SUPREMO AMICUS

VOLUME 24 ISSN 2456-9704

# A DETAILED LEGISLATIVE COMMENT EXPLORING THE BROAD CONTOURS AND NUANCES OF THE PERSONAL DATA PROTECTION BILL 2019

*By Abhilasha S G*
*From School of Law, Christ University, Bangalore*

## Abstract

In the wake of COVID 19 pandemic, India's digital growth has increased manifold. India's vision to become a progressive and developed country cannot afford to miss the opportunity created by digitisation. In pursuance of the same, India has drafted its long overdue Personal Data Protection Bill 2019. The objective of this article is to provide a thorough research on the broad contours and nuances of the Personal Data Protection Bill 2019. The article begins by creating a narrative for the requirements of such a Bill and also touches upon the recent jurisprudence by Indian judiciary on the regulation of personal data. The author seeks to provide a descriptive account of the key provisions of the Personal Data Protection Bill 2019 in its current form and provide constructive criticisms by examining each issue in detail. The article further explores the challenges associated with formulation and implementation of a data protection regime in a technologically dynamic world. In addition, the article analyses and compares the similarities and deviations of the Personal Data Protection Bill 2019 from General Data Protection Regulation which is considered a global standard benchmark for any sound personal data protection regulation. The author concludes with probable solutions to make the Personal Data Protection Bill 2019 more effective and argues that carefully drafted suitable amendments are the need of the hour. The author is hopeful of its potential benefits as it sets the foundation for a booming digital ecosystem in India.

Key words – data protection, privacy, General Data Protection Regulation, data protection authority

## Introduction

In the 21st century especially in the era of 5th industrial revolution, data is not just the new oil but much beyond that. With the advent of sophisticated technologies, the very definition of personal data has expanded. For instance, analysing meta-data such as a set of predictive or aggregated findings, or by combining previously discrete sets of data, Big Data has radically expanded the range of personally identifiable data.[1] Since technologies such as Big Data, the Internet of Things and Artificial Intelligence are here to stay and hold out the promise of welfare and innovation, India will have to develop a data protection law which can successfully address the issues relating to these technologies, so as to ensure a balance between innovation and privacy.[2] India does not have any exclusive legislation dealing with data protection and is governed by Information Technology Act 2000 at present. The IT Act, 2000 is grossly unequipped to

[1] Kate Crawford and Jason Schultz, *Big Data And Due Process: Towards A Framework To Redress Predictive Privacy Harms*, 55(1) Boston College Law Review 93 (2014).

[2] *White Paper of the Committee of Experts on a Data Protection Framework for India*, Ministry of Electronics and Information Technology, Government of India.

deal with the pace of booming digital ecosystem and more importantly it applies to companies only, leaving out the government.

The ubiquitous and dynamic nature of digitisation and technology is such that – '*Uber' the world's largest taxi company, owns no vehicles. 'Facebook' the world's most popular media owner, creates no content. 'Alibaba' the most valuable retailer, has no inventory and 'Airbnb' the world's largest accommodation provider, owns no real estate.*[3]

This underscores the requirement for a data protection regulatory bill especially in the backdrop of the landmark Judgement of the Apex Court on the right to privacy (*K.S. Puttaswamy vs. Union of India*[4]), WhatsApp's new privacy policy, digital governance measures like digital health mission, digital India campaign, among others. Digitisation has also got a boost like never before due to COVID 19 pandemic. In pursuance of this, India's long overdue bill regarding data protection has finally been drafted and it is currently referred to the joint parliamentary committee. This is the Personal Data Protection Bill, 2019 (hereinafter referred to as "Bill") which has its roots from the B N Srikrishna committee report whose objective was "to ensure the growth of the digital economy while keeping personal data of citizens secure and protected". The Bill is heavily influenced by the European Union's General Data Protection Regulation.

**Indian Judiciary on regulation of personal data**

The Kerala High Court in *Balu Gopalakrishnan v. State of Kerala*[5] passed an interim order on April 24, 2020 on the export of COVID-19 related data by the State Government of Kerala to a US-based entity, 'Sprinklr' for data analytics. The High Court held that certain measures were to be implemented by the State Government before granting Sprinklr access to the data such as anonymizing the data, obtaining specific consent from citizens, and ensuring the return of data once contractual obligations end.

The Odisha High Court in *Subhranshu Rout @ Gugul v. State of Odisha*[6] observed in its order on November 23, 2020 the importance of the right to be forgotten of an individual where the case involved objectionable content regarding a woman that was posted online. The court encouraged the victim to seek appropriate orders for the protection of her fundamental right to privacy even in the absence of an explicit right to be forgotten. The court went on to recognise such a right by law that would help in safeguarding woman's rights online, thus highlighting the importance of strong individual privacy rights.[7]

**Key highlights of the Bill**

The scope of this Bill applies not only to private companies but also to government and foreign companies thereby expanding its

[3] Tom Goodwin, *The Battle is for Customer Interface*, TechCrunch (3 March 2015).

[4] *K.S. Puttaswamy vs. Union of India*, (2017) 10 SCC 1.

