# AN ANALYTICAL STUDY ON THE LATEST DEVELOPMENTS IN THE PERSONAL DATA PROTECTION BILL AND ITS IMPACT ON THE DATA PRINCIPAL

**Sandra Paul**

## ABSTRACT

The Personal Data Protection Bill 2019 was a landmark achievement after the 2017 Puttuswamy judgement which recognized the right to privacy and acknowledged data privacy as a subset to it. The paper deals with the features and loopholes of the 2019 bill and all the changes brought in by the 2021 revision. It discusses about the privacy by design policy , about the institution of data protection authority, about the newest sandbox for innovation etc. Furthermore, important rights like confirmation to access , correction and erasure , data portability and most importantly the right to be forgotten is derived and utilised from General Data Protection Regulation of the European Union , 2016. It also discusses if the revision sufficiently cements the drawbacks. and concludes that it doesn't. We conclude the article by highlighting four core issues of data protection like the failure of consent based mechanism, raising the compliance cost , burdening the DPA with regulatory and preventive obligations and finally the problems rising due to the increased government autonomy in providing exemptions which has not been sufficiently addressed in the revised bill.. This is a simple straightforward article to understand the PDP bill from its inception up to where it stands now.

## INTRODUCTION

The Personal Data Protection bill, 2019 was launched by the Honourable Minister of Electronics and Information technology Mr.Ravi Shankar Prasad on 11th December 2019 and sought to protect the data privacy of individuals , technically called the data principals , with regard to their personal data and to establish a regulatory authority namely, the Data Protection Authority to safeguard the same.[1] The data fiduciaries who collect and store data, like big corporate companies say, Google, Meta, Amazon , Reliance and data processors third parties who aid in processing the data for data fiduciaries , say , Paytm or various software companies are all brought under the ambit of this Bill.

[1] Angelina Talukdar, *India:Key features of the Personal data protection Bill*, 2019 (16 March 2020) https://www.mondaq.com/india/data-protection/904330/key-features-of-the-personal-data-protection-bill-2019

## FEATURES OF THE BILL

### PARTIES BROUGHT UNDER THE AMBIT OF THIS BILL

The proposed Personal Data Protection Bill, 2019 or from here on the PDP seeks to bring within its ambit all data, defined under the IT Act, 2000 , either collected or shared or disclosed within the territory of India , which could be by an Indian state , any Indian Company including one person company[2], by any individual be it common man or politicians , any body of persons or individuals as mentioned earlier who were incorporated under the ambit of Indian laws and the processing of personal data by those data fiduciaries or data controllers, who though not incorporated in India , has a business in India and collects data of Indian Data Principals in that process[3]. It also includes those Data Principles and Data Processors who simply provide goods and services in India. Data profiling in general falls within its ambit. An exception to its application was for anonymized data and non-personal data which has undergone changes in the new amendment which shall be discussed later.

**What is Personal Data?**

Personal data is defined to mean those data relating to only natural persons who through certain characteristics or traits or attributes or any other feature or through a mix of these can be directly or indirectly identifiable . These data can be collected online or offline and **may include a combination of the abovesaid features with any other complementary information which could help draw inferences about this natural person for profiling purposes.**[4]

**Sensitive Personal Data**

Sensitive Personal Data as the name suggests is any data that which according to **section 4**[5] of

[2] Personal Data protection bill,2019, No. 373,Acts of the Parliament,2019(India)

[3] Ankit Viramani and Sonali Saraswat*, Data Privacy Bill All you Need to Know*, PWC , https://www.pwc.in/consulting/cyber-security/data-privacy/personal-data-protection-bill-2019-what-you-need-to- know.html

[4] *Supra* note 2 at Section 2(28)

[5] *Id*

the act can only for a specific, clear , lawful purpose due to its very nature. It includes all those data that reveals intimate details about a person like health, finance, sexual orientation, biometric data, caste/tribe, genetic details, intersex/transgender/sex life, religious beliefs and political affiliations. It also includes any other data that may be recognized as critical or sensitive by the respective sectoral regulators.[6] Thus the abovesaid data can only be used with the consent of the data principal and if used without consent only for the related purpose of the specific purpose for which data was collected in the first place[7] in a fair and reasonable manner.

The data fiduciary must according to **Section 9** [8]of the PDP bill delete the data procured upon the completion of its processing and must not retain it beyond the period required for processing or stipulated period and must seek additional permission from the data principal for extension.[9]Also **Section 12** of the act talks about situations where personal data can be processed without consent or in short exemptions, like when the parliament or state legislature mandates it, during an epidemic outbreak, natural disasters, in situations where the data principal benefits from the state for its service in return for the data provided, in order to comply with any judgement or order passed by the judiciary be it courts or tribunals or for the issuance of any license or certification for the activity of the data principal. **Section 14** of the act interestingly justifies the collection of personal data for operation of search engines, mergers and acquisitions, prevention of unlawful activity like fraud, credit scoring , recovery of debt etc and categorizes it as reasonable.

