Page 6173 - 6185 **DOI:** *https://doij.org/10.10000/IJLMH.111228*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

The Privacy and Data Protection Conundrum in India Context and Concerns

AISHWARYA SIHAG[1]

ABSTRACT

The Supreme Court of India in 2017, in the case of Justice K. S. Puttaswamy vs Union of India, proclaimed privacy as a fundamental right and highlighted the need for a sturdy and robust legal structure in India with regard to data protection. Further in 2018, the European Union laid down certain limits on organizations concerning the processing and managing of personal data by means of the General Data Protection Regulation. Following several data breaches by various business organizations in India, Justice B.N. Srikrishna Committee was created in 2018 to fill this gap in Indian laws with respect to data protection. The committee submitted its report and proposed the Personal Data Protection Bill, 2018 to the Ministry of Electronics and Information Technology. Recently, a spin-off version of this bill called Personal Data Protection Bill, 2019 was passed by the Lok Sabha. However, this bill has been facing severe global criticism ever since its formation. This paper attempts to discuss the key features of the bill, its loopholes, its distinction from EU's General Data Protection Regulation and further suggests some changes that can be introduced in the bill to promote the right to privacy of an individual in its real sense. This paper also elaborates on the dangers of the blanket powers to access citizens' personal information conferred upon the Indian government by the bill.

I. INTRODUCTION

Personal Data Protection was first introduced in Lok Sabha on 11th December, 2019 by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad. Inspired by the GDPR, the PDP Bill was to bring about a comprehensive overhaul to India's current data protection regime, which is currently governed by the *Information Technology Act, 2000* and the rules thereunder.

The Bill gives out mandate for how personal data must be processed and preserved, and also lists rights of individuals regarding their personal information. It aims at creating a new

[1] Author is an Advocate at High Court of Delhi, India.

 [ISSN 2581-5369]

independent Indian regulatory authority, the Data Protection Authority to implement this law. The bill also sets out grounds for exemption.[2]

Applicability of the Bill

The Personal Data Protection Bill applies extra territorially to non-Indian organizations in the event certain nexus requirements are met, and also imposes hefty financial penalties in case of non-compliance.

This will not be limited to just e-commerce, social media and IT companies, but also include brick and mortar shops, real estate companies, hospitals and pharmaceutical companies. However, there will be some exceptions like small entities which includes small retailers businesses that collect information manually and meet other conditions to be specified by the Data Protection Authority.

A lot of global commercial and telecommunications companies are already subject to privacy and confidentiality prerequisites set out by their sectoral regulators, so they already follow some policies and procedures needed by the bill. But for all other businesses, these rules would be new and they would have comply with them.

II. WHAT IS IN THE BILL?

After the bill is implemented, businesses will have to disclose their data storage policies to users and request the consent of consumers. Evidence of the notice and consent of the users will have to be gathered and stored. Under the bill, consumers also have the right to the right to withdraw their consent. Additionally, they have the right to obtain access to, evaluate and erase their data. Corporations will have to put in place ways to authorize consumers to do so.

The consumers are also allowed to transfer their data along with any inferences made by corporations based on such data, to other businesses. All businesses will have to come up with ways to make this happen for consumers.

The bill demands the corporations to start by making organizational modifications to preserve and protect data in a more advanced way. These will comprise of the approach of privacy by design principles where the primary consideration in organizing business will be privacy and security safeguards.

The bill also specifies that all sensitive data of the consumers has to be stored in India and that

[2] Anirudh Burman and Suyash Rai, What is in India's sweeping personal data protection bill?, Carnegie India, (March 9, 2020), https://carnegieindia.org/2020/03/09/what-is-in-india-s-sweeping-personal-data-protection-bill-pub-80985

 [ISSN 2581-5369]

crucial private data should not be transmitted out of India. The trade driven decisions of corporations to access the best data storage facilities will be manipulated as a result, and corporations will be forced to keep such data locally in India.

Extra duties of auditing data and appointing data protection officers would be allotted to a cluster of prominent data fiduciaries.

Finally, the bill also incorporates rules about data that is not personal. As per the bill, the authorities can demand any business to share valuable non-personal data such as total transportability particulars collected by applications like Google maps and Uber. The bill does not give any guidelines on the compensation of corporations for their loss. This has chances of unfavourable long term reverberation on innovation and financial advancement.

