

ISSN 2582 - 211X

LEX RESEARCH HUB JOURNAL

ON LAW & MULTIDISCIPLINARY ISSUES

VOLUME I, ISSUE IV

JULY, 2020

Website - journal.lexresearchhub.com

Email - journal@lexresearchhub.com



DISCLAIMER

All Copyrights are reserved with the Authors. But, however, the Authors have granted to the Journal (Lex Research Hub Journal On Law And Multidisciplinary Issues), an irrevocable, non exclusive, royalty-free and transferable license to publish, reproduce, store, transmit, display and distribute it in the Journal or books or in any form and all other media, retrieval systems and other formats now or hereafter known.

No part of this publication may be reproduced, stored, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

The Editorial Team of **Lex Research Hub Journal On Law And Multidisciplinary Issues** holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not necessarily reflect the views of the Editorial Team of Lex Research Hub Journal On Law And Multidisciplinary Issues.

[© Lex Research Hub Journal On Law And Multidisciplinary Issues. Any unauthorized use, circulation or reproduction shall attract suitable action under applicable law.]

EDITORIAL BOARD

Editor-in-Chief

Mr. Shaikh Taj Mohammed

Ex- Judicial Officer (West Bengal), Honorary Director, MABIJS

Senior Editors

Dr. Jadav Kumer Pal

Deputy Chief Executive, Indian Statistical Institute

Dr. Partha Pratim Mitra

Associate Professor, VIPS. Delhi

Dr. Pijush Sarkar

Advocate, Calcutta High Court

Associate Editors

Dr. Amitra Sudan Chakraborty

Assistant Professor, Glocal Law School

Dr. Sadhna Gupta (WBES)

Assistant professor of Law, Hooghly Mohsin Govt. College

Mr. Koushik Bagchi

Assistant Professor of law, NUSRL, Ranch

Assistant Editors

Mr. Rupam Lal Howlader

Assistant Professor in Law, Dr. Ambedkar Government Law College

Mr. Lalit Kumar Roy

Assistant Professor, Department of Law, University of Gour Banga

Md. Aammar Zaki

Advocate, Calcutta High Court

ABOUT US

Lex Research Hub Journal On Law And Multidisciplinary Issues (ISSN 2582 – 211X) is an Online Journal is quarterly, Peer Review, Academic Journal, published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essays in the field of Law and Multidisciplinary issues.

Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. **Lex Research Hub Journal On Law And Multidisciplinary Issues (ISSN 2582 – 211X)** welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

CRITICAL ANALYSIS OF THE PERSONAL DATA PROTECTION BILL 2019

Authors –

Akash Krishnan

Student (B.B.A. LLB)

ICFAI Law School, Hyderabad

Kushagra Gahoi

Student (B.B.A. LLB)

ICFAI Law School, Hyderabad

ABSTRACT

“Privacy is not something that I’m entitled to, it’s an absolute pre-requisite”

- Marlon Brando

Since the inception of documentation, data privacy has been of utmost concern. Authorities would mark a set of data as confidential which could be limitedly used for authorised purpose which in present times is known as ‘personal data’. But why do some set of characteristics of our lives become so evidently important as to its unauthorised access makes others culprit? Well, the statement answers for itself. Some attributes of our lives define our existence. Any act by any person that jeopardizes that attribute actually puts our own existence in jeopardy. Now, when our lifelines are ‘online’, we do everything digitally. Making government documents, paying bills, shopping, connecting, surfing, learning, all these activities may expose our personal data, fiscal facets and privacy rights prone to predators and exposing it to high risk of hacking and fraud. This problem magnifies when the data is saved in a remote server on an anonymous computer source as it not only becomes difficult to identify the source of fraud, but to search for methods to eliminate it. Problematically, the existing IT Act lacks the capability to deal with the evolving needs of the current situation. The government after focussing on dynamism and gravity of the issue introduced the Personal Data Protection Bill, 2019 which emphasizes the need for consent and remedies ignorance.

Keywords: Data Privacy, Data Protection, Right to Privacy.

