circumstances where providing notice to the data principal is not required, especially in cases where such notice substantially

[14] Personal Data Protection Bill, 2019, s 4
[15] Personal Data Protection Bill, 2019, s 11
[16] Personal Data Protection Bill, 2019, s 5
[17] Personal Data Protection Bill, 2019, s 6

prejudices the purpose of processing the data[18]. The bill also requires the data fiduciary to maintain the sanctity of data collected by it and ensure that the personal data being processed is complete, accurate, and up-to-date.[19] The principle of storage limitation is also enshrined in the provisions of the bill. It obliges a data fiduciary to not retain any personal data beyond the period necessary to fulfill the purpose of processing. Regular review by the data fiduciary is required to determine whether it is important to retain a particular data set[20]. The bill puts the onus of complying with its provisions on the data fiduciaries.

CONSENT

The relationship between the data principal and the data fiduciary is skewed in favour of the latter. One way to balance this relationship is by giving power to the hands of the data principal. Consent and notice play this role in the data protection framework. Consent is an expression of an individual's autonomy. The bill attempts to not only bestow this power on the data principal, but it aims to ensure that the consent given is meaningful and not a mere formality lacking any force of authority. The bill provides that consent, in order to be valid, has to be free as per the standards set out in section 14[21] of the Indian Contract Act, i.e., it must not be caused by coercion, undue influence, fraud, misrepresentation, or mistake. Moreover, consent should be informed, specific, clear, and capable of being withdrawn. The bill also provides differentiation between personal data and what is called "sensitive personal data". Sensitive personal data is such data that has a higher potential to cause wrongful loss or gain in the event of unlawful processing. It may include financial data, biometric data, health data, religious or political beliefs, sexual orientation, etc. Given the delicate nature of such data, the bill provides that consent for the processing of sensitive personal data shall be taken explicitly over and above the general consent after informing the data principal about the additional risks associated with the processing of such data.

[18] Personal Data Protection Bill, 2019, s 7
[19] Personal Data Protection Bill, 2019, s 8
[20] Personal Data Protection Bill, 2019, s 9
[21] Indian Contract Act, 1872, s 14

It is important to note that a data fiduciary cannot make delivery of goods or services conditional upon consent for the processing of personal data not necessary for that purpose, and the burden of proof is on the data fiduciary to show that the necessary consent was obtained before commencement of processing of personal data.

NON-CONSENSUAL PROCESSING

The importance of consent in data protection law cannot be undermined, but there can be certain circumstances in which the whole framework of notice and consent can prove to be counterproductive and hamper the interests of society at large. Although the consent framework is an integral part of a free and fair digital economy, other interests cannot be ignored altogether. In the Puttaswamy judgement[22], Chandrachud, J, enumerated four such state interests that should be considered alongside the individual interest of privacy. These are national security, prevention and investigation of crime, protection of revenue, and allocation of resources for human development. Hence, the personal data protection bill provides for two categories of data processing without the consent of the data principal: (i) GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT and (ii) EXEMPTION FROM LAW. The former represents situations where interests other than the individual's consent prevail over it; however, all other obligations of the law applicable to such processing; while the latter constitutes restrictions on the right to privacy.

GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT

The bill provides for certain cases where the processing of personal data does not require the consent of the data principal. It includes Performance of functions of state like providing some service or benefit to the data principal or issuance of any license or permit and if a law passed by legislature demands such processing or it is required to comply with an order of the Court or tribunal in India. Furthermore, consent is not required in the case of a medical emergency or in a matter of public health, like providing health services to an individual during an epidemic. Providing assistance during a disaster or breakdown of public order also does not

[22] Justice K.S. Puttaswamy (Retd) (n 13)

require the consent of the data principal.[23] Processing of personal data, excluding sensitive personal data, in the course of employment of a data principal also does not require the consent of the data principal if such processing is done for recruitment or termination, to provide some benefit or service to the data principal, to verify his attendance or to assess his performance[24]. Other than the above circumstances, personal data can be processed without the consent of the data principal if it is necessary for a reasonable purpose as specified by regulation.