III. HOW DID THE BILL COME ABOUT?

Multiple policies and legal tools have been proposed in India that prescribe those certain types of data must be stored in servers. This comprises of the draft Personal Data Protection Bill, 2019 notifications by the Reserve Bank of India, draft E-Pharmacy Regulations along with the report on monitoring of non-personal data.[3]

The origin of the bill lies in the landmark case issued on August 24, 2017. In that ruling, the Supreme Court declared privacy 'a fundamental right' under the Constitution of India. On September 26, 2018, the Supreme Court asked the government to set strong data protection rules.

Concurrently, the Supreme Court was looking at evidence in ***K. S. Puttaswamy (Retd) v Union of India[4] case***, in which case the Aadhaar Card Scheme was disputed on the ground that collecting and compiling the demographic and biometric data of the residents of the country to be used for various purposes is in breach of the fundamental right to privacy personified in Article 21 of the Constitution of India.[5]

The government of India formed a committee of experts in 2017 on data protection to scrutinize the issues relating to data privacy, chaired by a retired Supreme Court judge, B. N. Srikrishna. The committee put forward a report one year later and a draft bill. The present bill in parliament is an amended report of the draft bill.

[3] Trilegal, Data protection and privacy 2021, Chambers and Partners (March 9, 2021), https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2021/india/trends-and-developments

[4] KS Puttaswamy v. Union of India, (2017) 10 SCC 1

[5] Economics Law Practices, Data Protection and privacy issues in India, (September 1, 2017), /elplaw.in

IV. DISTINCTION BETWEEN THE NEW BILL AND THE OLD BILL

The most important differences between the new bill and old draft bill are the exemptions that the government agencies receive, the exemption for small business organisations gather data manually, the penalization of some activities, and the handling of non-personal data.

To start with, Indian government gets much more liberty for exemption under the new bill. The old bill permitted exemption to use personal data in the interests of 'national security' but only in the case if it was approved by the parliament and considered essential and proportionate. Under the new bill, government is permitted to exempt its agencies from the law on considerably broadly defined grounds.

Secondly, both versions of the bill permit exemptions for small businesses that gather individuals' personal information manually. Such businesses which qualified under the old bill was based on three following conditions: annual turnover, whether they shared personal information and the amount of personal data they processed. But now under the new bill, the new Data Protection Authority determines which small businesses qualify for exemption.

Thirdly, under the old bill, several actions were enumerated as criminal offences. These comprised inducing harm by obtaining, transferring or selling personal data; and re-ascertaining and processing anonymous personal data without permission. Under the new bill, only the latter is a criminal offense even though other violations could also be punishable.

Fourthly, the old bill did not include nonpersonal data. The new bill permits the Indian government to acquire and use nonpersonal data, in order to efficiently deliver services or to generate evidence based guidelines and policies.

The last major distinction applies to where personal information is stored. The old bill only demanded a copy of all personal data to be stored in India whereas the new bill requires storing all sensitive personal data in India. Such data may be transferred out of India if required for health or other emergency services, or if the government chooses to permit it.[6]

V. SALIENT COMPONENTS OF THE PERSONAL DATA PROTECTION BILL, 2019

Duties of Data Fiduciary

Under the bill, the processing of personal data will be contingent on specific motive, collection and retention constraints such as the following:

[6] Shreya Nandi, Exemptions for government agencies in data bill can be disastrous, (December 16, 2019), https://www.livemint.com/news/india/exemptions-for-govt-agencies-in-data-bill-can-be-disastrous-justice-srikrishna-11576456701898.html

a. Personal information shall be stored only for the purpose for which it is processed and shall be removed at the end of the processing.

b. For a definite, coherent and legal motive.

c. Notice is required to be given to the individual for gathering or processing of personal data.

d. Collection of personal data shall be restricted to such data that is essential for the objective of processing.

e. Data Fiduciary must confirm the age of the individual and obtain sanction from parents for processing sensitive personal data of children.

f. Permission is needed to be taken from the data principal at the outset of the data processing.

