VOLUME 29 | MARCH, 2022 ISSN 2456-9704

ANALYSIS OF SOME MAJOR ISSUES OF THE PERSONAL DATA PROTECTION BILL, 2019

By Nikita Lamba
From Manipal University Jaipur

Introduction

The State of Mobile 2021 report by App Annie, a mobile analytics firm, shows that Indians spent more than 650 million hours using mobile applications in 2020. During that time, consumer spending through apps hit $500 million (Rs 3,652 crore)[1], which results in sharing of their personal data with all those applications.

India has not yet authorized explicit enactment on data protection. There are no particular conventions to get assent for handling individual data have been expressed. The "option to be failed to remember" isn't perceived as such in India, and there are no arrangements of law that accommodate this. As on date, India isn't perceived by EU as a country with sufficient degree of information assurance, hence, from an Indian viewpoint, it gets basic for such Indian substances to actualize the information security necessities specified in the EU Regulation inside their frameworks. Forbes India reports that "there are worries that the Bill gives the public authority cover forces to get to residents' information."[2] As the arrangements are generally dissipated, there are different holes in the current lawful structure. Additionally, their pertinence is confined to electronically produced and sent personal sensitive data. Moreover a portion of the arrangements can even be abrogated by an agreement.

The existing Information Technology Rules (2011), which govern many aspects of data protection, but which remain terribly unenforced. It is not even clear what the existing mechanism for enforcement should be. However, given the growing swiftness of the digital economy, the Act has limitations with respect to how personal and sensitive data is defined, and provisions that can be easily superseded by companies using a contract. "Further, the IT Act applies only to companies, not to the government."[3] The Cyber Appellate Tribunal, set up as a forum to rectify cyber fraud, had not adjudicated a single case in five years, according to a report in December 2016.[4] Notwithstanding, the Indian assembly revised the IT Act (2000), which give a privilege to pay for ill-advised exposure of individual information only.

The Supreme Court expressed that "right of people to solely economically misuse their character and individual data, to control the data that is accessible about them on the web and to spread certain individual data for restricted purposes alone" radiates from this right.[5] The judgment also declared informational privacy to be a subset of the right to privacy, along with holding that

[1] ForbesIndia. (n.d.). *Data protection bill: Can it ensure your privacy online?* Forbes India. From https://www.forbesindia.com/article/take-one-big-story-of-the-day/data-protection-bill-can-it-ensure-your-privacy-online/65815/1

[2] Ibid

[3] Ibid

[4] *What India's Data Protection Committee can learn from US, EU and China*. The Wire. (n.d.). from https://thewire.in/tech/what-indias-data-protection-committee-can-learn-from-us-eu-and-china

[5] Justice K.S Puttaswami and another Vs. Association of India (2017) 10 SCC 1

privacy is a fundamental right. The court also setup a committee, the Justice BN Srikrishna committee which submitted its report on data protection containing a draft of "The Personal Data Protection Bill 2018".[6] The bill was delayed in the Indian Parliament by the Ministry of Electronics and Information Technology on 11th December 2019. As of March, 2020 the Bill is being scrutinized by a Joint Parliamentary Committee (JPC) in discussion with specialists and partners.

The concept of personal data as in the PDP Bill is also likely to raise significant legal uncertainty. According to Clause 3 (28), this concept covers data about or relating to a 'natural person', who can be recognized either directly or indirectly. The problem here is that identifiability may only result from supplementary information or data available to and from the data fiduciary. This, as such, prevents anonymisation.

The position on data localization and cross border sharing of data is yet to be finalized, that could be a policy decision which will impact most businesses operating in India. However, in the backdrop of the PDP Bill, we anticipate to continue to see industry-specific data policies and regulations by sectoral regulators such as drone-related policies which may give rise to new issues including cyber security and obligatory disclosure to the Government.[7]

Objectives of the Research

In the depiction of privacy as an end rather than a means to protect other vital societal ends that are specific to India's political economy, the bill significantly strengthens the state without adequately protecting privacy. The aim of this research is to identify key issues relating to the Personal Data Protection Bill which may give rise to new issues.

The objectives are:-

- Whether the bill resolves the issue of privacy.
- Whether the bill's reliance on strengthening consent-based mechanisms for protecting personal data would be effective.
- Whether the bill could lead to significant compliance expenses for private businesses.
- Whether the vast supervisory powers of DPA are helpful.
- Whether the exemption of government agencies helpful.