INTRODUCTION

In May 2018, the European Union effectuated the General Data Protection Regulation, to meet the various requirements of protection and privacy of data across the Union. Thereafter, India started taking initiatives to formulate a data protection regime on the lines of the GDPR. A Committee of

Experts on Data Protection Framework was appointed by the Indian Government, which submitted a report in July 2018.

In December 2019, the Personal Data Protection Bill was introduced before the Indian Parliament. The main object of this proposed legislation is to protect the private data of individuals and to formulate institutions for the same purpose. While this bill does finally address the need for legislation centring data protection in India, it has also been heavily criticised for not addressing the same in a manner which was necessary.

In this regard, mention may be made of the Personal Data Protection Bill, 2006. This Bill was loosely based on the European Union Data Privacy Directive of 1996, and aimed at providing a comprehensive framework for collecting, processing as well as distributing personal data. Thereafter, in 2011, the Government of India came up with the Privacy Bill which was an improvised version of the previous proposition and tried to address the crucial aspects of collection, processing, storage and disclosure of personal data.

The 2019 Bill was built upon these precursors. In 2017, the Right to Privacy was declared to be a fundamental right under Article 21. The report which was submitted by the Committee of Experts didn't provide a detailed analysis of the financial impacts of adopting such a data protection regime. Therefore, it is absolutely necessary for the Government to consider the impact that the adoption of the Data Protection Bill will have on the economy of the country.

However, the various vital aspects that have been covered by this Bill are those of obligations of the data fiduciaries, rights of individuals and data principals, aspect of data processing without consent, the transference of data outside India and the Data Protection Authority.

LAW ENFORCEMENT:

In a country like India where we are going through a digital revolution and the number of people with accessibility to the internet is increasing day by day, the phenomenon of cyber-bullying, trolling and online crimes are also on the rise. The inadvertent rise in the online form of harassment through commenting, trolling publishing videos and photo of a person without their consent,

posting fake information about someone which may or may not incite hate against a person is becoming a hassle to deal with. The culprit usually hides behind a screen and mostly the cyber-bullying goes unreported. There is no specific law dealing with Cyber-bullying but rather certain laws can be extended to this crime as well are as follows:

THE INFORMATION TECHNOLOGY ACT – There exist no specific provisions pertaining to cyberbullying but various provisions can be used in this regard: -

Section 66A – Sending offensive messages through communication service, etc.

Sec.66C – Identity Theft

Sec.66D – Cheating by personation by using the computer resource

Sec.66E – Violation of privacy

Sec.67B – Punishment for publishing or transmitting of material depicting children in any sexually explicit act, etc. in electronic form

Sec.72 – Breach of confidentiality and privacy

INDIAN PENAL CODE - also has a certain section which may be extended to cyberbullying

Sec.503 – Sending threatening messages through email (covered under criminal intimidation)

Sec.509 – Word, gesture or act intended to insult the modesty of a woman

Sec.499 – Sending defamatory messages through email (as covered under defamation)

Sec .500 – Email Abuse (as covered under defamation)

The extension of this IPC section to the digital arena shows how courts are recognizing the vices in the digital media and how it is equally powerful for perpetrators to commit a crime.

AWARENESS:

Various awareness campaigns are organized by the Cyber cell authorities to the aware public at large. Some of the important questions are discussed by UNICEF to aware people about Cyber-Bullying and Cybercrimes.¹

- **Are you being bullied online?**

There is always difference between joking and bullying.

UNICEF: All friends joke around with each other, but sometimes it's hard to tell if someone is just having fun or trying to hurt you, especially online. Sometimes they'll laugh it off with a "just kidding," or "don't take it so seriously." But if you feel hurt or think others are laughing at you instead of with you, then the joke has gone too far. If it continues even after you've asked the person to stop and you are still feeling upset about it, then this could be bullying. And when the bullying takes place online, it can result in unwanted attention from a wide range of people including strangers. If you are not happy about it, you should not have to stand for it.

