LawPublicus
The Legal Portal

Volume 1 : Issue 8
2021

June, 2021

Email ID: Lawpublicusportal@gmail.com
Website: www.Lawpublicus.com
Address: A18 Dayanand Colony Lajpat Nagar - 4
New Delhi

Disclaimer

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of ***LawPublicus*** The Legal Portal. The Editorial Team of ***LawPublicus*** 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 reflect the views of the Editorial Team of ***LawPublicus***. Though all efforts are made to ensure the accuracy and correctness of the information published, ***LawPublicus*** shall not be responsible for any errors caused due to oversight or otherwise.

FOR *LawPublicus* The Legal Portal

Editorial Team

Editor(s)

Dr. Vijeta Verma
Assistant Professor – JEMTEC Greater Noida
Contact: +91-9911393623
Email ID: Vijetaverma.gn@jagannath.org

Dr. Prashant Kumar
Assistant Professor – IMRT, Lucknow
Contact: +91-9889109882
Email ID: Prshntkumar6@gmail.com

Dr. Shishma Kushwaha
Assistant Professor – JEMTEC Greater Noida
Contact: +91-9718485919
Email ID: Shishmakushwaha.gn@jagannath.org

Ms. Shivangi Sharma
Assistant Professor – CLS, Gitarattan International Business School
Contact: +91-9891496247
Email ID: Shivangi.sharma@gitarattanedu.in

Ms. Kriti Sharma
Assistant Professor – GGSIPU
Contact: +91-9891354307
Email ID: Kritisharmaks30@gmail.com

Ms. Yantakshikaa Sharma
Partner - LawPublicus LLP
Career Counsellor
Contact: +91-9711249637
Email ID: Yantakshika@gmail.com

About Us

LawPublicus The Legal Portal is a leading journal of multidisciplinary research. It is a free, peer-reviewed, open-access journal that provides insight into diverse and dynamic legal matters.

LawPublicus is a novel initiative by legal minds. As the its name suggests, it is platform for young minds to ignite their willingness and inventiveness in order to contribute to the field of law through new ideas, opinions and thereby contributing to an informed citizenry.

We hope to provide a forum for young and enthusiastic writers to voice their feelings and research on interdisciplinary approaches. We also have in view to evaluate, explore and deliberate, under the tutelage of seasoned editors and academic experts, on current trends and projections based thereon in legal studies. LawPublicus focuses not only on the scholarly writings but also on numerous other approaches such as discussions, interviews, and debates with experts and qualified & industrial professionals.

We are determined and excited to bring authentic, creative and individual ideas and socially-related problems into attention.

LawPublicus calls for research papers, articles, short notes, book reviews & case commentaries, that are distinctive and unpublished.

With this thought, we hereby present to you

LawPublicus The Legal Portal

Critical Analysis of the Personal Data Protection Bill, 2019

Authored By:

Ms. Dhairya Arora

Designation: 5th Year B.A. LL.B (H) Student

Institute: School of Law, KIIT University, Bhubaneswar

Co-Authored By:

Mr. Anirudh Jena

Designation: 5th Year B.A. LL.B (H) Student

Institute: School of Law, KIIT University, Bhubaneswar

Critical Analysis of the Personal Data Protection Bill, 2019

By: Dhairya and Anirudh

ABSTRACT

Today almost everything about your daily life is being monitored, such as locations you visit, pictures, any transaction you make, etc. is being tracked by corporations and this information is being sold to organizations by companies who monitor your data. All this is done without your permission, which is morally incorrect. In this rapid age of technology and the internet, data is the greatest asset for a person, but at the same time the most insecure asset. About every area of everyday life, not only limited to health care, banking, travel, etc., allows us to share our private information with another person or organization for the same to be processed in order to provide us with the relevant services. Some of the information is exchanged willingly and, in some situations, inadvertently where we are obliged to disclose the information to make use of the service needed. A blazing example of this will be access to data that is virtually forked out of us to use Smartphone devices. However, particularly in the case where information is exchanged voluntarily, we would not want the same thing to remain in the hands of someone else forever or, worse still, to be more shared and used for reasons other than that for which it was meant to be used at the time of compilation. Unfortunately, as this is the grim truth of the day and, for all practical purposes, we have no power over our personal information as soon as it exits our jurisdiction and one of the greatest casualties of this is the privacy of the citizen. With Internet penetration recording an all-time high of 58 percent, data has been a straightforward alternative to much of today's issues. The most substantial data protection regulation in the world, the General Data Protection Regulation (GDPR) took the European Union by storm when it entered into force on 25 May 2018. Despite having the second-largest Internet user in the world, there was a shortage of robust data security laws in India. The need for such a rule has been discussed by the Personal Data Privacy Bill 2019 (PDPB).

In order to put a stop to the problem, it was high time for democratic provisions across the spectrum to sit down, take care and establish a judicious mix between the power of a person over his or her data and the gathering of the same data so as not to obstruct the flow of services.

The proposed Personal Data Protection Bill was submitted by the Justice Sri Krishna Committee on 28 July 2018. The plan called for a lot of criticism of some provisions, such as the policy on the position of results. The bill was passed in Parliament on 11 December 2018. Subsequently, it was referred to the Joint Select Committee, which would present its recommendation at the meeting of the Parliament for the 2020 budget. This paper attempts to objectively examine the Indian Data Protection Bill and also seeks to include little information about the European General Data Protection Bill and how the Indian Data Protection Bill is particular and contentious.

KEYWORDS: Personal, Data, Protection, Regulation, Bill

INTRODUCTION

Data Security refers to a system of privacy rules, regulations, and procedures aimed at mitigating the infringement of the processing, storing, and distribution of personal data into one's privacy. Personal data usually refers to information or data belonging to a person that, whether obtained by any government or by any private entity or agency, may be defined by that information or data[1].

An urgent question has arisen in recent history: Are data public utilities or a private good, like oil? Like sunlight, data can be freely exchanged for the good of humanity and the well-being of its inhabitants. Think of the information on the Internet. Conversely, like gasoline, data has to be refined over time in order to have much use. According to a survey released by Statist, there are reportedly almost 700 million Internet users in India. This number is estimated to rise to more than 974 million users by 2025. In reality, India ranked the second largest online market in the world in 2019, second only to China[2].

In this digital age, people intentionally or unknowingly post confidential personal data on different digital channels such as e-commerce pages, Smartphone applications, webinar platforms, net banking, e-wallets, etc. Members of these sites shall allow the use of personal data by merely clicking on 'I adhere to the terms and conditions with or without reading the Privacy Policy. This vulnerability leaves millions of users exposed to hackers and multiple threat actors.

The intrinsic malleability of the data has contributed to greater concerns regarding control, enforcement, and sovereignty. So far, India has failed to deal with these problems. India's violated privacy statute is scarcely heard and rarely enforced.

Privacy in India is a nascent term, validated by the Supreme Court, which extended Article 21 of the Constitution and accepted it as a constitutional right in K.S. Puttaswamy (Retd.) & Anr. V. UOI[3]. The Supreme Court ruled that, like most other human rights, the right to privacy is

---

[1] The GDPR: What exactly is personal data? Luke Irwin , 12th Nov 2020<https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data>

[2] Number of internet users in India from 2015 to 2020 with a forecast until 2025 by Sandhya Keelery, Oct 16, 2020<https://www.statista.com/statistics/255146/number-of-internet-users-in-india/>

[3] (2017) 10 SCC 1

often subject to multiple checks and balances, including fair limitations. In other words, to ensure that constitutional rights remain inviolable and that they are not infringed, the settled judicial stance is that there should be a valid purpose of the state versus unconstitutional action, and the limitation of any intended rule must be "reasonable."