Additionally, the data fiduciaries must engage in specific ingenuousness and liability measures like-

(i) compose privacy policy, (ii) take required action to preserve transparency in dealing with personal data (iii) enforcing safety provisions such as warding off misuse of data (iv) notify the officials of breach of any personal data (v) examine its policies and regulation of policies every year (vi) manage data impact evaluation where noteworthy data fiduciary undertakes management of data that includes new technologies or sensitive personal data (vi) data fiduciary shall appoint a data protection officer for the purpose of guiding and supervising the activities of the data fiduciary, and (vii) establish grievance redressal process to deal with complaints of individuals.[7]

Processing of Personal Data without consent

The Bill proposes processing of data by fiduciaries only if consent is provided by the individual. There are certain exceptions provided under which Personal Data can be processed without consent such as: (i) if required by the State for providing benefits to the individual, (ii) legal proceedings, (iii) to respond to a medical emergency, (iv) employment related, (v) necessary for reasonable purposes such as prevention of fraud, mergers and acquisitions, recovery of debt etc.

[7] Personal Data Protection Bill, 2019, Section 3(13)

 [ISSN 2581-5369]

The powers of a 'Data Principal' [8]

The Bill mentions particular rights of the data principal which includes the right to: (i) acquire verification from the fiduciary on whether their personal data has been processed, (ii) obtain rectification of incorrect, insufficient or revise personal data, and (iii) right to be forgotten- control persistent disclosure of their personal data by a fiduciary if it is no longer required or in case permission is retracted.[9]

Data Protection Authority

The Bill suggests a Data Protection Authority that shall take measures to safeguard the concerns of individuals, ward off exploitation of personal data, check compliance with the Bill along with promoting knowledge about data protection. An appeal of the orders of the Authority can made to an Appellate Tribunal. Appeals against the order of the Tribunal can be registered at the Supreme Court of India.[10]

Prohibitions on Transfer of data outside India

Sensitive personal data may be transferred abroad for processing if expressed consent is given by the individual and subject to other specific conditions. Nonetheless, such sensitive data should resume to be stored in India. Certain personal data considered as crucial personal data by the authorities can exclusively be processed in India.

Exemptions

The central government of India has the right to exempt any agency of the Government from applicability of the Act if it deems necessary for the sake of sovereignty and integrity of India, the safety of the State and amicable relations with foreign states; and preventing instigation of commission of any cognisable offence related to the above mentioned matters.

The Bill also excludes processing of personal data for certain other objective such as- (i) prevention, inspection or prosecution of any breach or felony, or (ii) personal, domestic, or (iii) journalistic purposes, (iv) for research archiving or statistical objective.

Perils of non-compliance with the bill

There are two levels of penalties and renumeration:

[8] Personal Data Protection Bill, 2019, Section 3(14), Section 3(7)

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

[10] Prasanna Mohanty, Personal data protection bill 2019: unrestrained power to central government may undermine privacy, (December 17, 2019), https://www.businesstoday.in/current/policy/personal-data-protection-bill-2019-central-government-power-may-undermine-privacy-of-citizens-people/story/392186.html

 [ISSN 2581-5369]

- Negligence of the data fiduciary to fulfil its responsibilities for data protection may be penalised with a penalty which may extend to INR 5 crores or 2 percent of its total global revenue of the preceding financial year, whichever is more.
- Managing data in violation of the provisions of the bill is penalised with a fine of INR 15 crores or 4 percent of the annual income of the data fiduciary, whichever is more.[11]

The act of Re-identification and processing of de-identified personal data without consent is penalized with imprisonment of up to three years, or fine, or both.[12]

VI. WHAT ARE THE DIFFERENCES BETWEEN INDIA'S NEW BILL AND THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION?

There are some notable differences between the two.

To begin with, under the bill, the central government gets the power to exclude any government organization from the bill's requirements. This exemption can be given on justification of state security, state sovereignty and public order.

While the General Data Protection Regulation(GDPR) offers EU members identical escape clauses, they are strongly supervised by other EU directives. Under the Personal Data Protection bill, central government of India gets power to access individual data over and above existing Indian laws such as the Information Technology Act of 2000, which dealt with cybercrime and e-commerce.