Several local and international groups have voiced their opposition to the proposed legislation. They have raised concerns about aspects like the inclusion of non-personal data, classifying social media as publishers, and the Data Protection Bill's structure. According to Economic Times, a recent research commissioned by the European Data

[6] *India's journey to personal data protection and Data Privacy Law*. IBM. (n.d.)., from https://www.ibm.com/cloud/blog/indias-journey-to-personal-data-protection-and-data-privacy-law

[7] *The Personal Data Protection bill, 2019*. PRS Legislative Research, from https://prsindia.org/billtrack/the-personal-data-protection-bill-2019#:~:text=The%20Personal%20Data%20Protection%20Bill%2C%202019%20was%20introduced%20in%20Lok,Protection%20Authority%20for%20the%20same.

Protection Board (EDPB) has identified India's data regulations as a source of worry, notably the exemptions requested by the government under Section 35 of the Data Protection Bill. The information technology industry has also petitioned the government, claiming that lawmakers' extensive exemptions will harm India's $190 billion IT-BPM industry in the European Union. Meta Platforms (previously known as Face book) expressed concern about India's planned privacy legislation, which seeks local storage and in-house processing of data, in a filing with the Securities and Exchange Commission (SEC) earlier this month. In previous SEC filings, Google indicated similar concerns about regulatory impediments.

Currently, the bill has three main flaws that could result in severe regulatory ambiguity. To begin with, it lacks a clear definition of vital personal data. Second, it has no criterion for permitting cross-border data transfers. Third, it allows the government authority to compel the release of non-personal data, with no restrictions on how it can be used or specifics on how compensation will be paid.[8]

Whether the bill resolves the issue of privacy

The bill fails to adequately address privacy-related issues in India's data economy. Instead, the bill provides a preventative framework that over-regulates government intervention while strengthening the state. This might result in a large increase in compliance costs for businesses across the economy, as well as a concerning dilution of privacy in the eyes of the government. While privacy protection is a crucial goal, it also serves as a method of achieving other goals, such as freedom of speech and sexual autonomy. A framework for preserving personal data must be based on a better understanding of the function of privacy in society and the harms that result from individual privacy violations.

The majority of it focuses on privacy in the context of the harms that can be created by a breach of privacy. In 2017, the Supreme Court of India ruled in Justice K.S. Puttaswamy v. Union of India[9] that the Indian Constitution contains a basic right to privacy. The court's conclusion focused on the lack of a "doctrinal formulation" that might be used to determine whether privacy is guaranteed under the Constitution. The verdict proclaimed informational privacy to be a subset of the right to privacy, in addition to holding that privacy is a basic right. The bill aims to safeguard individuals' informational privacy by establishing a preventive framework that governs how corporations gather and use personal data by focusing mostly on controlling data-related practices, rather than protecting informational privacy in light of the harms that a breach of such privacy may bring. This is problematic not just because the proposed framework is unlikely to sufficiently guarantee privacy, but also because the law dramatically extends the state's engagement in the data economy, dilutes data property rights, and boosts state surveillance authority without necessary checks and balances. This is likely to have negative repercussions for economic

[8] MoneyControl. (n.d.). *Personal Data Protection bill will further strengthen privacy: Union it minister*. Moneycontrol, from https://www.moneycontrol.com/news/business/personal-data-protection-bill-will-further-strengthen-privacy-union-it-minister-7753981.html

[9] Justice K.S Puttaswami and another Vs. Association of India (2017) 10 SCC 1

innovation while leaving the claimed goal of safeguarding informational privacy unmet.

The bill is based on this new definition of privacy, and it fails to develop a well-designed regulatory framework that appropriately addresses market failures in the digital economy as a result.

Whether the bill's reliance on strengthening consent-based mechanisms for protecting personal data would be effective

Its reliance on consent-based systems for personal data protection is unlikely to be effective. Increased disclosure obligations to users about the use of their data are becoming inadequate in light of modern technological changes, according to a huge corpus of academic work. Reliance on such systems could be counterproductive, leading to people providing their data with less responsibility. The measure mandates notice and consent for data collection, as well as other substantial data processing duties. These, considered combined, may not effectively protect privacy because they are based on data regulatory concepts developed before the current market system existed. These also do not protect users from the consequences of a breach of privacy. Instead, these responsibilities may exacerbate moral hazard and cause consumers to overestimate the benefits of privacy legislation.

The bill lacks any empirical knowledge of the trade-offs people make when sharing their data. More research was supposed to be done in order to determine the exact scenarios in which users are prepared to give personal data for benefits. Evidence from other jurisdictions suggests that such trade-offs vary depending on the transaction's context. To the degree that the law preserves privacy without demonstrating its relevance to consumers, it may stifle the benefits of data-driven innovation while failing to adequately secure personal data.[10]

Whether the bill could lead to significant compliance expenses for private businesses

The bill's proposed preventive framework could result in considerable compliance expenses for private enterprises. The bill regulates the use of data in all areas of the economy and imposes significant new compliance obligations on the vast majority of firms involved. Except for those who are specifically exempt, the expenses of compliance will be shared by both small and large firms. Because the majority of firms in India are tiny, this is a concern. They would be particularly burdened by such regulations. The government can also require businesses to provide non-personal data with it under this bill. This could have long-term negative effects for innovation and economic growth.