**Privacy By Design Policy**

This is a mandate imposed on Data Fiduciaries under **Section 22** of the act to prepare and design a policy to protect , secure and prioritize data privacy at their managerial level, to incorporate the same into their business practices and other technical domains. It is also considered as an obligation upon the data fiduciary to exercise it while processing personal data, that the businesses develop their

---

[6] *Id*

[7] Personal Data Protection Bill,2019 of § 4 and 5 , No. 373, Acts of the Parliament,2019(India)

[8] Personal Data Protection Bill, 2019 of section 9 , Acts of the Parliament , 2019 (India)

[9] Wendell J. Bartnick , Shenna Bradshaw, Alexandra Chughtai-Harvey & Mary Isensee, *Present and Future Data Privacy* Outlook, 24 Currents: J. INT'l ECON. L. 70 (2020).

legitimate interests for innovation and expansion without compromising privacy, that they give a high priority status to data from its collection stage up to the stage of deletion. That all these planning and executions be done in a transparent manner. It also provides that the interest of the data principal be accounted for at every stage and that the data fiduciary is liable to submit the design policy to the regulatory authorities for certification.[10]

**Data Protection Authority**

Data Protection Authority is a newly setup statutory body that consists of a chairperson and 6 other members whose appointment is conducted by a special committee consisting of qualified individuals whose specifics are as mentioned in **section 42**, by the Central Government. Sections 41-50 of the PDP bill highlights the composition, appointment , qualifications, criteria for removal, terms of dealing with vacancies, the powers of the chairperson , powers and functions of the authority, codes of its practice etc.

The DPA is authorized , in addition to enforcement and monitoring of the provisions under the act ,to maintain a database on its website to provide **data trust scores** to significant data fiduciaries so as to indicate their level of compliance and obligations. It is also to take immediate and suitable action to respond to personal data breach. It is even responsible to examine **data audit reports** of companies and take related actions in case of non-compliances. It issues certificate of registration, renewal, withdrawal, suspension and cancellation and maintains a database for such registered data auditors. It is also obliged to specify the qualifications, code of conduct, accountable to conduct practical trainings for the functions performed by data auditors. It monitors cross- border transfer of personal data and lays down the code of conduct. Finally it categorizes data fiduciaries for example like significant and non-significant data fiduciaries.[11]

**Data Protection Officer**

DPO's are officers appointed by those body corporates or individuals, qualified to be termed as Significant Data Fiduciaries. These officers are exclusively responsible to nudge the data

[10] Personal Data Protection Act,2019,§ 22 , No. 373, Acts of the Parliament,2019(India)

[11] Personal Data Protection Act,2019,§ 40-50 , No. 373, Acts of the Parliament,2019(India)

fiduciary to enforce compliance with the PDP. He /She must have the requisite qualification to carry out the following obligations namely, delivering advice and information to the data fiduciary, to ensure that the Data Fiduciary progresses out data processing without infringing the provisions as well as aiding it to conduct Data Protection Impact assessment and its review process. This is given under **Section 27(4)** of the bill. Now, it is also required to advice the data fiduciary to plan and develop internal mechanisms to comply with the act and should maintain an inventory of records under **Section 28** of the act. They are to act as an intermediary between data principal and data fiduciary under **Section 32**.[12]

**Rights of Data Principal**

**1.Right to confirmation and access**

The data Principals are empowered to receive corroboration on whether their data is being processed or has already processed the same. It also has the right to know the details about data being processed or that has already been processed by the data fiduciary or a summary thereof .A summary of the processing activities can be demanded by the data principal inclusive of any information provided in the notice related to such processing. The data principal has the statutory permission to identify as to whom the information has been shared and how it has been shared.[13]

**2.Right to correction and erasure**

This a is very significant right given to the data principal that enables it to correct inaccurate and misleading data as well as to complete the incomplete personal data. It can also demand to update the personal data which is out of date as well as seek erasure of the personal data which has completed its processing or is no longer needed for the same.[14]

**3.Right to data portability**

The data is processed automatically and the data principal is entitled to receive the data in a structured, commonly used , machine readable format like the personal data given to the data

[12] *Id* at Section 30

[13] *Supra* Note 9 at 17(1)

[14] *Id at* 18(1)

fiduciary, the data used during the provision of services or goods by the data fiduciary, or data included in any profile of the data principal or which is obtained by the data fiduciary, or even to have the data transferred to any other data fiduciary.[15]

**4.Right to be forgotten**

If the purpose for which the data collected from the data principal with consent has been satisfied or is no longer a purpose , then the said consent can be withdrawn by the data principal. This is a right given in EU's GDPR and is a landmark right. If the consent has been given under **Section 11** it can be withdrawn. The same can be done if it is made contrary to the provisions of PDP or any other existing laws.[16]

**Obligations of Data Fiduciaries**

Data fiduciaries, be it a class like significant data fiduciaries are categorized on the basis of various factors like, the volume of data processed, whether it processes personal data or sensitive personal data, based on the turnover of the data fiduciary, on the risk of potential threat or harm to the data fiduciary, the usage of latest technologies for processing data, the potential harms caused by such processing of data etc.[17]