The PDP bill was introduced in 2019 to bring about a thorough reform of India's existing data security system, which is currently regulated by the Information Technology Rules 2011, Information Technology Act, 2000, and the laws thereunder. The latest draft of the PDP Bill lays out enforcement standards for all types of personal data, broadens the protections provided to persons, establishes a national data privacy authority, and institutes requirements for the localization of data for certain forms of sensitive data. The PDP bill extends extra-territorially to non-Indian entities if such nexus conditions are fulfilled and also introduces substantial financial sanctions in the event of non-compliance.

The PDP Bill was forwarded for recommendation to the Joint Parliamentary Committee (JPC) on 12th December 2019. The report of the JPC, following the timetable extensions given, is now due to be sent to the Parliament at the Budget Session to be held on an interim basis in January 2021.

The JPC has held a variety of meetings with government ministries, business bodies, and other stakeholders, as well as meetings based on the provisions of the PDP Bill. Importantly, as noted in recent news, the JPC is also preparing to extend the reach of the PDP Bill from only personal data to 'encompass overall data security and non-personal data. According to further reports, members of the JPC remain undecided and fragmented on these core issues of data translation and government access to data kept in particular by social media sites, among others, and some reports have reported that the PDP Bill will not be passed in its current iteration and that it will be "re-drawn" by the JPC.

The bill extends to all government and private enterprises involved in data functions. There is a provision for the appointment of Data Controllers who have general superintendent ship and authority over subjects covered by the bill. It also specifies that, in addition to restitution for costs to claimants, judicial penalties can be imposed on perpetrators.

Clearly, the bill is a step in the right direction. However, owing to the lack of details, the bill has been up in the air.

NEED FOR DATA PROTECTION IN INDIA

Data is the oil of today's modern era, in which each user, by internet interaction, leaves an impression of individual data supervised by others. Actually, similar to oil in the last century, information is currently the world's most valuable asset; rather it goes about as a main thrust for development and change. The assortment and storing of data have significant security ramifications, nationally as well as internationally. Hacking and stealing sensitive data is central to cyber espionage. The global data economy is dominated by a few tech titans such as Alphabet (Google's parent company), Amazon, Apple, Face book and Microsoft. These giants are vacuuming massive volumes of data that help to create a digital profile of each user, including personal interests, foibles, and secrets. Data collection can show as much about an individual as government oversight, if not more.

Today's data vendors are financially empowered to collect and monetize personal data from people around the world. However, the data collected were not exclusively used for commercial purposes. Nor is it left isolated in the business sector. Thanks to Edward Snowden and other disclosures, we know that the government of the United States is using a range of methods to collect data from internet giants. And by its National Security Service, it has full links to Google, Facebook, Apple, and other systems. America's vast archive has an Orwellian potential to map digital fingerprints and personal records of people, both Americans and abroad, including decision-makers. Indeed, the 2015 US Data Security Intelligence Sharing Act has effectively allowed all kinds of government and business espionage. This serves as a reminder that the internet, while a big benefit, is that we cannot exist without security facilities. It is paradoxical that those in India who have created a hullabaloo on how the digital identity of the Aadhaar scheme violates privacy and are silent on the wider and more important topic of the monopoly dominance of the most dominant technology firms on the data of all, including Indians. It is as if they claim that Aadhaar, aimed at converting parts of India's data economy into public networks to do away with subsidies and discourage false identities, is riskier than the vast data vaults of global tech giants.

The Governments' Personal Data Security Bill has been on the news in India, which aims to protect rights of Indians by reclaiming data from these multinational behemoths and mandating

storage locally. Not unexpectedly, the bill was attacked by the giants and the US administration.

THE PERSONAL DATA PROTECTION BILL

The Personal Data Protection Bill 2019 was introduced at the Parliament's Winter Session and was presented to the Joint Legislative Committee; the bill lays down some responsibilities and obligations for the collection of personal data and grants protections to people whose personal data is being handled. The Data Security Authority shall also be set up for this reason.

