|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 2|JUNE 2020|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2019): 2.32|
|IMPACT FACTOR (2018): 2.527|

|LAW AUDIENCE JOURNAL®|

|VOLUME 2 & ISSUE 2|JUNE 2020|

|ISSN (O): 2581-6705|

EDITED BY:

LAW AUDIENCE JOURNAL'S

EDITORIAL BOARD

|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 2|JUNE 2020|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2019): 2.32|
|IMPACT FACTOR (2018): 2.527|

Email: lawjournal@lawaudience.com, info@lawaudience.com,

Phone: +91-8351033361,

Website: www.lawaudience.com.

Facebook: www.facebook.com/lawaudience

Instagram: www.instagram.com/lawaudienceofficial

Contact Timings: 5:00 PM to 9:00 PM.

|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 2|JUNE 2020|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2019): 2.32|
|IMPACT FACTOR (2018): 2.527|

DISCLAIMER:

Law Audience Journal (ISSN (O): 2581-6705) and Its Editorial Board Members do not guarantee that the material published in it is 100 percent reliable. You can rely upon it at your own risk. But, however, the Journal and Its Editorial Board Members have taken the proper steps to provide the readers with relevant material. Proper footnotes & references have been given to avoid any copyright or plagiarism issue. Articles published in ***Volume 2 & Issue 2*** *are the original work of the authors.*

Views or Opinions or Suggestions ***(if any)****, expressed or published in the Journal are the personal point of views of the Author(s) or Contributor(s) and the Journal & Its Editorial Board Members are not liable for the same.*

While every effort has been made to avoid any mistake or omission, this publication is published online on the condition and understanding that the publisher shall not be liable in any manner to any person by reason of any mistake or omission in this publication or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this work.

All disputes subject to the exclusive jurisdiction of Courts, Tribunals and Forums at Himachal Pradesh only.

|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 2|JUNE 2020|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2019): 2.32|
|IMPACT FACTOR (2018): 2.527|

"POLE STAR ON A MOONLESS NIGHT OR JUST ANOTHER IOTA OF SAND IN THE DESERT? AN INTRICATE ANALYSIS ON THE PERSONAL DATA PROTECTION BILL, 2019."

AUTHORED BY: MR. SWARAJ GANGARAM KARIYA, CO-AUTHORED BY: MR. UJJWAL CHETAN SHETH, FACULTY OF LAW, THE MAHARAJA SAYAJIRAO UNIVERSITY OF BARODA,
EMAIL IDS: SWARAJK645@GMAIL.COM, SHETHUJJWAL28@GMAIL.COM,
PUBLISHED AT: WWW.LAWAUDIENCE.COM.

I. ABSTRACT:

"In times when data analysing companies in the garb of "political consultancies" can manage to manipulate entire elections, in times when every input on the internet leaves behind a digital footprint, in times when Right to Privacy online is just a myth and the real meaning has gone to the gutters; it is up to the governments of the States to be nonchalant and pretend to live in a cave or take concrete measures against it. The Government of India introduced the ***Personal Data Protection Bill, 2019*** *amidst the backdrop of incidents like data manipulation and it's selling in the general elections of the country by a British political consultancy* ***'Cambridge Analytica'*** *came to light.*

The bill governs the processing of data by the government, companies and other organisations. It is revolutionary in the sense that it includes provisions for rights of data principals, consent and even grievance redressal. The bill is the first-ever legislation introduced in India with regards to the data protection. The bill is also immaculate in the sense that it has apt classifications for different categories of data fiduciaries and also has categorised data in order of sensitivity. The airtight provisions and new tribunals for Data

Protection will serve as a deterring effect on data principals and will lead to a more careful way of handling and processing data. With penal provisions included in the form of offences and various punishments to them, the bill will ensure that selling and manipulation of data are prevented and the faith of the general public is restored in privacy."

II.INTRODUCTION:

Those were the days of yore when gold was the superlative of exchanges, the era of oil as a factor of power dynamics is slowly sailing past. The age of information technology has ushered this world into a new era where data is the most invaluable commodity. In an age where most of look from groceries to real estate on the internet it would be foolhardy to assume that our data is protected or even safe with the host websites, every click, every letter typed, every search initiated leaves a digital footprint in the cyberspace; the "footprint" hence leaves certain data traces which are then used to tailor our search results and any other digital activity with the use of various algorithms. With an increase in digitalisation, there have been raising issues of concerns over user privacy and data protection. In 2016, 57% of the users reported that they were more concerned about their online privacy than they were in 2014[1].