EXEMPTION FROM LAW

It is important to reconcile individual autonomy with the legitimate interests of the state. The Supreme Court in Puttaswamy's judgment has stated that any restriction on the right to privacy has to withstand three tests: (i) the restriction must be by law; (ii) it must be necessary and proportionate; and (iii) it must promote a legitimate state interest. Thus, a data protection regime must provide for watertight exemptions that cannot be misused. The bill provides power to the central government to exempt any government agency from its provisions. The central government may pass an order exempting any agency from following the provisions of the bill after recording reasons to do so. Such an order can be passed in the interest of the sovereignty and prevention of a cognizable offence against the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, and public order[25]. The central government may also exempt certain data processors incorporated in India if they are only processing personal data of individuals present outside the territory of India[26]. Additionally, the bill also provides other circumstances where some of the provisions of the act are muted. These include processing for prevention, detection, investigation, and prosecution of contravention of law, processing for the purpose of a legal proceeding, processing for personal or domestic purposes, or processing for a journalistic purpose[27]. Processing for research, archiving or statistical purposes is also exempted from the provisions

[23] Personal Data Protection Bill, 2019, s 12
[24] Personal Data Protection Bill, 2019, s 13
[25] Personal Data Protection Bill, 2019, s 35
[26] Personal Data Protection Bill, 2019, s 37
[27] Personal Data Protection Bill, 2019, s 36

of the bill, along with the exemption granted to manual processing by small entities from some of the provisions.

RIGHTS OF DATA PRINCIPAL

Even though the entire data protection regime formulated by the Personal Data Protection Bill is aimed at securing the rights of the data principals, the Bill provides certain rights explicitly to the data principals. These rights, which are based on the principles of autonomy, transparency, and self-determination, give data principals control over their data. These include

- Right to Confirmation of processing and access to the personal data processed by any data fiduciary, whereby the data fiduciary is obliged to provide the data demanded in a clear and concise manner. Furthermore, this right includes the right to access in one place information about all the data fiduciaries with which his data is shared[28].
- Right to correction and erasure of personal data in case of any inaccuracy, defect or in case the data is out of date. The data principal can also demand erasure of his personal data if it is no longer necessary to satisfy the purpose of processing. In the event of a dispute between the data fiduciary and data principal with respect to the accuracy of data, the data fiduciary shall indicate the same alongside the personal data[29].
- Right to data portability in case of automated processing. The principal has the right to receive or transfer such personal data to another data fiduciary in a machine-readable format[30].
- Right to be forgotten i.e. the data principal has the right to stop disclosure of his personal data if it has served its purpose, if the principal has withdrawn his consent, or if such disclosure is made in contravention of the provision of this bill[31].

[28] Personal Data Protection Bill, 2019, s 17
[29] Personal Data Protection Bill, 2019, s 18
[30] Personal Data Protection Bill, 2019, s 19
[31] Personal Data Protection Bill, 2019, s 20

The above rights, except for the right to be forgotten, can be exercised by the data principal by making a written request to the data fiduciary to that effect. The data fiduciary is allowed to charge a fee for complying with such a request. Moreover, the data fiduciary can refute such a request after giving reasons for such refusal in writing and informing the principal about his right to seek redress from appropriate authorities.

TRANSPARENCY AND ACCOUNTABILITY MEASURES

Lack of information about the processing of their personal data is one of the prime hurdles in securing the rights of data principals. Hence, the Bill provides for certain measures to ensure that the data principal is aware of the whereabouts of his personal data. Every data fiduciary is mandated to publish a "privacy by design policy" on its website after due certification by the Authority prescribed under the bill. This policy shall contain all the required information, like organisational and technical systems used by the fiduciary to prevent harm to the principal, obligations of the data fiduciary, and technology used in the processing of data[32]. The data fiduciary is expected to inculcate transparency in the collection of personal data of data principals.