The bill proposes imposing high compliance costs on data processing companies. While small firms are free from certain requirements, some exemptions will only apply to businesses that process data manually. As a result, a wide range of economic actors would be forced to bear enormous expenditures in order to implement the measure. The clauses forcing enterprises to pass over non-personal data to the

[10] Nitin Dhavate, R. M. (2022, January 5). *A look at proposed changes to India's (personal) data protection bill*. A look at proposed changes to India's (Personal) Data Protection Bill. from https://iapp.org/news/a/a-look-at-proposed-changes-to-indias-personal-data-protection-bill/

government are very burdensome and amount to a major infringement of property rights which can lead towards long-term detrimental consequences for innovation and economic growth.[11]

The term "harms" is not properly defined. Many of these actions are part of the decision-making process in many businesses. The bill's concept of harm might have a considerable impact on company regulation while providing no privacy protection.

Whether the vast supervisory powers of DPA are helpful

Another key flaw in the bill is the Data Protection Authority's planned structure. This entity will be in charge of enforcing the bill's provisions, including systems for obtaining consent, data use constraints, and cross-border data transfers. The DPA's supervisory mission is broad, considering that it is responsible for enforcing a wide range of preventive measures, such as security protections and transparency standards on firms. In the larger context of India's relatively inadequate regulatory capacity, this broad mission is being proposed. As a result, it is likely that the DPA will be unable to adequately execute the bill or defend informational privacy. Because of its multi-sectoral mandate, the DPA may find it difficult to develop internal competence, resulting in either under regulation or overregulation. The former would undermine the bill's intent, while the latter would impose unneeded costs on conforming enterprises. There are structural flaws in the DPA's design. The bill's comprehensive preventive structure will put severe capacity limits on it. The authority's planned structure does not allow for independent input or monitoring. The authority, for example, would lose its ability to govern the right to access, the right to be forgotten, and other rights. It would also lack the authority to decide how commitments like purpose limitations should be applied. In its regulatory-making powers, the DPA may not be obligated to follow sufficient consultative processes. Furthermore, the law lacks sufficient checks and balances to ensure that the central government and the DPA use their considerable supervisory powers responsibly.[12]

Whether the exemption of government agencies helpful

The bill empowers the government to exempt any of its agencies from the legislation's provisions, as well as determine what safeguards would apply to their data use. This might provide national security services with a new source of power to conduct surveillance—and, ironically, could erode rather than protect privacy. The government's abilities to exempt government entities from the law for surveillance purposes represent a new and autonomous ability to gather personal data. The law does not include enough checks and balances for the use of these powers, and it is unclear why this provision is necessary.[13]

---

[11] *Personal Data Protection bill - ministry of electronics ...* (n.d.). from https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

[12] *Fresh legislation may replace Data Protection bill*. The Economic Times. (n.d.). from https://economictimes.indiatimes.com/tech/technology/fresh-legislation-may-replace-data-protection-bill/articleshow/89624369.cms

[13] *Data bill waivers sought by Govt Worry Indian it firms*. The Economic Times. (n.d.). from https://economictimes.indiatimes.com/tech/information-tech/data-bill-waivers-sought-by-

Suggestions

In relation to Consent and Privacy

Without consent, data should not be collected and used. Businesses that breach this concept would also be violating Indian constitutional informational privacy laws as well as individuals' property rights. Simultaneously, consenting adults must be permitted to bear responsibility for their decisions. In other consumer-oriented industries, regulation frequently entails deciding if particular contractual conditions and practices are unfair, dishonest, or misleading to customers. The bill's focus should shift away from enforcing preventive measures and toward identifying and regulating such practices, as well as data sharing agreement provisions.

The bill does not provide appropriate protection against specific injuries or harms to users. Individuals and society should be protected from harm caused by breaches of data privacy, such as discrimination on constitutionally protected grounds, identity manipulation, financial theft, fraud, and challenges to sovereignty and national integrity. This emphasis on injury prevention must also be applied to the harms clauses. Data fiduciaries should be held liable if they cause the types of injuries listed above. They should not, however, be forced to take precautions against all potential data misuse. Market failures should be specifically addressed by regulation. A change away from obligations like privacy by design and the hiring of data protection officers would be required to reorient to a narrowly focused approach.