[5] Balu Gopalakrishnan v. State of Kerala, Kerala High Court, WP (C) Temp. no. 84 (2020), April 24, 2020.

[6] Subhranshu Rout @ Gugul v. State of Odisha, SCC OnLine Ori 87.

[7] Nishith Desai Associates, Privacy and Data Protecction – India Wrap 2020, National Law Review, Vol.XI, No.15.

jurisdiction and regulations. The Bill primarily seeks to regulate personal data of individuals with respect to processing, storage and collection of such data.

The owner or generator of the personal data is known as the data principal. Rights of data generator include right to know what is being done with their personal data, erasure of personal data, correct or update it, right to data portability, right to be forgotten and restrict the disclosure of personal data upon withdrawing consent.

There also exists a data fiduciary who collects data about data principle. The obligations of a data fiduciary include processing of data only for lawful purpose while ensuring privacy is protected. They are also supposed to process data only to the extent needed for the purpose for which it is intended while having a transparent privacy by design policy that explains how security of data and privacy would be ensured.

Another entity is the data processor. These are parties who can use/process the personal data collected from a data principle, for the purpose of advertisements for instance. However, the Bill has numerous exceptions where data may be processed without consent by data principle such as in case of emergency health services, the performance of any state function, in compliance with order of court/tribunal, by an employer with respect to his employee (data principle), national security, exemption by any govt agency from any provisions of the bill and exemption of data processors outside India from the provisions of the bill.

The law will be enforced by a Data Protection Authority whose main functions include monitoring application of the Act, taking action for personal data breaches, conducting enquiries about data fiduciaries if it is suspected of infringing digital rights, issuing directions to fiduciaries to provide any relevant data (binding on them), prevent misuse of personal data and promote data protection awareness.

**Criticism of the Bill**

The employer can have access to employee's data without his/her consent as allowed according to the exemption mentioned. This exemption can impact employees right to form association or unionise as guaranteed under Art 19(1)(c) of the Constitution of India. Since government and private entities can both use publicly available data without consent, these entities could use the data for profiling individuals on political, religious grounds etc.

Moreover, the Bill asks individuals to voluntarily verify their identity on social media. This may cause anonymity to be compromised because dissidents, sexual assault victims etc often use anonymity as as an opportunity for expression.

The Data Protection Authority is not independent in spirit because it is bound by directions of central government. 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 having judicial representation and should be subjected to only judicial oversight and

monitoring and not executive supervision as envisaged in the current Bill.[8]

Also, exemption of any government agency from any provisions of the Bill may amount to surveillance without reasonable and strict guidelines for the same. The Bill in its current form is different from the draft suggested by B N Srikrishna committee report with respect to expanding the scope of exemptions for the government, and it additionally provided that the government may direct data fiduciaries to provide it with anonymised or non personal data for better targeting of services.[9] There are very minimal checks and balances in this regard. Since the exemptions are broad, it may create the danger of diluting right to privacy while increasing scope for government surveillance.

Justice Srikrishna has expressed his concern stating that the 2019 Bill can turn India into an "Orwellian State with big brother snooping on us".[10] MEITY has constituted an expert committee under the chairmanship of Kris Gopalkrishnan to study various issues relating to non-personal data and to deliberate over a data governance framework for the regulation of such data. Thus, the provision relating to non-personal data must be deleted and the scope of the bill should be limited to protection of personal data only.[11]

Lastly, access to justice is limited because no court is empowered to take cognizance of any offence under the Act, save on a complaint made by the Data Protection Authority. Thus, the data principal has no locus to approach any court in case of infringement of any of his/her rights envisaged under the Bill.[12]

**Challenges associated with data protection regime**

After the introduction of the Bill, the major challenge will be to translate legal tenets into technological implementation using existing technologies.[13] The functioning of the Data Protection Authority must be dynamic to keep pace with technological changes and the Act itself must be flexible enough to accommodate emerging challenges posed by cyberspace.

Data localisation requirements under certain provisions may not ensure security of personal data because even if the data is stored in the country, the encryption keys may still be out of reach for the national agencies.[14]

If personal data are stored on blockchain-based databases, such uses would be subject to the requirements of the bill. For example, the bill would require a central node or person to be accountable for the operation of the blockchain as a data fiduciary.

[8] Amar Patnaik, *View: Personal Data Protection Bill, in current form, grants extraordinary powers to the Centre*, The Economic Times, Feb 17, 2021.
[9] Anurag Vaishnav, *The Personal Data Protection Bill, 2019*, PRS Legislative Research, Dec. 23, 2019.
[10] Shreya, *India's Data Protection Bill, 2019 – The beginning of an Orwellian Era*, University of Pennsylvania Carey Law School, Feb 10, 2020.
[11] Amber Sinha, Elonnai Hickok, Pallavi Bedi, Shweta Mohandas, Tanaya Rajwade, *Comments on the Personal Data Protecction Bill 2019*, The Centre for Internet & Society, Feb 12, 2020.
[12] Kunika, *A Critical Appraisal of the Data Protection Bill*, The citizen is Hopeful, October 25, 2020.
[13] Ram Govind Singh, Sushmita Raju, *A Technical Look At the Indian Personal Data Protection Bill*, May 28, 2020.
[14] Karishma Mehrotra, *Explained: The issues, debate around the Data Protection Bill*, The Indian Express, Dec. 7, 2019.