Following the decision of the Supreme Court in 2017, which declared privacy a constitutional right the government was forced to enact data security regulations. In India's use of personal data or citizens' information is currently governed by the IT rules of the year 2011 under the IT Act 2000. The act applies only to businesses but not to the government. 2019 Data security bill refers to all organizations handling personal data both by the Government and by businesses incorporated in India and also extends to international companies concerned with personal data of individuals in India to avoid abuse of data and to ensure overall conformity with the legislation creating a data protection authority. The bill describes personal data as any piece of information from which an individual may be identified. Individuals may request correction of incorrect, incomplete personal data entities and whether personal data have been processed to correct the incorrect or incomplete personal data and to pass their personal data to some other trustee under certain circumstances. Individuals can also restrict access to personal data if it is no longer necessary for the data agency to maintain that access.

This bill has numerous requirements and is not meant to fully regulate the sharing of data, but this bill does so by categorizing data into sensitive personal data and essential personal data and allows for the protection of critical personal data in the country so that people whose data it is may exercise greater control over whether they want to exchange data for a long time. There is no full ban on it, but there are certain limitations on it, which are again being extended to the security of privacy as the decision of the Hon. Supreme Court in the Justice ***K.S.Puttaswamy(Retd) vs Union Of India***[4] where privacy has been proclaimed a fundamental right and in Article 21 of the Constitution of India.

[4] (2017) 10 SCC 1

KEY HIGHLIGHTS FROM SRIKRISHNA COMMITTEE REPORT ON DATA PROTECTION:

The Justice BN Srikrishna Committee forwarded its report to IT Minister Ravi Shankar Prasad on data security. The report was submitted during a press event at the IT Ministry, along with a draft Data Security Bill, titled, "A Free and Fair Digital Economy-Protecting Privacy, Empowering Indians". The ten-member committee was tasked with researching and defining key problems relating to data security and recommending strategies for resolving them. Here are some of the highlights of the report and Bill:

- **Restrictions on the transmission and storage of personal information/data**

  The Committee advises that the processing (collection, documentation, review, dissemination, etc.) of personal data should be performed exclusively for 'simple, precise and legitimate' purposes. Just the data required for such collection shall be obtained from everyone.

- **Production of personal data for "State functions"**

  One of the most controversial recommendations of the Committee is that it indicates that your personal data may be collected by the Government if it is deemed appropriate for the work of the Parliament or the State Legislature. This requires the provision of utilities, licensing, etc. It appears incredibly ambiguous in the face and may lead to misuse.

- **Right to be Forgotten**

  The Committee proposes that 'the right to be lost' be granted 'data values' (persons whose personal data are being processed). This ensures that they will be able to limit or prohibit the showing of their personal data until the object of the disclosure of the data has been terminated or the data principal withdraws consent to the disclosure of their personal data. In the EU, individuals have been used to receiving unflattering records of them on news outlets pulled down after the matter is no longer a matter of public concern. This privilege is one of many privacy principles, including the right to confirm what information is being retained or released and, if necessary, to correct it. The Odisha High Court further established the relevance of this right in the case

of Subhranshu Rout @ Gugul v. State of Odisha[5] wherein the court established the importance of the right to be Forgotten and how it will especially benefit women's rights online. It further mentioned how this right is still unaddressed in our Indian legislation.

- **Data Localisation**

  Personal data will need to be maintained on servers located inside India, and transactions outside India will need to be secured. However, vital personal data can only be stored in India.

- **Critical personal data collection in order to seek express permission**

  The Committee advises until anyone gives their express permission — what factors in the intent of processing — "sensitive" data (such as passwords, financial data, sexual orientation, biometric data, religion, or caste) should not be processed. Therefore, you would not give your name and your attention to an advertisement agency if your sexual identity was mentioned in an interview where it had been told that it was used for determining the number of persons with such advice in a specific location, as it was separate from your accepted intent.

- **Data Protection Authority**

  The Committee proposed creating a Data Protection Authority to be responsible for protecting the rights of data administrators,' for avoiding abuse of personal data and for ensuring that businesses, governments, or those who process data (called 'data fiduciaries') meet the protections and responsibilities under the data security system. The data trustee's responsibilities entail audits and ensuring that they employ a data security officer and a complaints resolution process – all these issues would enable the Authority to publish realistic codes. The Authority shall be empowered to prosecute and take actions against the data fiduciaries responsible for any breach of the data privacy regime.