With the increasing inflow and circulation of data increasing need was felt for data protection laws, since without a ***Data Protection Act*** in place companies and various other organizations could easily mislead the consumer and collect data by using fraudulent methods, only sensitive data like hospital records, biometric information etc., were inaccessible and could only be processed with the permission of appropriate authorities and hence the ***Personal Data Protection Bill, 2019,*** was introduced in Lok Sabha by ***Minister of Electronics and Information Technology Mr Ravi Shankar Prasad*** on ***December 11, 2019***. The Data Protection Bill, India is at present considering a few bills that to embroil the security rights. For instance, in March 2018, the Indian Health Ministry proposed another law, the ***Digital Information Security in Healthcare Act,*** which would give information subjects

[1] Centre for Internet Governance Innovation – Ipsos, '2016 CIGI-Ipsos Global Survey on Internet Security and Trust', 2016.

"possession" of their computerized health information. The Bill was modelled around the ***EU's (European Union) General Data Protection Regulation (GDPR)*** which itself came into effect on ***May 25, 2018***, and replaced the minimum standards for processing data provided in ***Data Protection Directive of 1995***. The ***Data Protection Bill states that it will override the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,*** but does not enumerate any other existing laws that it supersedes or replaces. The ***Srikrishna Report*** accompanying the Personal Data Protection Bill lists fifty different laws, including the ***Aadhaar Act*** that may be impacted by the Data Protection Bill and recommends that the respective ministries amend these laws as necessary.[2]

Amending all of the laws identified in the Srikrishna Report is a tall order and will likely spawn litigation over whether existing legislation is inconsistent with the Data Protection Bill, the extent of any inconsistencies, and whether the ***Personal Data Protection Bill*** completely supersedes the existing legislation. For example, if businesses comply with the data residency requirements of the Personal Data Protection Bill by storing a copy of personal data in India, are they still required to comply with the Reserve Bank of India's data residency requirements by storing personal data related to payment processing only in India and not in any other countries. The Personal Data Protection Bill additionally permits organizations to process individual information for a reason sensibly coincidental to the reason for which the information was gathered. For instance, if individual information is gathered regarding a competitor's work application, it might likewise be allowable to process similar information to give business-related advantages to the in this way utilized subsequently. *"The law also permits the processing of personal data for a reasonable purpose. Some non-exhaustive examples of reasonable purposes are data processing for mergers and acquisitions transaction, for network security purposes, or for credit scoring."* ***The Personal Data Protection Bill*** also establishes the ***Data Protection Authority***, which is expected to clarify what these terms mean and what processing they permit.

[2] Sri Krishna Committee, The Quint (May 4, 2020 8:35 PM)https://www.thequint.com/news/india/key-highlights-from-srikrishna-committee-report-on-data-protection.

III. JUSTICE BN SRIKRISHNA COMMITTEE'S REPORT:

The committee submitted its report on Data Protection and highlighted the various issue about privacy, the government looked into it and made changes pursuant to it. Justice Srikrishna said data privacy is a burning issue and there are three parts to the triangle. "The citizen's rights have to be protected, the responsibilities of the States have to be defined but the data protection can't be at the cost of trade and industry. The report has proposed penalties for violations, criminal proceedings, setting up of a data authority, provision of withdrawal of consent and concept of consent fatigue.

Some of the suggestions worth highlighting in the report were[3]:

i. *Processing of personal data only for specific and lawful purposes*
ii. *Firms and agencies to appoint Data Protection Officers*
iii. *Provision of exemption for processing data for a personal, domestic or journalistic purpose*
iv. *Individuals will have the right to withdraw consent*
v. *'Critical' personal data to be only processed by servers located in India.*
vi. *2-4% of the worldwide turnover of the companies to be imposed as penalties or fines in the range of Rs. 5-15 crore whichever is higher.*

IV. THE CORNERSTONES OF THE PERSONAL DATA PROTECTION BILL, 2019:

The cornerstones of the Personal Data Protection Bill, 2019[4] which would prove to be the defining aspects of this Bill are:

IV.I Right to Privacy:

[3] Justice BN Srikrishna's report on 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians, The Hindu Centre (May 5, 2020 7:12 PM) https://www.thehinducentre.com/resources/article24561547.ece/binary/Data_Protection_Committee_Report-comp.

[4] Ministry of Electronics and Information Technology- The Personal Data Protection Bill, 2019 (May 5, 2020 7:20 PM) https://docs.google.com/viewer?url=https%3A%2F%2Fmeity.gov.in%2Fwritereaddata%2Ffiles%2FPersonal_Data_Protection_Bill%2C2018.pdf.

The Personal Data Protection Bill clearly states that it is necessary to protect personal data as an essential facet of informational privacy. Clause 4 of chapter 2 clearly states that any person processing personal data owes a duty to do so in a manner that respects the privacy of the individual. Clause 29 of the Bill gives a detailed insight into various aspects of privacy in the bill, according to clause 29(d) the Bill makes sure that any legitimate interests of the business are achieved without compromising the privacy interests of any individual. Clause 29(e) also protects the privacy is protected from the processing till the deletion of the data.