Call it what you will – if you feel bad and it doesn't stop, then it's worth getting help. Stopping cyberbullying is not just about calling out bullies, it's also about recognizing that everyone deserves respect – online and in real life.

- **What are the effects of cyberbullying?**

UNICEF: When bullying happens online it can feel as if you're being attacked everywhere, even inside your own home. It can seem like there's no escape. The effects can last a long time and affect a person in many ways:

- Mentally — feeling upset, embarrassed, stupid, even angry
- Emotionally — feeling ashamed or losing interest in the things you love
- Physically — tired (loss of sleep), or experiencing symptoms like stomach aches and headaches.

¹ The Information Technology Act, 2000. ACT NO. 21 OF 2000 [June 9, 2000].

- **Why is reporting important?**

UNICEF: If you think you're being bullied, the first step is to seek help from someone you trust such as your parents, a close family member, or another trusted adult. In your school, you can reach out to a counsellor, the sports coach, or your favourite teacher. If you are in immediate danger, then you should contact the police or emergency services in your country.

Anyone can become the victim of Cyber-Bullying. For bullying to stop, it needs to be identified and reporting is the key.

UNICEF: Think twice before posting or sharing anything online – it may stay online forever and could be used to harm you later. Don't give out personal details such as your address, telephone number, or the name of your school.

There are various tools which are available on social media handles for community support:

- Mute -removing an account's Tweets from your timeline without unfollowing or blocking that account.
- Block - restricting specific accounts from contacting you, seeing your Tweets, and following you.
- Report - filing a report about abusive behaviour.

OVERVIEW OF THE BILL

The Personal Data Protection Bill as introduced in Lok Sabha, protecting the privacy of an individual and ensuring the free flow of the economy is applicable on personal data processed within the territory of India, by the State², Indian Company, any citizen of India or body of persons incorporated under Indian Law. The bill is not restricted to the territorial boundaries of India and thus also makes it applicable to data processed by data fiduciaries³ or data processors⁴ not present

² Article 12 of Indian Constitution, 1949

³ Section 3(13) of PDP,2019

⁴ Section 3(15) of PDP,2019

within the territory of India if the data processing is in connection with a business/ activity carried out in India.

It also gives an exception processing of anonymized data but a special power has been given to the government which presents the government as omnipotent who can direct any data fiduciary to provide any personal anonymised or non- personal data.

Personal Data as defined under Section 3 of the bill⁵: **“personal data means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.”**

The bill provides a detailed chapter on the obligations of data fiduciary to ensure the protection of privacy of data principal. The data should only be processed in a lawful manner and with the full (free and clear) consent of the data principal explaining the purpose. And the data shall not be stored after the purpose is complete. The data principal also has the right to withdraw his consent. It is the duty of data fiduciary to ensure that the personal data is updated and if the personal data is being shared with other data fiduciaries, the data principal has a right to be notified about it.

The bill distinguishes between personal data and sensitive personal data of children and provides guidelines as to how to personal data of children should be treated with sensitization.

The data principal has been given some rights under the bill to collect the information regarding his data through data fiduciaries. He can confirm, whether his data has been processed or not by the data fiduciary and can ask for corrections, completion, updating and erasure his data.

Even though these rights are provided to the data principle, it is the duty of each and every data fiduciary to take relevant measures in order to protect the personal data of individual. In case any breach of data occurs during processing which can cause harm to the individual, that breach shall be reported to the authority by giving notice. Every data fiduciary shall have an effective mechanism to redress the grievances.

⁵ Sec 3 of PDP, 2019

There are some exemptions provided in the bill through which data can be transferred outside India. The Central government has been given powers under which it can exempt any agency of the government from the application of this bill when it is in the interest of sovereignty and integrity of India, the security of the state, friendly relations with the foreign states, public order and to prevent any incitement to the commission of any cognizable offences.

Chapter IX of the bill lays down that for the protection of personal data an authority can be established which is called as “Data Protection Authority of India”. Section 42 of the bill provides that authority shall consist of a chairperson and not more than six whole-time members, of which one shall be the person having qualification and experience in law. The chairperson and members of the authority are selected by the Central government on the recommendations made by the selection committee.