- **Aadhaar Act Amendments**

[5] BLAPL No. 4592 of 2020.

The Committee proposed to ensure the autonomy of the UIDAI and 'enhance data security' suggestions under the Aadhaar Act 2016. Their right to file charges stays with the UIdai only. This involves offline checking of Aadhaar numbers and new civil and criminal punishments.

- **Amendments in RTI Act**

  To make sensitive information freely accessible, the Committee proposed amending subsection 8(1) (j) of the RTI Act. The amendment must be amended by the committee. Ancient 8(1)(j) said that there would be no requirement to report personal information not associated or infringing on the topic of 'governmental action or concern.' New 8(1)(j) discusses a balance between, on the one hand, the public interest in accessing the information and, on the other, the damage caused to the data controller.

WHAT IS PERSONAL DATA?

The definition of 'personal data' as set out in the 2019 Bill has been considerably broadened to read as 'personal data' means data involving to a natural person who is directly or indirectly recognizable, having regard to any qualities, attributes, or other features of the identity of that natural person, whether online or offline or any combination of such features with any other in the Bill[6].

Under the 2018 bill, the definition stated that "data about, or linked to, a natural individual who has a direct or indirect identification in regards to any traits, characteristics, qualities or any other feature of or mixing those characteristics with any other data is erroneous[7].

The extension of the concept of personal data is without a doubt a welcome step in broadening the reach of the 2019 Bill, which in return strengthens the privacy protection of data directors. Besides, the term also includes any conclusion derived from personal information to make profiles, since the inference normally leads to a natural person's indirect identity. This is important because many companies use new technology to target online ads and to tailor their advertising by using their online behaviors and pattern. Even if the information obtained from

[6] Section 3 (28) of The Personal Data Protection Bill, 2019.
[7] Section 3 (29) of The Personal Data Protection Bill, 2018.

online activity cannot identify a person uniquely, it can also contribute to the identification of a person when jointly or in conjunction with other characteristics.

GROUNDS OF PROCESSING OF PERSONAL DATA

The 2018 Bill clarified that if such processing is required for the operation of the parliament or other national legislative body, personal data can be processed. The 2019 Act has repealed this clause and prohibited personal data collection for the delivery or advantage of any operation or gain to the data controller of the State or for the grant of any attestation, warrant, or authorization to the State's acts or practices concerning the duties of a State permitted by statute, without permission of the data controller[8]. The 2018 Bill clarified that, without the permission of the Authority, personal details may be collected for any legitimate purposes. The Authority may define the appropriate objectives that include the prevention and identification of criminal activity, including bribery, whistleblowing, fusions and acquisitions, protection of network and records, credit ranking, debt recovery, and public processing of personal information. The 2019 Bill expanded the definition of the 'fair goals' by adding 'search engine activity' to the list which can be notified as a reasonable object subject to certain conditions. Personal data may then be processed for search engine activities without the permission of the data principal. While the nature and degree of the permitted handling of personal data under this head would be determined by the rules, this will most likely be deemed to be a welcome change by search engine operating firms who would otherwise have been burdensome to seek data managers' approval – which could impede their service's performance.

ADDITIONAL RIGHTS OF DATA PRINCIPAL

The 2019 Bill grants the Privacy Standards 2 (two) extra privileges with respect to their personal data:

1. The privilege to access in one position to the identification information of the data guardians with which the data has been shared[9]:

   While this proviso appears to have been executed for the information directors to have data about and admittance to the data trustees for which their own information has been

[8] Section 12(a) (i) and (ii) of The Personal Data Protection Bill, 2019.
[9] Section 17(3) of The Personal Data Protection Bill, 2019.

exchanged/stored, it is not known who will have the details of data trustees with which the individual information vaults have been shared.