Now, **Section 23(3**) introduces the concept of a consent manager which is an interoperability platform to provide transparency and accessibility to the data principals. Through this platform the data fiduciary lets the data principals to gain, withdraw, review and manage his consent. [18]

**Social Media Intermediaries**

These entities can be classified as significant data fiduciaries depending upon their user threshold, if the actions of the participants or they themselves are likely to have a significant impact on electoral democracy, state security, sovereignty and integrity of India, public order

[15] *Id* at 19(1)(a)

[16] *Id* at 20(1)(a)

[17] *Id* at section 26

[18] *Id* at section 23

etc. This list shall be formulated by the Central government in consultation with the DPA.[19]

**Security and Transfer of Data Outside India**

The whole act is about protecting personal data from breach or internal-external misuse. So the act obviously makes sure to specifically prohibit the processing of sensitive and critical personal data outside the Indian territory. Sensitive personal data can be transferred outside India on a condition that the original sensitive personal data must continue to be stored within the domestic territory. The same way critical personal data can only be processed within India. And what includes critical personal data would be notified by the central government from time to time.[20]

Data can be transferred outside India only with the consent of the data principal and must be sought only in three specific situations. **Firstly**, if it is collected in pursuance of a contract or an intra-group scheme. The DPA must approve such standard contractual clauses or intra-group schemes only when such clauses or schemes protect the rights of the data principals. Now if it is the data principal who seeks to transfer personal data it is to periodically certify that the transfer is made as per the standard contractual clauses or intra group schemes and that it shall personally bear the consequences of any harm or liability incurred due to this non-compliance. **Secondly**, if the Central government has approved the quality and extend of data protection afforded by the other country or entities based in that country or be it of International Organizations. That is if it is confident about the level of security, considering the laws applicable as well as international agreements that boosts the enforcement of such protection by authorities with jurisdiction. **Thirdly**, if the sensitive personal data or a class of sensitive personal data is being processed for a particular purpose, like actions under **section 16**, for the provision of emergency or health services. Another situation is if the Central government deems such transfer a necessity.[21]

**EXEMPTIONS[22]**

---

[19] Wendell J. Bartnick , Shenna Bradshaw, Alexandra Chughtai-Harvey & Mary Isensee, Present and Future Data

[20] *Supra* Note 16 at Section 33(1)

[21] *Id* at Section 41

[22] *Id* at section 35

The Central Government can in many situations be exempted from seeking consent from the data principals for processing data like to protect and uphold the sovereignty and integrity of India, to ensure the security of the State, to maintain and nurture friendly relations with foreign States, to keep up the public order, to prevent the incitement to commit any cognizable offence, direct that all or any of the provisions of this Act to not apply to any agency of the Government in respect of processing of such personal data[23]. Also for issues like prevention, detection, prosecution and investigation of any offences, for enforcing any legal right, for the exercise of judicial functions, journalistic purpose, by natural person for any domestic or personal purpose. Other Exemptions include for research, archiving or statistical purpose[24], exemptions for manual processing by small entities[25]

**Sandbox For innovation**

The authority shall for the purpose of encouraging innovation in artificial intelligence and machine learning and any other emerging technology create a sandbox. The advantage of inclusion in the sandbox is that the data fiduciaries would be exempted from the legalities under sections 5 ie, restriction on purpose of processing of personal data which impliedly means that it need not always be fair and reasonable, can collect more data than required[26].It even means that it can retain information for periods more than specified and subsequent relaxation in deletion.

**Re-Identification and processing of De-Identified Data[27]**

In order to further the pace of the digital economy, growth, security, integrity, prevention of misuse of policies governing personal data, the central government may direct, direct any data fiduciary or data processor to provide any personal data anonymized or other non- personal data to enable better targeting of delivery of services or formulation[28] of evidence- based policies by

---

[23] *Id* at Section 17(1)

[24] *Id* at section 38

[25] *Id* at section 39

[26] *Id* at section 26(4)

[27] Wendell J. Bartnick , Shenna Bradshaw, Alexandra Chughtai-Harvey & Mary Isensee, *Present and Future Data Privacy* Outlook, 24 Currents: J. INT'l ECON. L. 70 (2020)

[28] *Supra* Note at section 91(2)

the Central Government, in such manner as may be prescribed.[29]

**Penalties**

The act prescribes for strict penalties for non-compliance of any provisions by the data fiduciaries or processors on their behalf[30].In case of non-payment of any penalties under this act it may be treated as if they were to be recovered as arrears in land revenue.[31]