Bill also imposes penalties and asks data fiduciaries to pay compensation if they contravene certain provisions of the bill or fail to comply with the request of the data principal, the orders issued by the authority, or to furnish.

Chapter 11 of the bill talks about the establishment of the Appellate Tribunal which shall consist of a chairperson and the appointed members with at least 10 years' expertise in the field of data protection and information technology to hear and dispose of cases arising from various sections of the bill.

Clauses 78-79 talk about a fund dedicated to the bill called the Data Protection Authority Fund to which the Central Government may send funds and all the sums received by the Authority from any source as may be decided upon by the Central Government.

It further says that any person who, knowingly or intentionally re-identifies personal data which has been de-identified shall face imprisonment for a term not exceeding 3 years or with fine which may extend to 2 lakh rupees or both. Any act which is punishable under this bill shall be cognizable and non-bailable.

Section 91 of the Bill enables “the Central Government to require Data Processors or Data Fiduciaries to provide it with anonymized Personal Data, or other non-personal information (which

was expressly excluded from the scope of the Draft Bill) to enable the targeting or delivery of services, or the formulation of evidence-based policies. The provision does not provide for any form of compensation or remuneration for such data. It also reaffirms the right of the Central Government to formulate policies for the digital economy to the extent that such policies do not govern personal data. This is particularly relevant because of the proposed E-Commerce Policy”⁶.

THE NEED OF THE HOUR

There are countless examples where considering the present scenario the privacy of an individual can be put to risk which ultimately will be the violation of article 21 of the constitution. Which makes this bill the need of the hour. The recent one being Aarogya Setu App. After the COVID-19 pandemic, the government launched its own application- *Aarogya Setu [(setu)bridge to being(aarogya)disease-free]*. Functionally, the app is to track your every movement and update its functioning after every 15 minutes; in case you come in contact with any of the infected person or you as an infected person meet anyone, the app through Bluetooth technology will inform you and other users of the danger. The concern here is about personal data being available, processing and utilised without any acquired consent (the precautions are so taken somehow leave a lacuna thus endangering the data of ‘mandatory’ users). Enforcing the bill can now help the victims who if wish to sue the government for this breach can legally held them responsible.

AREAS COVERED UNDER THE BILL

Additional restrictions of data entities

The bill places additional responsibilities on data entities processing all the data. All the data fiduciaries are required to implement security safeguards such as data encryption and prevent misuse of data and they must set up a grievance mechanism to address complaints of individuals.

⁶ Department of Industrial Policy and Promotion, Draft National E-Commerce Policy, February 23, 2019.

It also covers the Institute mechanism for age verification and parental consent while processing personal data of children. Moreover, social media interferers with consumer above a certain limit and whose actions can affect public order should provide voluntary user verification mechanism for users in India.

Sensitive personal data and Critical personal data

Personal data protection bill has created various subcategories on personal data like sensitive personal data, critical personal data and personal data. The sensitive personal data further subcategories the data belonging to children and to adults because the children are much more vulnerable than adults, so by categorizing personal data into various categories the administrative impact and the privacy enforcement become easier.

HOW DOES THE BILL AFFECT OTHER AREAS OF LAW?

Data is like water, if not given direction it will overflow. Once this bill is enacted, it will replace Section 43 of the Information Technology Act, 2000 which talks about penalty and compensation for extracting an individual's personal data stored on the computer. It also replaces IT rules 2011 which is called "Reasonable security practices and sensitive personal data or information." The 2011 rules have been framed under Section 43A of Information Technology, 2000.

Other areas of Law-

1) Banking and Finance Law-

As Corona virus spreads and taking precious lives. People are cautious of going outside and using digital platforms for daily needs. As marketing through e-commerce websites increases, sensitive data of the public tends to get vulnerable and thus compromise. First, these companies promise their users that they give utmost priority to safeguard their data and at second they steal and sell user data in order to know the market position.