IV.II The Role and Importance of Consent:

The bill includes a wide array of sections which highlight the importance of consent of data principals i.e., the individuals or persons. Clause 12(1) clearly states that the data can only be processed after obtaining explicit consent from the data principal no later than the stage of commencement of data processing. Clause 12(2) also states that the consent thus obtained should be free, informed, specific and clear. A revolutionary step inserted in Clause 12(4) of the bill provides for the onus of the burden of proof of consent on the data fiduciary i.e., the individuals or corporations processing the data.

Under this bill the data has been classified into categories like Personal data and Sensitive Personal Data the later includes data like genetic data, biometric data, sexual orientation etc. and to protect these Clause 18 of the bill states that explicit consent needs to be obtained before processing of sensitive personal data in adherence to the rules stated earlier in Clause 12. To protect the data of children Clause 23 of the bill mandates obtaining parental consent before data fiduciaries can process any data of a child. Also, it is necessary under clause 41 of the bill that the explicit consent of the data principal needs to be obtained before exporting any sensitive personal data outside the country.

IV.III Data Audit:

The bill mandates a compulsory annual data audit by an independent data auditor under Clause 29 of the bill who shall evaluate the compliance of data fiduciary. The bill makes it compulsory for a data fiduciary to appoint a data auditor to conduct a Data Protection impact assessment which should contain the description of the data processed, assessment for

measuring potential harm and measures for managing and minimising or removing the risk of harm.

IV.IV Consent Manager:

A "consent manager" is a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform. A consent manager works as an agent of the data principal and he may give or withdraw his consent to the data fiduciary through a consent manager. Clause 23(4) of the Personal Data Protection Bill, 2019 states that where the data principal gives or withdraws consent to the data fiduciary through a consent manager, such consent or its withdrawal shall be deemed to have been communicated directly by the data principal.

IV.V Data Fiduciary and Significant Data Fiduciary:

Data fiduciary is any entity that processes the data of any individual and stores it in their database. Under Section 26, certain data fiduciaries can be deemed "significant data fiduciaries" based on factors such as the volume of data processed, the turnover of the fiduciary, the risk of harm, or the use of new technologies in the processing[5]. These entities will then have to comply with certain additional obligations such as preparing data protection impact assessments, appointing a data protection officer, and ensuring annual audits by an independent data auditor.

IV.VI Data Protection Officer:

Clause 30 of the Personal Data Protection Bill states that every significant data fiduciary (SDF) shall appoint Data Protection officer possessing relevant qualifications who would provide guidance and information to data fiduciary, monitor personal data processing of the fiduciary and ensure the compliance of data processing standards, provide advice on development of internal mechanisms for compliance and maintain an inventory of records to be maintained by the data fiduciary.

IV.VII Grievance redressal mechanism:

It is mandated by clause 32 of the Personal Data Protection Bill, 2019 that every data fiduciary must have a grievance redressal procedure and mechanism to redress the grievances

[5] Personal Data Protection Bill, 2019: Considering Consent and Offences, Rishab Bailey & Vrinda Bhandari, Medianama (May 6, 2020 7:40 PM) https://www.medianama.com/2020/01/223-pdp-bill-2019-consent-and-offences-views/.

of data principles in a speedy and effective manner. The data principal has to file a complaint to the data protection officer and the data fiduciary has a time limit of 30 days to resolve the complaint, failing which the data principal can complaint to the appropriate authority. Clause 41 of the bill mandates the setting up of a Data Protection Authority of India as a body corporate of further redressed of complaints, which would consist of a chairperson and not more than six whole time members.[6]

V. CONCLUSION:

The bill is a progressive legislation towards data protection, although pending approval before a joint parliamentary committee this bill is a revolutionary step considering the continuing lack of data protection infrastructure in India. Finally, non-personal data has found its way into the text of the revised bill. Sticking to the grand vision of ensuring that India's data is used for the development, the government included a provision clarifying its power to frame any policies that would benefit India's digital economy, so long as it did not concern personal data. It goes on to state that, in consultation with the Data Protection Authority (DPA), it can direct any data fiduciary to hand over personal data or other "non-personal data" with no clarity on what evidence-based policy-making might entail. In times when Data can influence elections, change governments and impact millions of people with a single click it is absolutely necessary that a country has an iron-clad legislation for data protection in place. The act serves as a deterrent to any lurking threats and protects the user from data theft. It is understandable that compliance and execution to such a legislation which in itself is rudimentary in nature is a mammoth task, but once Data Protection and security is achieved, it will open up a plethora of avenues for the development of the IT industry and will also serve as a boost to the economy.

[6] Data Privacy Bill 2019, Price Waterhouse Coopers (May 4, 2020 6:35 PM) (https://www.pwc.in/consulting/cyber-security/data-privacy/personal-data-protection-bill-2019-what-you-need-to-know.html).