## LOOPHOLES

A. **Lack of clarity in objectives :** The loudest criticism against the PDP bill is its lukewarm approach which can be traced back from Justice SriKrishna Committee's report. It in many ways confuses the public as to its intention. The preamble of any legislation which ought to provide the real intent behind any legislation and which aids in its interpretation provides a vague idea without context here. The preamble contains its objective like creating a collective culture which promotes a free and fair digital economy, progress and innovation, while respecting informational privacy .It does not in any way emphasize that the legislation intents to protect the fundamental right to privacy of an individual through protecting their data. As a result, the entire focus is on economizing rather than safeguarding. Furthermore, the bill fails to provide a limit on how much private data the government can obtain and has little safeguards against such access. The global evolution of privacy makes it painfully clear that stringent legislation must be enforced to safeguard against government interference in personal records.[32]

B. **Preference to private and fiscal interests over data protection:** The PDP Bill, has come up with an innovative mechanism through section 40 , to tackle the problems of regulatory compliance hampering technological innovations. It proposed for the creation of a sandbox for innovation a concept adopted from the Singaporean Data Protection

[29] Id

[30] *Supra* Note 24 at 64

[31] *Id* at Section 66

[32] *A Public brief and Analysis on Personal Data Protection Bill,2019*, INERNET FREEDOM FOUNDATION (January 25,2020) 10https://saveourprivacy.in/media/all/Brief-PDP-Bill-25.12.2020.pdf

Rules, and subsequently implemented in UK which provides large carve-outs for anonymized non-personal information. The principle aim is to provide a controlled regulated environment including access to historic data details of data principals without their consent to test new products related to artificial intelligence or say machine learning to promote innovation and thereby technological advancements. Another feature here is that data fiduciaries can apply to be in the sandbox for fixed period when they will enjoy relaxed rules and whether or not to allow them and the criteria used for granting permission is absolutely discretionary without any proper guidelines. There are unusual insertions that are not found in global data privacy regulations. The PDP Bill's requirements would not extend to anonymized data (Section 2(B)). Anonymized data is best described as data that is in its least identifiable form when compared with its original data, or in other words has been converted to such an extent that it hardly related to its original data sets. It cannot be now identified according to the authority's requirement under sections 3(2) and (3).

The Biggest exception and perhaps the most important is that the Central government can after consulting with the DPA demand for both anonymized and Non-anonymized from any data fiduciary or processor for providing better services to the public as well as in the name of law enforcement. All of which have no proper guidelines. The central government will also develop digital economy policies as long as they do not regulate personal data (Section 91). There is no verified literature or provision on what constitutes non-personal information. The most notable pitfall is that there is no clear demarcation between anonymized data ,when it get mixed with non-anonymized data which happens a lot these days. This mixing eventually reveals the identity of the data principal breaking the intention behind the anonymity. [33]

C. **Collection of data without consent and denial of services:** There are a number of circumstances in which the government and other agencies can collect data without permission and refuse critical services without data principal's permission such as for delivering facilities, incentives, licenses, complying with a court's decision or order, responding to medical emergencies, and taking action in the event of a catastrophe or a

[33] *Supra* note 29 at section 34(1)

collapse in public order. Furthermore, the exemption from consent extends to personal data obtained by employers for training, verification of attendance, performance evaluation, and so on (Section 13), as well as other 'reasonable reasons' (to be defined by regulation) ranging from whistleblowing to the functioning of search engines as specified in Section 14. The exemptions listed out are extensive with very frugal clarity which raises queries as to the extend of delegation of powers afforded without check and thereby violating privacy. The data collection of minors require to be done with the consent of a trustee again challengeable and the age verification of any data principal is done by a data fiduciary as per section 16. It is said that the acquisition of a product or service, or the enjoyment of a lawful right or argument, or the like, shall not be withheld due to a lack of permission to process data that is not required for that reason. However, if permission is granted and then withheld for whatever cause, the data principal will be held responsible for all legal implications (Section 11). There have been several instances of service denials of essential resources such as rations and medical assistance being deprived off to the beneficiaries, hence not very clear about the implications of refusal to provide essentials[34]

D. **Strengthen user rights:** Although certain consumer rights are present, rights such as exemption from automatic decision making are not given to individuals. Other exemptions and carve-outs must be reconsidered. Section 18 provides the right to data modification, completion, updation, and erasure, although it is restricted because the data fiduciary's duty to comply to these rights is contractual, and it can also deny a user request. **Section 19** provides for the right to data portability, but data fiduciaries can refuse it on the basis of technological infeasibility or the security of a trade secret. Personal data is not a trade secret in this context since it specifically affects people's human rights. The data fiduciaries are allowed to charge a specific amount for giving in to the requests made by the data principals. This is explained in section 21. These basic privileges afforded to the data subjects must not be overpriced. As per Section 25 in the event of a data breach, the data fiduciary must contact the Data Protection Authority as soon as practicable if the breach is likely to inflict damage to another data principal.[35]

[34] *Id* at section 34(1)