2) The Right to Privacy

On August 2017, the Supreme Court declared the Right to Privacy as a fundamental right which is incorporated in Article 21 of the Indian Constitution. After the introduction of this bill, eyebrows have been raised in the drafting committee. The chairperson of the drafting committee of the original bill of 2018, Justice B.N Srikrishna who conducted the study and submitted the draft criticized the revised bill and said that "The government wants to intrude into private data of its citizens citing sovereignty and public order." He further added that this law may violate the fundamentals of democracy i.e. "Right to Privacy."

FACTORS WHICH CAN FACILITATE THIS BILL TO BE A SUCCESS- RECOMMENDATIONS

Firstly, this bill will require affective regulation of the authority as prescribed indirectly. Secondly, the companies must have an Indian office as prescribed in IT intermediary rules as well as a grievance mechanism system that will also be required so that individuals are the collective users and have the grievance redressal.

In the Consumer Protection Act, there is provision for the class action suit so in that type of data violation, that provision should also be incorporated in the new bill so that collectively users can sue all the claim compensation against the corporate.

SURVEILLANCE FEARS

The government can collect data of users without much restraint and use this data in opaque ways. Besides, the Bill doesn't stick with the Supreme Court ruling on the proper to privacy within the Puttaswamy judgement⁷ which mandates government and authority to declare specific objectives for gathering or collecting personal data.

⁷ Justice K.S. Puttaswamy (Ret'd) v. Union of India and Ors, W.P(Civil) 494 OF 2012

A recent Pegasus-WhatsApp interception scandal is often taken as an example of this. Under the proposed bill, the government could empower a security agency, like the NSA, to undertake such an operation without contravening any laws.

INCLUSION OF NON-PERSONAL DATA

The Bill further doesn't offer any explanation for the inclusion of non-personal data. As per the new Bill, the government can ask any company to offer it anonymised personal or non-personal data for policy formation and better delivery of services. The provisions in non-personal data should be included and the government should not be treated as omnipotent.

NO JUDICIAL MEMBER WITHIN THE DPA COMMITTEE

The Data Protection Authority (DPA) team majorly comprises secretaries from the cupboard, Department of Legal Affairs and therefore the MeitY. This raises a serious concern about the DPA being independent of the government.

IMPACT ON COMPANIES

The Bill, if implemented in its current form, will have a three-fold impact on companies. It will mention a level of legal compliance which didn't exist earlier for the businesses. Thereby requiring companies whenever they gather data of users to put clear notices to users what data is being collected and what purpose it will put towards use. Businesses will need to revamp their data handling practices.

In reference to the utilisation of the info by the businesses, some companies are often exempted by the government.

CONCLUSION

The bill has looked into some important concepts such as consent, protection, and keeping of personal data, reasonable apprehension to such data, reasonable purpose, consent while processing personal data.

While it has paid attention to mix in itself some of the most important features of law concerning protection of privacy rights of data principle it has also relaxed some of the stringent laws found in the 2018 bill.

Remembering the developing need of the advanced economy, having an administrative sandbox set up might be the need of great importance, be that as it may, giving the administration unregulated and expansive forces to exclude government organizations from the arrangements of the 2019 Bill for specific conditions may nullify the point of the 2019 Bill and endanger a person's fundamental right to security.

The bill by providing for increased certainty may prove to be business-friendly, but a lot of other changes that have been mentioned above may prove to be a point of concern.

The PDP Bill is a breakthrough to deal with the requirements of an evolving data protection regime of India. However, several aspects of knowledge protection (such as categorization of private data as sensitive personal data and important personal data, details on anonymized data, conditions for exemption from certain provisions of the PDP Bill, categories of SDFs, conditions for registration as a consent manager and processing of private data and sensitive personal data of children), which can be key to an efficient and successful implementation of the new regime, are delegated to the DPA and/or the Central Government. With the inclusion of other aspects that will bridge the gap in the bill, the bill could be perceived as futuristic but the important impact of the PDP Bill is going to be visible once the relevant rules and regulations are in place.