Secondly, Personal Data Protection bill permits the government to order firms to share any non-personal data they collect with the government. GDPR does not contain this sort of provision.

The bill claims this is crucial for the advancement of the delivery of government services. But it does not give any explanation on how this data will be utilized, whether it will be shared with private businesses or whether any renumeration will be given for the use of this data.

Thirdly, businesses are not supposed to keep EU data within the EU territory under the GDPR. They can transfer it overseas as long as they abide by the customary contractual clauses on data protection, codes of conduct or certification systems that are approved before the transfer.

[11] Talukdar, *supra* note 8

[12] Ministry of law and justice, Personal data protection bill, Bills and Acts, https://prsindia.org/billtrack/the-personal-data-protection-bill-2019

Under the Personal Data Protection bill, personal data can only be transferred outside India if it meets conditions that are similar to those of the GDPR. It is pertinent to note that such data cannot be 'stored' outside India and can only be transferred outside India to be 'processed.' This is likely to create technical complications in identifying between groups of data that have to meet this prerequisite and it will further magnify compliance expenses of businesses.[13]

VII. IMPLICATIONS FOR INDIA AND THE WORLD

The global commerce community has expressed criticism over some aspects of the proposed legislation ever since the bill was introduced. U.S.-India Business Council President criticized the ostensibly privacy focused bill for reaching into other areas such as obligation of social media intermediaries which should be handled in separate legislation.

There are also massive business expenses linked with data localization compliance that a lot of foreign organizations would prefer to steer clear of. Undoubtedly, many companies incorporated within India and specifically those incorporated beyond, will continue to push back against other existing data localization prerequisites which increase storage and processing costs. The amended data localization clause in the new bill talks about these costs as the directive is limited to sensitive personal data and critical personal data.

Apart from these concerns, some observers in the business collective may worry about the data localization rules since these rules can result to valid cybersecurity and national security concerns. For instance if we talk about the case of Russia, more aggressive data localization rules have led to discord between the Russian government and Western technology organizations. This has happened in the first place because the Russian government has coerced foreign organizations to store their encryption keys within the country's borders, as part of a broader tightening supervision of Russian cyberspace. This problem has resulted into concerns about unchecked government access to sensitive information. Foreign organizations may have similar concerns around local data storage in India's case.

At G-20 summit, the U.S. has openly opposed data localization and policies which have been used as a tool to restrict digital trade flows and breach privacy and intellectual property safeguards.

The U.S. basically looks at the protection of online data and information as less the government's responsibility than for example, many counterparts in the European Union.

[13] Ikigai law, Comparative analysis: general data protection, 2016 regulation and personal data protection bill, 2018, (September 21, 2019), https://www.ikigailaw.com/comparative-analysis-general-data-protection-regulation-2016-and-the-personal-data-protection-bill-2018/#acceptLicense

 [ISSN 2581-5369]

China has referred to the GDPR as a prototype for building out some elements of its emerging data governance policy. India's proposed bill represents yet another country attempting to base its data governance policy on the GDPR's privacy guidelines. India's bill reflects the GDPR's further entrenchment as the global standard on which to base early-stage data protection regulations.[14]

VIII. WHETHER THE PERSONAL DATA PROTECTION BILL, 2019 UNDERMINES THE RIGHT TO PRIVACY?

Following years of contemplation and numerous modifications, Personal Data Protection Bill is finally likely to be proposed in Parliament.

Specialists have pointed out to Clause 35 of the Personal Data Protection Bill, which authorizes the government of India to give a blanket exemption to law imposition and exempts other organizations from necessitating the consent of data owners.

Increasing expenses accruing from requirements of data localisation and ambiguous policies for critical personal data are also a reason for concern.

Experts have indicated concern on how the current version of the bill seems to have sidestepped from what was initially conceptualised by the Srikrishna Committee which was given the approval by the authorities to draft the legislation back in 2017.

The Srikrishna Committee had demanded the bill to be equally applicable to both private players and government organizations, but clause 35 of the bill authorizes the central government to exempt any government agency from the application of the act, in the interest of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states and public order.[15]

That clause continues to be the biggest point of dispute for those eagerly observing all developments in reference to the bill.