[35] Id at 32

E. **Social Media Entities:** The laws surrounding social media organizations using consequences, including increased monitoring and profiling. The Bill describes a social media agent and provides that it can be graded as a major data fiduciary based on the number of users and the effect on political democracy, state security, public order, and so on (Section 26). Such social media intermediaries must allow their users to "voluntarily" validate their accounts in the manner described, and such authenticated accounts must be marked with a noticeable label. This could adversely affect the chances of whistleblowers and victims of social harassment from coming out and sharing important information or their experiences under the garb of anonymity.[36] It is unclear if the means devised support the appropriate forum for addressing the specified intent. That would result in more data gathering by major social media platforms based on government IDs, as well as more targeting and surveillance. Such a clause is not found in any data security legislation anywhere in the world, and it deviates from existing privacy norms. This provision would also raise the risk of data breaches aids in the concentration of control in the hands of major data giants who can afford to advance and retain those authentication systems. There are fears that amendments to the Information Technology Act of 2000 and its regulations would require intermediaries to disclose accounts that do not validate themselves to the government, making them a target for political censorship and chilling dissent.[37]

F. **Data localization:** The data localization clauses was inadvertently inserted into the data privacy legislation. They are broad, ambiguous, and offer the government a lot of leeway. Although there is no provision for "personal data" to be localised, the Bill does note that "sensitive personal data" can be transmitted outside India (by securing express permission from the data principal and enforcing additional protections such as deciding if sufficient security would be provided), but must be retained in India . The term "sensitive personal data" is nowhere specified in the Law. But, the government is allowed to identify critical personal data in the future stags of such collections, and identify such data which cannot be transmitted outside India at all except for timely

[36] *A Public brief and Analysis on Personal data Protection Bill,2019*, INERNET FREEDOM FOUNDATION.1,3(2020) 10https://saveourprivacy.in/media/all/Brief-PDP-Bill-25.12.2020.pdf

[37] Id

intervention during a health emergency or to an institutional agency or named individual, or any foreign organization to which the Central Government permits such transfers under Sections 33 and 34. Though the government is allowed to collect and store persona data the Bill mandates collecting and manipulating confidential and vital personal data in India, it raises questions about the state's unbridled invasion of privacy. The GDPR of the EU divides data into two categories: personal data and non-personal data/Special categories. The former is close to the Bill's concept of personal data. The latter contains information about race, gender, political views, religious beliefs, and so on. It is necessary to remember that the GDPR does not have a provision for data localization.[38]

G. **Surveillance reforms:** One of the most apparent flaws in the PDP Bill, 2019, is the vast number of provisions given to the government in order for it to exclude its own agencies from the law's implementation. Furthermore, there is a total lack of action to capitalize on the historic potential for privacy changes. Section 35 of the Bill empowers the Central Government to exclude 'any department' of the government from any or any aspects of the data protection legislation by order if it is in the interest of India's dignity and independence, the welfare of the state, good ties, public order, and the prevention of incitement to commit an offence. The only means of check and balance would be the necessity of having a written government order required to assert that the actions taken are "necessary and proportionate". This is an advantage which can be used only in exceptional situations but the extent to which it would safeguard the users and their data is not guaranteed. These disclosure exemptions will benefit not only the governments data fiduciaries but also to the data shared with other institutions by these data fiduciaries. Thus the central government becomes the sole custodian or protector of such procured data and vests the discretion of whether or not to disclose and if chooses to do so , under what conditions, with nobody to question. Section 36 expands on the specific situations in which such protections won't apply. Section 37, which deals with foreigners data being accessed and processed by the Central government is vague. The majority of India's intelligence services lack formal supervision, and there are no rules that specifically describe or restrict their powers. Another important pitfall is that the Bill provides no explanation for scenarios like phone tapping or email

[38] *Supra* Note 33 at Section 39

interception etc which at hindsight implies that the bill is pro government and that it equips the state with ample opportunities for mass surveillance and chances for a big brother is not completely sidelined.[39]

H. **DPA's selection, staffing and independence:** Another backdrop of the PDP Bill, 2019, is the lack of guidelines or lucidity in the DPA's selection committee, which is made up solely of government officials with little input from the courts, the opposition, or civil society. This is significant because the DPA is designed to shield people from both private and public bodies. According to Section 42, the Appointment Committee for selecting Authority members would be made up exclusively of members of the executive. The draught bill from the Srikrishna Committee in 2018 called for a diverse selection committee of executive, legal, and outside experience**.** Seeing that this new legislation still shields consumer data from the government, there is a lack of impartiality since the regulatory mechanism would be enforced primarily by the government. This setting would cause several hardships on the DPA committee to function without having to bend before government interests. The Bill further grants central government with the power to send binding directives on the DPA which greatly falters its independence. Section 86 says so. It should also be noted that DPA is a state authority and is burdened with lots of responsibilities which makes it subtle to have state authorities to delegate power to but this has not been envisaged in the Bill which could prove fatal in the long run. Section 62 deals with adjudication of complaints and the adjudication officers are to be selected by the committee forming the DPA which essentially are government representatives. This questions the autonomy in their decisions. Also as per section 63 they are permitted to only look into enquiries[40].