However, certain kinds of blockchain designs, such as decentralized blockchains, have no central issuer or controller. The use of such systems could lead to difficulties in how accountability for data processing is assigned.[15]

It is essential that data protection rights which are often complex and technical to understand and enforce, must be able to benefit fully from representative actions by non-government bodies (NGOs) to enforce all aspects of the law, and to seek remedies for data principals. Enabling such NGO actions is a key principle of the General Data Protection Regulation (Art. 80).[16] This expansion of locus-standi should be allowed under the current Bill.

Other concerns include increasing nature and sophistication of cybercrimes such as snooping by various agencies such as heckling of Indian citizen's WhatsApp accounts by Pegasus (Israeli software) and Facebook-Cambridge Analytica scandal where millions of users' personal data was used for political advertising without their consent. All these should be kept in mind before drafting a comprehensive and robust legislation.

**Deviation from General Data Protection Regulation**

The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The current Indian bill is largely modelled on this with some degree of variance.

Localization requirements represent a significant area of divergence between the Bill and GDPR. The Bill includes novel provisions that could require organizations to turn anonymized data over to the government. The Bill is significantly more stringent than the GDPR in that it assigns responsibility for defining "reasonable purposes" to the Data Protection Authority rather than to the controller/data fiduciary. The factors the Data Protection Authority must consider under the Bill are generally similar to those enumerated under guidance by EU regulators, but there is no requirement for the Data Protection Authority to enumerate any or all of the reasonable purposes set out in the Bill.

There is a wider definition of sensitive personal data under the Bill which means that a broader spectrum of activities will be affected by the conditions for data processing. There is significant overlap between the ways sensitive data is defined under each framework, but the definition of sensitive data is broader under the Bill. The Bill includes "financial data" within the scope of sensitive data. It also allows the government to define additional categories of sensitive data, whereas the list of categories under the GDPR is finite.

[15] Matthias Berberich and Malgorzata Steiner, *Blockchain Technology and the GDPR—How to Reconcile Privacy and Distributed Ledgers*, Eur. Data Prot. L. Rev. 2 (2016): 424.

[16] Graham Greenleaf AM, *India's Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards*, Professor of Law & Information Systems, University of New South Wales, Australia February 12, 2020.

The Bill reserves the right to access the locally stored data to protect national interests. This implies that the Bill would treat citizens' data as a national asset. In this respect, the Bill differs from GDPR, which imposes no locational storage requirements or preferential access to data for protecting national interests.[17]

With respect to right to be forgotten, unlike the GDPR, the Bill places responsibility for determining the scope of application of the right to be forgotten on adjudicating officers appointed by the Data Protection Authority, rather than the controller. By requiring adjudicating officers to consider a number of contextual factors and to balance various interests, it is likely that the Bill's right to be forgotten will be interpreted more narrowly than the corresponding GDPR right.[18]

Further, the Bill has left out important rights like the right to object to processing of certain personal data and right to seek exemption from automated decision making, both of which are guaranteed under Articles 21 and 22 of GDPR.

**Conclusion**

While the Bill is definitely a step in the right direction, there must be more focus on implementation and enforcement, instead of over regulation. Sectoral regulations might also be a better alternative than an overarching authority since multiple players are involved in data dynamics making it difficult to uniformly apply data laws.

This data regulation framework has direct bearing on key issues such as e-commerce policy, national digital health initiatives, cross border data transfers and affects MNCs operating in India thereby having domestic and international ramifications.

The Bill reveals that the competing interest of the state and citizens are not balanced fairly as it has authoritarian leanings. The glaring loopholes need to be filled and concerns mentioned above need to be addressed as the Personal Data Protection Bill 2019 will be one of the pillars for supporting India's potential to create over US $1 trillion of economic value from the digital economy by 2025 as predicted by MEITY report.[19]

It is a known fact that increasing number of litigations can drastically come down if laws are carefully drafted without any ambiguity and uncertainty when a policy transitions into laws. In this regard, many of the provisions in the Bill are vague, broad and beyond the ambit of a rights centered data protection regime. It is suggested that they be suitably modified for better protection of individuals' rights.

Therefore, ultimately it is important to see the privacy of the citizens as the paramount end goal of any data protection legislation. Only a vision in this direction can

[17] Vijay Govindarajan, Anup Srivastava and Luminita Enache, *How India Plan to Protect Consumer Data*, Harvard Business Review, Dec. 18, 2019.

[18] Kurt Wimmer, Gabe Maldoff and Diana Lee, *Indian Personal Data Protection Bill 2019 vs. GDPR*, International Association of Privacy Professionals.

[19] *India's trillion-dollar digital opportunity*, Ministry of Electronics and Information Technology, Government of India.

resolve the competing interests of the government for governance and welfare, the private sector for its commercial interests using personal data and most predominantly, the ability of individuals to exercise their right to privacy.

*****