In relation to Preventive Measures

The remaining preventative regulatory duties should be layered based on a cost-benefit analysis. Firms who do not process data intensely or handle sensitive personal data should have their obligations lowered in proportion to the risks posed by their activity. One such reduction might be the removal of the need that firms handle data manually in order to qualify for the exemptions. Uncertainty in the regulatory environment must be reduced. To promote business certainty, ambiguities in the bill must be reduced.

In relation to Exemption by Government

The government's ability to exempt any federal agency from the law's provisions should be balanced by reasonable safeguards outlined in the bill itself.

In relation to management of powers of DPA

The DPA's mandate should take into account India's state capacity restrictions. Because of the nature of the data economy, effective data processing regulation will be nearly impossible. Removing the ambiguities would give the DPA more clarity on how to carry out key aspects of the bill. Finally, lowering the exemption threshold would dramatically limit the number of organizations subject to the DPA's authority, allowing it to concentrate on data-intensive industries. The DPA and the government should make decisions in a highly participatory manner. Because the bill's provisions have cross-sectoral applicability, this is far more

govt-worry-indian-it-firms/articleshow/89167985.cms

significant in this case than it is for other regulators.

As a result, the law should be amended to require the government and the DPA to conduct a rigorous consultative process when drafting any rules, regulations, or codes of practice. The Financial Industry Legislative Reforms Commission (2013) suggested and had codified in law a detailed consultative process for financial sector regulators. This required the board or the regulator's apex decision making authority to start the regulation-making process by first posting a draught of the proposed regulation, together with a note explaining why it was being suggested and a cost-benefit analysis. It was also proposed that before framing the final regulation, all financial sector regulators solicit public views on the draught and publish a broad response to them.

Before enacting laws, the Telecom Regulatory Authority of India, the Airports Economic Regulatory Authority, and the Insolvency and Bankruptcy Board of India, among others, go through extensive consultation processes. The bill mandates that the DPA engage in a collaborative process. This provision, however, only applies to the creation of codes of practice and entrusts the government with determining the details of the consultative process. The thoroughness with which Indian regulators interact and the exact features of such consultative systems entrenched in the appropriate statute is inextricably linked. As a result, the bill should be changed to ensure that the DPA follows best practices for drafting regulations and codes of practice.

Finally, because the DPA's operation has a significant impact on the market, it should be composed in such a way that it can take advantage of independent inputs in an institutional manner. The DPA should be made up of both full-time and part-time, self-employed members. Independent members should not be involved in the agency's day-to-day operations. This would provide for independent input as well as a framework for the agency's external oversight.

Conclusion

The research might help in enforcement agencies to work efficiently, effectively and narrowly focused and designed toward protecting individuals and society against any injury resulting from data processing. The outcome of the research will help the enforcement agencies to work properly and protect personal data effectively.

In the data sharing and data processing sectors, there are fundamental limits to the problems that regulation can fix. This is especially true in India, where regulators' capacity across industries is relatively limited. As a result, data protection legislation must be laser-focused and designed to safeguard individuals and society from harm caused by data processing. A framework created with this goal in mind would result in a better balance of privacy and creativity.

These concerns point to the need for a more pragmatic and modest approach to data protection and the risks of personal data misuse. The proposed structure is preventive, all-encompassing, and heavily regulated because the bill respects privacy as a goal. As a result, the state's ability to regulate organizations that collect data is greatly strengthened, and the state has more levers with which to undertake surveillance. The efficacy of preserving privacy through this legislative framework has apparent constraints. Instead, the framework should

concentrate on problems that can be effectively handled by legislation in a focused and specific manner.

India has forged its own path toward data protection, inspired in part by the EU General Data Protection Regulation, with several unique provisions such as combining personal and non-personal data under one umbrella, data localization, hardware device coverage, social media platform management, and more. Though it still has certain flaws, when fully implemented, it will bring India's data protection rules up to pace with those of other countries. Companies should begin preparing for compliance with the various provisions as soon as possible.

This new design may provide for a more detailed and practical framework for protecting individuals' personal data while still allowing the Indian economy to profit from advances in personal data processing. The suggested legal framework for preserving citizens' privacy must be adjusted to the reality of the Indian economy and regulatory landscape. It's critical to have a practical approach to data security. The bill greatly enhances the state without effectively safeguarding privacy by treating privacy as an aim rather than a means to secure other essential societal ends that are unique to India's political economy. A pragmatic assessment of the costs and advantages of data protection for India is the only way to design a more precise and pragmatic regulatory framework.

The Data Protection Bill is a long-awaited and desperately needed piece of legislation that would replace India's current archaic, obsolete, and inadequate data protection policy. It would assist preserve individual privacy rights and promote fair and transparent data use for innovation and growth, unlocking the digital economy, as compared to present standards. It has the potential to generate jobs, raise user knowledge of their privacy, and hold data fiduciaries and processors accountable.

*****