Blanket Exemption for Government Is Unconstitutional

Blanket exemptions and lack of executive or judicial safeguards will fail to meet the standards laid out by the Supreme Court in the *KS Puttaswamy v. Union of India*[16] *case*. The court had

[14] Arindrajit Basu and Justin Sherman, Key Global Takeaways From India's Revised Personal Data Protection Bill, (January 23, 2020), https://www.lawfareblog.com/key-global-takeaways-indias-revised-personal-data-protection-bill
[15] Personal Data Protection Bill, 2019, Clause 35
[16] KS Puttaswamy v. Union of India, (2017) 10 SCC 1

ruled that measures prohibiting the 'right to privacy' must be strongly supported by law, fulfil a legitimate purpose, be proportionate to the purpose of the law and have procedural protection against misuse. Some major concerns which need to be addressed are ambiguous grounds that prompt exemptions, the lack of procedure in permitting exemptions and lack of autonomous supervision.

Clauses 35 and 36 increases the surveillance technology of the government and provides it the authority to retrieve personal data without limitations. Unfettered access to personal data, without safeguards, is potentially unconstitutional. The exemptions granted in Clause 35 entirely undo the objective of this bill. It places power in the hands of the central government and specifically makes it a party, judge and adjudicator of its own cause. There are no checks and balances. Clause 35 stands to nullify the enjoyment of personal privacy and other digital liberties.[17] Latest media statements suggested that the joint parliamentary committee headed by member of the Lok Sabha, Ms. Meenakshi Lekhi, has in its final report suggested as many as eighty nine amendments and one new clause be adjoined to the current bill.

Clause 42 of the bill discusses about the selection committee that will determine the structure of the Data Protection Authority. [18]As per the bill, this selection committee will have three members, all secretary level officers from the central government. This needs to be rectified and some members from the judiciary ought to be involved in the committee as well.

An additional disharmonious point at issue in the bill is how it tri-furcates personal data. The umbrella group is all personal data which can be used to identify an individual. Some types of personal data are considered sensitive personal data (SPD) which the bill defines as financial, health, sexual orientation, biometric, genetic, transgender status, caste, religious belief, and more. Another subset is critical personal data, which hasn't been defined in the bill.

The sub-classification of data in three categories could make life complicated for multinational businesses which have been operational in India for years. These companies would already have massive amount of data from their Indian customers. To further ask them to separate all data into these categories and put constraints on offshore processing, could certainly increase their regulatory woes. Industry voices have expressed the need to prevent the internet in India from becoming 'splinternet'.[19]

[17] Mohanty, *supra* note 9

[18] Clause 42, Personal Data Protection Bill, 2019

[19] Harshit Rakheja, From blanket exemption to rising cost of compliance: the personal data protection bill conundrum, (February 11, 2021), https://inc42.com/buzz/from-blanket-exemptions-to-rising-cost-of-compliance-the-personal-data-protection-bill-conundrum/

 [ISSN 2581-5369]

IX. THE WAY FORWARD

The highest number of cases filed in the Supreme court or High courts for infringement of the fundamental rights of citizens is against the state. Only recently citizens have approached the courts to enforce their privacy rights against big technological companies, e-commerce platforms and retail marketing businesses. Therefore, it is quite possible that even in situation of the proposed new data law, citizens would approach the courts against the states for enforcement of their fundamental rights of informational privacy.

Following the introduction of the proposed bill, a large part of the judicial function which involves the regulation of informational privacy of citizens, is suggested to be transferred to a Data Protection Authority. In the Puttaswamy case, the honourable Supreme Court ordered the government to pass a law which would manage informational privacy not only from non-state actors but also from the state parties and other individuals.

Preserving a balance between informational privacy and the advancement of a robust digital economy is a truly challenging function, necessitating a qualified and neutral body at the helm. A core judicial task with the Data Protection Authority would be to penalise government authorities and infact suspend their operations in case they fail to preserve an individual's personal data.

In light of the crucial adjudicatory duty of the Data Protection Authority to regulate not only private parties but also the central government, there arises a requirement to set up a Data Protection Authority independent of the central government which can implement the Personal Data Protection Bill in an unprejudiced manner. It cannot appear to be under the direct command and control of the central government.