I. **Miscellaneous Findings:** Provisions on the effect on the RTI Act and the need for the protections to apply exclusively to natural persons must be considered. It is worth noting that the Bill does not recognize a natural individual as the owner of their records. Another disadvantage of the bill is its prospective nature. It does not apply to the data collected prior to the Bill and is in dearth of any transition clauses. Furthermore, the Bill

[39] *Id* at 35

[40] *Id* at 35

has been granted an overriding impact under Section 96. The EU GDPR revoked the EU's previous Directive also known as the Data Protection Directive. In EU the situation is handled in this manner, recital 171 clearly mandates that all those data that was processed under the previous directive is to be brought under the GDPR in a span of two years from the date of it coming into force. Also consent once given under the directive need not be repeated under the GDPR at any cost[41].

J. **Protection for vulnerability testers and whistleblowers**: In case of whistleblowing , Section 25 of the act only requires a data fiduciary to highlight wrongdoings , breaches and evasions and need not reveal the name of the informant. The provision of a water-tight identity protected process is important for the employees to enquire and take the requisite actions during investigations without the fear of being backlashed or thrown into institutional troubles and media trials. Though such an analysis is excluded from Section 38 obligations, there are no specific protection criteria in place to protect qualified cyber security researchers who engage in such vulnerability testing. Many of those brave hearts who engage in the same are mostly subjected to vexatious accusations and prosecutions along with media trials.[42]



## THE REVISED BILL

**1. Specified the timelines for implementation : The clause 1 of the revised** DPA bill, 2021 provides data fiduciaries and principals will be given 24 months to make changes in their infrastructure, internal policies and processes so as to comply with the provisions of the proposed act. The DPA is suggested to start functioning within 6 months, the data fiduciaries to complete their registration within 9 months and the Data Protection Appellate Tribunal to commence functioning within 12 months. The 2019 bill had not specified any time limit for the implementation of its important provisions.

**2.Scope of the Act : As per clause 2** the most notable change to the PDP bill is that post revision it has expanded its scope to include non-personal data whereby the bill will from

[41] *Id* at 35

[42] *Id* at section 64

now on be known as the Data Protection Bill,2022.The same regulator ie, the Data Protection Authority (DPA) regulates non-personal data because it is difficult to distinguish personal and non-personal data now as the volume of data generated, exchanged and converted has become humungous.

***NON-PERSONAL DATA***[43]

Though the PDP Bill, 2019 mentioned non-personal data, it was not brought under its ambit but was considered pertinent to better enable the Central government[44] to target delivery of services and to formulate evidence based policies"[45]. It was only in the Non-personal Data framework proposed by the committee under the Ministry of Electronics and Information Technology (MeitY) did Non-Personal data get a solid identity. The PDP Bill defined NPD to include all other data than the personal data. However here the Committee classifies it into three categories- **1.Public data 2.Community Data 3.Private Data**

Public Data includes all those anonymised data available like land records, public health information, vehicle registration etc.[46] Now community data includes those data sets collected by municipal corporations and public electric utilities, datasets comprising user information collected even by private players like telecom, ecommerce, ride hailing companies.[47] Finally private data would be the inferred or derived data or insights involving application of algorithms-proprietary knowledge etc.[48]

The main issue likely to crop up is that some NPD's are as mentioned before the proprietary knowledge of businesses, procured through huge investments and restricting or regulating the same would raise controversies.

**3.Defining Terms**

---

[43] Vidushi Marda, *Non-Personal data: The Case of the Indian data protection bill, definitions and assumptions,* (15 October 2020) https://www.adalovelaceinstitute.org/blog/non-personal-data-indian-data-protection-bill/

[44] *Id*

[45] *Id*

[46] *Id*

[47] *Id*

[48] *Id*

**Clause 3 of the bill has** many terms previously undefined but which has been defined in the revised bill. Terms not limited to but including "consent manager," "data auditor," "data breach," "data fiduciary," "data processor," "data protection officer," "harm" and "non-personal data."

**4.Processing of personal data without consent**

This concept has been improved to balance the interests of both the data principal and data fiduciary as visible in **clauses 13 and 14** The provision has been modified to support the data fiduciary when it comes for employment purposes.What is a reasonable purpose is determined by the regulatory authorities and legitimate interest is the criteria to be used by the regulators to process personal data.[49]

**5.Processing of personal data of children**

Personal data of children are processed to protect the "rights of the child" now against "the best interests of the child" earlier. The Data fiduciaries exclusively dealing with children's data must compulsorily register with the DPA and inform the child three months prior attaining majority so as to get his/her consent again. This is reiterated **in clause 16** of the revised bill.

**6.Modifying the rights of data principal or user rights** Just like how a probate or will transfers an individual's property or as bank nominees enjoy the security after the principal's expiry , the data principal can choose a legal representative or a legal heir who will decide how to handle the principal's data upon his death or any other casualty. Also trade secrets are no longer a ground to deny porting of data except for reasons like technical feasibility. And this has to be directly determined by regulations. Additionally the data fiduciary is responsible to ensure transparency and fairness of the algorithms and methods utilised for processing data.