It is the prerogative of the data fiduciary to ensure the safety and security of personal data of data principals through active measures like de-identification and encryption. The data fiduciary is required to prevent any kind of misuse, unauthorised access, or disclosure of personal data and must conduct a periodic review of safeguards taken[33]. If any personal data breach takes place regardless of the safety measures in place, the data fiduciary is obliged to report such breach to the Data Protection Authority constituted under the provisions of the bill through a notice[34]. The bill also provides for the classification of a data fiduciary as a "Significant Data Fiduciary" based on factors like volume and sensitivity of personal data processed, turnover of data fiduciary, risk of harm, etc. It is mandatory for a Significant Data Fiduciary to register itself with the Data Protection Authority[35]. As the potential for harm

[32] Personal Data Protection Bill, 2019, s 22
[33] Personal Data Protection Bill, 2019, s 24
[34] Personal Data Protection Bill, 2019, s 25
[35] Personal Data Protection Bill, 2019, s 26

caused is greater in the case of significant data fiduciaries, the bill provides additional regulations for them. Such a data fiduciary is required to appoint a Data Protection Officer that can act as a single point of authority for all things related to data privacy in the organisation structure of the data fiduciary.[36] Significant data fiduciaries also need to perform a Data Protection Impact Assessment before commencing the processing of any sensitive personal data[37] and maintain a record of all operations carried on personal data, review of safety measures, data protection impact assessment, and any other aspects of processing. A social media intermediary which is notified as significant data fiduciary shall enable its user to voluntarily verify their identity[38]. A significant data fiduciary is also required to get its policies and method of processing personal data audited annually by an independent data auditor. Data fiduciaries have also been required to set up an effective mechanism of grievance redressal within their organisational structure. A data principal may file a complaint with the data protection officer in case of significant data fiduciary, or with the designated officer in other cases, alleging a violation of the bill's provisions. Such complaint shall be resolved within 30 days; otherwise, the data principal is entitled to reach out to the Data Protection Authority. It is important to note that the bill makes the Re-identification and processing of de-identified personal data a criminal offence, whether done by an individual, company, or the state[39].

CROSS-BORDER TRANSFER OF DATA

The last few decades have seen an unprecedented interlinking of global economies. It has allowed the free flow of goods and services across national boundaries, and as a result, the internet has also been globalized. Naturally, it has an effect on the personal data of individuals. Information created in one country is easily available in other countries today. Such a flow of data has actually proven beneficial for the overall growth of economies. This makes it imperative for any data protection regime to provide protection against harm caused

[36] Personal Data Protection Bill, 2019, s 30
[37] Personal Data Protection Bill, 2019, s 27
[38] Personal Data Protection Bill, 2019, s 28
[39] Personal Data Protection Bill, 2019, s 82

by misuse of data stored domestically as well as against the data that has been transferred abroad.

Globally, two approaches are followed in regulating the transfer of data outside the territory:

- Based on the adequacy principle, wherein data transfer is allowed to pre-identified countries whose laws provide an adequate level of protection for personal data.
- Based on the accountability principle in which the transferor entity is wholly responsible for any breach in data privacy no matter where the data is transferred.

The Personal Data Protection Bill adopts a new approach by balancing the above two principles. The bill identifies two types of data when it comes to cross-border transfer- Sensitive personal data and Critical personal data. The central government has the power to notify which data is considered Critical Personal Data.

Sensitive Personal Data of a data principal can be transferred outside the border of India with the consent of the data principal but the bill makes it a condition on the data fiduciary that a copy of such data has to be stored inside the territory of India. However, such a transfer of data shall be pursuant to a contract or intra-group scheme that provides for effective protection of rights of data principal and provisions for determination of liabilities in case of a data breach. Moreover, the bill has also given the power to the central government to allow the transfer of sensitive personal data to countries where the data would be subject to an adequate level of protection. The Data Protection Authority can also allow the transfer of a specific class of sensitive personal data. In the case of critical personal data, the transfer can only be made when the entity is engaged in health or emergency services or when the central government has deemed it fit to do so. In the former scenario, the data fiduciary is bound to notify the data protection authority in a timely manner.

ENFORCEMENT MECHANISM

Any law is only as effective as its enforcement. The absence of a proper mechanism for enforcement would render the law toothless. Therefore, the bill proposes the establishment of

a robust and independent "Data Protection Authority" to oversee the entire framework of data protection regulations in the country[40]. The Authority is prescribed to be a sector-agnostic body corporate consisting of six whole-time members and a chairperson appointed by the Central Government on the recommendation of a selection committee. The chairperson and members of the Authority should be people of integrity with adequate experience in the field of data protection and security[41]. The chairperson is vested with all the powers of general superintendence and all other powers that are supposed to be exercised by the Authority. The Authority is entrusted with the duty to protect the interests of the data principal while ensuring compliance with the law of the land. It has been assigned a pivotal role in making sure that the rules and regulations are followed in its letter and spirit. The Authority is empowered to specify codes of practices to data fiduciaries to act as a guiding force for complying with the obligations for data fiduciaries as set out in the bill like model forms for notice, the manner for processing data, methods of de-identification and anonymisation, etc[42].