The present framework of the Bill provides a broad range of powers to the central government, in the sense it solely the responsibility of the central government to safeguard the informational privacy rights of citizens. For instance, the members of the Data Protection Authority are nominated by a committee which consists of officers of the central government instead of a judicial or bipartisan parliamentary body or panel. The structure of the bill effectively leads to central government regulating itself.

This framework will also adversely affect the federal structure of the Constitution. For instance, a grievance registered against a minister's Office for data infringement will be decided by a body appointed by the central government as to whether such an infringement took place or not and if held to be so, what would be the punishment or quantum of fine of their penalty.

Likewise, the bill authorizes the central government to decide if an event or incident arising in a

 [ISSN 2581-5369]

remote location in a state comes under public order or not and hence, necessitating exemptions from application of the various protection conditions. This cannot be permitted as it creates fertile grounds for data hegemony by the Centre and is a huge concern for federalism.

Similar central overhang can be witnessed by Clauses 15, 33, 35, 44, 86 and 91 of the proposed Bill. Such powers should vest solely with an independent Data Protection Authority which must be the primary rule making body under the Bill.

The Data Protection Authority must therefore be established not as a regulatory body appointed by the central government but as a quasi-judicial independent body with judicial representation and should be subjected to only judicial oversight and monitoring and not executive management as envisioned in the current Bill.

Additionally, there is an overarching need for a decentralised Data Protection Authority composition with state bodies and bodies at the district level such as the Consumer Protection regime and the Right to Information regime. Meagre copying and pasting the regime paradigms of the Competition Commission of India or the Telecom Regulatory Authority of India or even the Income Tax and Central Excise will not suffice. As a matter of fact, provided the overarching and overwhelming role of the Data Protection Authority as an umbrella regulator over the sectoral regulators, there is a serious need to make it not only independent and competent, but also efficient and effective.

The need of the hour is that the government pays heed to these suggestions on a serious note. India can only unlock its true digital potential as a data commerce market with an independent Data Protection Authority, and not by a regime that is irreparably detrimental to our constitutional values and rights of the citizens to informational privacy.[20]

X. CONCLUSION

India is an major player in the global internet policy space. Indian government leadership is keen to place itself as a global leader on democratic data regulation and has largely succeeded.

The introduction of a data protection bill in furtherance of a constitutionally guaranteed right to privacy is a very small step toward occupying a leadership position on democratic data governance. Nonetheless, the text of the bill mainly appears to be a rudimentary amalgamation of terms in the GDPR with an autocratic penchant. Under the bill, these cover the framework

[20] Amar Patnaik, Uphold right to privacy: Personal data protection bill in current form, grants extraordinary powers to the government, (February 16, 2021), https://timesofindia.indiatimes.com/blogs/toi-edit-page/uphold-right-to-privacy-personal-data-protection-bill-in-current-form-grants-extraordinary-powers-to-the-centre/

 [ISSN 2581-5369]

for government surveillance which indubitably establishes government power to threaten citizen privacy. In addition, the obfuscating of the differentiation between non-personal data and personal data continues to remain concerning. The bill eventually diminishes safeguards on individual data rights by authorizing the government to access anything it feels would deem fit within the formulated categories of exemptions.

India's capability to guide emerging trade economies and smaller democratic states is ultimately subverted by these authoritarian leanings. The bill brands India as a more than less appealing model for the nations looking to draft a new vision of data governance that amalgamates the right to privacy with other vital civil liberties. Though some privacy-safeguards in the bill impersonate various provisions of the GDPR, the legislation needs considerable amendments if India aims to be a pioneer in forging a democratic, privacy protecting approach to the internet.

India's strategic interest lies in making sure that it endorses its constitutional responsibility to its natives and gives more weightage to citizen rights and economic welfare over meagre business interests. Specifically, because of concerning exemptions in the text of the Personal Data Protection Bill, 2019, it is not explicit whether this objective is fulfilled. As the Joint Parliamentary Committee starts its deliberations on the draft of the bill, it remains to be seen whether the policymaking pendulum swings the right way.[21]

*****

[21] Basu and Sherman, *supra* note 13

 [ISSN 2581-5369]