**7. Breach reporting**

As per the 2021 study report by cyber security company Surf Shark the data of 86.63 million users have been breached and this is 17.85% higher than 2020.[50]An IBM study reports that his average

---

[49] Nitin Davate, Ramkant Mohapatra *, A look at proposed changes to the Personal data protection Bill* (5 January 2022)https://iapp.org/news/a/a-look-at-proposed-changes-to-indias-personal-data-protection-bill/

[50]*Key Takeaways: The JPC Report and data privacy* Report (16 December 2021) https://internetfreedom.in/key-takeaways-the-jpc-report-and-the-data-protection-bill-2021-saveourprivacy-2/

data breach costs 16.5 crores[51].Thus as per the new developments data breach now includes both personal and non-personal data. The timeline for reporting has become 72 hours within first coming to knowledge about the breach. The DPA can adopt any measures to promptly remedy or mitigate the harm caused due to the breach. But **clause 25** still allows the DPA to retain the discretion to report such breaches to the data fiduciary depending upon the severity .

Also the 2019 bill did not have a whistle blower protection and **section 25** provided the Data fiduciary with a discretion to report such infringements to the DPA ie, "where such breach is likely to cause harm to the data principal". This phrase has been removed in the revised bill. The revised bill continues to ignore the skilled cyber security experts conducting vulnerability tests and affords no exemption or protection to them.[52]

**8.Social media platforms**

The Joint Parliamentary Committee had stated in its report that social media platform has been designated as intermediaries and that the IT Act, 2000 failed to regulate the same. Hence it proposed to consider them publishers as they publish content and they can even select the receiver and accessors of the contents. However, this was not incorporated into the 2021 bill, which is disappointing as it diminishes the liability of these platforms. The committee had explicitly mentioned about the need to have a specific regulation like UK's Online harms Whitepaper to regulate them. However, the preamble changes the term social media intermediaries to social media platforms.

**Clause 26** determines a social media platform to be a significant data fiduciary depending on the prescribed thresholds notified by the authority as well as on the lines of the impact it would have on the sovereignty and integrity of India, electoral democracy , security of the state and maintenance of public order. This also invites other regulatory mandates like to conduct data impact assessment under clause 27 and to register with the DPA, failure of which could attract penalty.

Due to increasing instances wherein anti-social elements create social media fake accounts and uses it to plan, instigate, organize and execute protests, riots and revolutions, the JPC suggested a mechanism wherein the users verify their accounts, submitting necessary documents and then the

[51] *Id*

[52] *Id*

social media intermediaries must verify these accounts. The other platforms to be held liable for the contents in their unverified accounts. However , the new bill allows the users to voluntarily verify their accounts. This too raises a threat, as such verified accounts will be marked and this could become a future norm through mass practice. This may effect minorities, victims of sexual harassment or even whistle blowers who seek anonymity. This regulation is also not found in any other country.[53]

9.**Data protection officer and data transfer**

While **clause 30** specifies the qualifications of the DPO **clause 34** has modified the data transfer mechanisms, ie now to transfer data through an intra-group scheme or contracts require the consent of the Central government to check if its against public policy. The government agencies which were unilaterally exempted from all or any provisions of this law can now avail this exemption if it is just reasonable and a proportionate procedure. This is provided under clause 35 of the act. Experts still find this an overarching provision that could be misused in future.

**10.Composition of the DPA**

Has been expanded to include the attorney general of India with one director from an IIM and one director from an IIT nominated to the DPA. The total number of expert members would be 6 and an independent expert would have to be identified by the government from the field of data protection, IT, data management or data science and data security services.

**11.Testing and certification of hardware devices**

Rightly identifying the lacunae in provisions to test hard wares , the bill proposes to setup dedicated testing labs and other units to test the efficiency, authenticity and security of the hardware and software for all digital and IOT devices .The bill envisions individuals to be able to test their devices and to approach the DPA if the device fails to meet the standard claimed by the manufacturer and take actions against them. This is laid down in **clause 49** of the revised bill.

**11.Data localization:** The act requires to mandatorily bring data into India within a fixed time period and to directed the government to make a comprehensive policy after discussing with the concerned sectoral regulators.

---

[53] *Id*

**12.Privacy-centric alternative financial payment system:**

Just like SWIFT Banking , which is a member owned financial trading co-operative providing secure transactions among its members, it also suggest a parallel financial system but which is privacy centric, with the aim to reduce online financial frauds, hesitation among consumers and to expand India's digital market.[54]

## CONCLUSION

The Personal data Protection Bill, 2019 was criticised for 4 specific reasons. The first that strengthening the " consent" based mechanism is ineffective because according to an IBM survey 71 % of the users were willing to use a technology giving up their privacy and only 16% opted to walk out of a company that misused their data.[55] Another survey on the online behaviour of 48,000 visitors to 90 online software companies showed that only 2 out of every 1000 software shoppers even accessed the End-User License Agreement.[56] Secondly that it would raise the compliance cost of small-midsized companies and thirdly that the new bill imposes a lot of responsibility on the DPA including preventive obligations, security measures , transparency and reliability measures which are regulatory in addition to the supervisory functions. Fourthly , the bill gave government a wide discretion to provide exemptions to the whole or any part of the bill to any body corporate.[57] This raised concerns of government surveillance and big-brother syndromes.