To perform the above functions, it is imperative that the Authority is given the powers required to perform them. The bill makes provision for the Authority to issue directions to data fiduciaries whenever required for the discharge of its function, and the data fiduciaries are bound to comply with such directions[43]. More importantly, the Authority is vested with the power of inquiry in case the activities of a data fiduciary are detrimental to the interests of data principals or are in contravention of the provisions of the bill[44]. For the purpose of the inquiry, the Authority is prescribed to appoint one of its officers as the "Inquiry officer" who shall submit a report on completion of the inquiry into the complaint, and the Inquiry Officer has been vested with the powers of the civil court as provided in the Code of Civil Procedure, 1908. Based on the report of the Enquiry Officer, the Authority can take appropriate action like issuance of a warning, reprimand, modification of business activities, suspension of business activities, etc.[45] The bill also provides for various forms of fines and penalties in case a data

[40] Personal Data Protection Bill, 2019, s 41
[41] Personal Data Protection Bill, 2019, s 42
[42] Personal Data Protection Bill, 2019, s 50
[43] Personal Data Protection Bill, 2019, s 51
[44] Personal Data Protection Bill, 2019, s 53
[45] Personal Data Protection Bill, 2019, s 54

fiduciary is found to be in contravention of the provisions of the law. Fines and penalties can be levied by an "Adjudicating Officer" appointed by the Authority in this regard after completion of an inquiry into a complaint. The Adjudicating officer also has the right to order the payment of compensation to a data principal who has suffered a loss due to a breach of data privacy. An appeal against the order of the Adjudicating officer can be made to an Appellate Tribunal established by the central government for this purpose[46]. An order of the Appellate tribunal can be executed as a decree of a civil court and such an order can be challenged in the Supreme Court of India on any substantial question of law.

APPRAISAL OF THE BILL: CONCLUDING REMARKS

The Personal Data Protection bill has been seen as a watershed moment for the privacy laws in the country. The bill has tried to provide a robust framework for data protection that can work as an enabler for a free and fair digital economy. However, there have been a few areas of concern that the bill has failed to recognize. The biggest point of critique towards the legislation has been the differentiation that the bill has caused to create between the private players and the state. The bill seeks to protect the privacy of data principles that have been read by the Supreme Court as part of the fundamental rights enshrined in the Constitution of India. It is to be noted that the state has been obligated to protect these fundamental rights, and the rights themselves are enforceable against the state. However, the Personal Data Protection bill has failed to make the state accountable for processing the personal data of its citizens. The provisions of the bill allow not only non-consensual processing of the data but, in certain circumstances, a blanket exemption from the law. Moreover, the Data Protection Authority, as envisaged by the bill, is also under the control of the state as the Selection Committee for its members only comprises the members from the executive wing of the government. Given the amount of data that the government processes, it is imperative that some form of parliamentary oversight should be established over the grant of exemption to the state. The private sector has also flagged issues with the provision of compulsory localization of the data. Arguments have been made that it would lead to an unnecessary increase in cost

[46] Personal Data Protection Bill, 2019, s 67

for the data fiduciaries without much benefit in terms of data privacy for the data principals. Furthermore, it is expected to have a bad impact on the overall ease of doing business in the country, aggravated by the bureaucratic nature of the Data Protection Authority. The bill was referred to a Joint Parliamentary Committee to further study the legislation and point out the issues that could be addressed. The JPC has recommended many changes in the bill, the most prominent being the inclusion of non-personal data in the ambit of the law and changing the name of the legislation to "Data Protection Bill". The JPC also recommends that the selection committee for the members of the Data Protection Authority should also include the Attorney General and one independent expert. However, the recommended changes are yet to be discussed by the Cabinet.