This is especially applicable to arrangements where data has to be exchanged between several data processors at various times. Furthermore, as of now, there appears to be little explanation as to how this privilege is applied under the 2019 Bill or who will be responsible for it.

2. The right to delete the data[10]:

While this new freedom to erase personal data on request has expressly entered into the 2019 Bill, the 2018 Bill already put a requirement on data trustees to remove personal data until the purpose for which the same data was gathered has been accomplished.

SOCIAL MEDIA INTERMEDIARIES

The 2019 Bill also incorporates the idea of 'social media brokers. Social intervention has been depicted under the 2019 Bill to incorporate 'an intermediary that permits, essentially or exclusively, online contact between 2 (two) or more clients and empowers them to create, transfer, trade, scatter, change or access data utilizing its administrations, yet does exclude middle people that principally: (a) permit business or business-arranged exchanges; (b) give admittance to data through its administrations . In light of the expanding concerns about the impact of web-based media locales on free and fair elections, particularly in the West, and the spread of bogus news around the globe, the 2019 Bill allows the Central Government the option to alarm any online media agent as a major information trustee. Significant information guardians are dependent upon more burdensome obligations, like reviews, record keeping, information security sway audits, and arrangements of information insurance officials.

Additionally, every substantial data trustee will permit clients who register their administrations from India or utilize their administrations in India to approve their accounts wilfully. A certifiable and obvious sign of authentication will be given for the intentional check of the records, which will be noticeable to all clients of the service. While such profiling confirmation may limit the dissemination of false news, it might raise the running expenses of

[10] Section 18 of The Personal Data Protection Bill, 2019.

such interpersonal organization mediators, since they will then be expected to uphold a framework that will urge a consumer to check their profile and increment transparency. Moreover, there is little explanation concerning what records will be endorsed for authentication purposes and what implications (assuming any) will result from this check. In the light of the above provision, the central government ought to be cautious about informing online media mediators . as significant data trustees and should advise only those social media intermediaries as significant data trustees who follow the appropriate requirements set out in the 2019 Bill.

RESTRICTION ON THE TRANSMISSION OF PERSONAL DATA ACROSS THE BORDER

The 2019 Bill wiped out the provisions for the localization of information (for example the prerequisite for every information trustee to store 1 (one) serving a duplicate of personal information on a server or data centre situated inside the purview of India). Albeit this is a much needed development in light of a legitimate concern for ease of business and empowering worldwide organizations to share and store individual information through different locales, the 2019 Bill additionally requests the conservation of a backup of classified individual information in India. Although the relaxing of data localization standards concerning individual information would mean a reduction in managerial expenses for distinctive associations/organizations that don't deal with delicate personal information, the safeguarding of confinement models for personal individual information under Bill 18 of 2019 is probably going to prompt more resistance from stakeholders.

This is especially important provided that the government has the power to broaden the definition of the data to be considered as confidential personal data under the 2019 Bill (please refer above). The 2019 Bill also laid down some requirements on the grounds of which confidential personal data can be passed outside India[11].

CODE OF CONDUCT AND TRANSITIONAL PROVISIONS

The 2018 Bill contained some new provisions on the Code of Conduct that had been precluded from the 2019 Bill. All in all, it is not, at this point a mandate for the Authority to distribute

[11] As per Section 34 of The Personal Data Protection Bill, 2019

codes of practice determining great information security standards or for the Authority to make such codes of practice unreservedly accessible on its website.

The 2019 Bill has wiped out conditions permitting the Authority or other adjudicator, court or regulatory entity to perceive the inability of any information trustee or processor to agree with the Code of Conduct in choosing if such information trustee or processor has broken the arrangements of the 2019 Bill. Another significant highlight to recall is that while the 2018 Bill had a whole chapter given to "transitional provisions' and took into consideration the staggering usage of the provisions,26 the 2019 Bill delivered a significant take-off from this methodology. This implies that the 2019 Bill will come right into action on the date(s) told. This can end up being particularly burdensome given the brief time frame to effectively satisfy all the prerequisites and responsibilities spread out in the 2019 Bill.