While the bill tries to ease the compliance costs to an extend , it fails to resolve the other three drawbacks which directly injures the common man aka data principals in this case. The revised bill through its **non-obstante clause in clause 35 makes government exemptions easier.** It says that not withstanding any other law for the time being in force the government can make exemptions.

---

[54] Nitin Davate, Ramkant Mohapatra *, A look at proposed changes to the Personal data protection Bill* (5 January 2022)https://iapp.org/news/a/a-look-at-proposed-changes-to-indias-personal-data-protection-bill/

[55] Erik Sherman*, "People Are Concerned About Their Privacy in Theory, Not Practice, Says New Study," Fortune,* (February 25, 2019) https://fortune.com/2019/02/25/consumers-data-privacy/.

[56] Yannis Bakos, Florencia Marotta-Wurgler, and David R. Trossen, *"Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts,"* SSRN ( January 1, 2014), https://papers.ssrn.com/abstract=1443256

[57] Anirudh Burman, Carnegie India, *Will India's proposed data protection law protect privacy and promote growth*https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-lawprotect-privacy-and-promote-growth-pub81217#:~:text=In%20December%202019%2C%20the%20government,for%20data%20protection%20in%20India.&text=Union%20of%20India%20held%20that,a%20fundamental%20right%20to%20privacy. March 09 2020

They added the words **just, fair , reasonable and proportionate** procedure but this is just a safeguard to institute suits once the data is breached and does not make it a precondition to exercise this exemption ground.[58] The preconditions or standards for granting exemptions are just two terms-"necessary" and "expedient". And the dictionary meaning of expedient would mean useful and necessary in a particular situation, but sometimes morally unacceptable.[59] The governments rights to cross-border transfer of data enjoys similar powers.

The revised bill like the previous draft does not address or regulate or provide provisions to control mass surveillance technologies and interception. Nothing in it regulates facial recognition nor does India have any law to regulate facial recognition usage. Thus the bill totally addresses only the conditions under which the data is gathered with consent and with prior notice by the government.

Secondly, the DPA is still subordinate to the Central Government. That is the composition of the DPA is such that it may not be able to function as an independent, autonomous body. As per clause 42 of the bill, the Selection Committee appointing the members of the DPA entirely comprises of the executive members. Though independent personnel like the attorney general, director of any IIT or IIM is chosen, these appointments are made at the pleasure of the Central government. Furthermore, **Clause 86** of the makes the DPA answerable to the Central government on "questions of policy". Now after the JPC's suggestion, the DPA is bound by the Central government under all cases and not just on questions of policy. This has made the DPA a puppet under the hands of the central government. **Clause 94** of the Bill has also further expanded the powers of the Central government into new subject areas. [60]

Thirdly, bill does not recognize ownership over his/her data by a natural person, rather classifies it as the new age currency and as an asset of national importance which has not been utilized and which is waiting to be tapped into, to fuel the country's economy. The setting up of innovation sandboxes under **Section 40** of the 2019 bill and retaining the same even after revision is an indication that data privacy can be compromised for the data fiduciaries. The DPA can setup innovation sandboxes to encourage innovations in the field of artificial intelligence , machine learning and any other emerging technology under the aegis of public interest. Now inclusion in this sandbox means

[58] *Key Takeaways: The JPC Report and data privacy* Report (16 December 2021) https://internetfreedom.in/key-takeaways-the-jpc-report-and-the-data-protection-bill-2021-saveourprivacy-2/

[59] *Id* at 51

[60] *Id* at 56

exemption from regulatory compliances. This could range anywhere between 12 months to 36 months upon re-renewal. All or any of the obligations of the data fiduciary or rights of the data principals under **sections 4, 5,6 and 9 can be modified or taken away** like the mandate to process the data of data principals for clear, legitimate purpose in a fair and reasonable manner and only for those data that have been given consent to be processed. That is consent requirement is thrown into the air. Also data can now be retained for periods beyond for which it was actually collected.[61] Thus all aspects of privacy and the value given to it has been compromised through this provision.

Fourthly, this act does not specify how to deal with the data collected prior to 2019. The data which is collected with consent but which does not confirm to the regulatory provisions of the bill. EU's GDPR had in its **Recital 171** solved such ambiguities by giving a 2 year period to bring those data that was processed under the previous Data Protection directive under the GDPR mandates.[62]

Thus all in all the Data Protection Bill, 2021 fails to recognize a data principal's ownership rights over its personal data rather limiting it to an asset of national importance and thereby granting an alarming amount of power to the Central government which has not always been the most reliable agency due to changing governments, politics and policies. And hence from a common man's point of view it might be beneficial in the short run with long term backlashes in the form of corporate houses controlling governments and government's exercising surveillance over its citizens.

[61] *Id*

[62] *Id*