CURRENT POLICIES PREVELANT IN INDIA WITH RESPECT TO DATA PROTECTION

India does not have any express data privacy regulations to secure personal information and data exchanged or stored in a verbal, written, or electronic format. However, the regulations on shares are predominant, and they are found in a mixture of legislation, instructions, and rules.

The applicable data protection laws are found in the Information Technology Act 2000 along with the Information Technology (Reasonable Security Policies and Procedures and Confidential Personal Data or Information) Regulations, 2011. (SDPI Rules). These regulations are the basis on which cybercrime and e-commerce conflicts are settled in India. Earlier in the IT Act 2000, the regulations on data privacy and security calling for the protection of confidential and sensitive information provided by electronic means were entirely missing. This lead to the passage of the 2008 Information Technology (Amendment) Act, enacted by section 43A of the Act, which states:

"A corporate body shall possess or deal with any relevant personal data or information and shall be incompetent in maintaining reasonable security to protect such data or information, thereby causing wrongful loss or wrongful gain to any person, and shall be liable to pay damages to the person(s) so affected."

It is essential to consider that there may be no maximum cap to the remuneration which can be promised by the individual concerned under certain circumstances. According to section 72A of the Information Technology Act 2000, the divulgence of records, knowingly and intentionally, without the permission of the person concerned and the violation of the legal agreement, was additionally punished by incarceration for a period of up to three years and a fine of up to Rs 5,00,000.

Information Technology (Reasonable Security Policies and Procedures and Sensitive Personal Data or Information) Laws deal with the preservation of 'Sensitive personal data or information of an individual,' which includes personal information consisting of:-
Passwords,
1. Financial records such as checking account or credit card or debit card or other specifics of payment instruments;
2. Physical, physiological and mental health conditions;
3. Sexual orientation;
4. Health records and history;
5. Details on biometrics.

These rules set out the rational security policies and methodology to be adopted by a corporate body or any entity collecting or preserving data in the interest of a corporate body when handling 'Personal confidential data or information.' In the case of any wrongdoing arising, the corporate body or the entity following up for the benefit of the corporate body, the corporate body may be found liable for the payment of damages to the negotiated party.

In the case of Balu Gopalakrishnan v. the State of Kerala[12], the High Court of Kerala released an interim order demanding that data be anonymize before it is given to Sprinklr, a US-based data analytics firm. The High Court has required the consent of the residents and guaranteed that the data must be returned upon dissolution of the contractual obligations. It also prevented any kind of publicity or commercial use of data by Sprinklr. While it is a step towards the establishment of the data privacy legislation in India, it is important to remember that there is no anonymization standard to be adopted.

[12] Kerala High Court, WP (C) Temp. no. 84 (2020), April 24, 2020.

In every case, there is a limit on the expansion and inclusion of the IT Act and the rules. The prevailing aspect of the agreement only refers to 'important personal data and knowledge' obtained by computers. The regulations are limited to business organizations involved in the mechanized processing of information and consumers are merely prepared to make an obligation move in compliance with a small subset of the agreements. There is no knowledge localization agreement that was the central concern and reason behind the ban on Chinese applications in India.

RECOMMENDATIONS

Though India has laid down its groundwork for the protection of the data mimicking the GDPR, it is certainly lacking in various ways. The text of the bill is basically an unpolished version of the GDPR with some of its enhancements. The framework for data surveillance by the government unquestionably erodes the citizen's Right to Privacy enshrined under the Puttaswamy case[13].

The bill lacks an explicit distinction between non-personal data and personal data which dilutes the individual data protection laws by authorizing the government access to anything and everything it deems to be fit obviously within the boundaries of exemptions, clearly violating the Right to Privacy.

The GDPR is tightly regulated by other EU directives. However, India has no such safeguards which give the Indian government a position prevailing above the Indian laws such as the Information Technology Act 2000, which deals with cyber-crime and e-commerce. Also, the bills allow any protentional nonpersonal data to be shared with the government without laying down any specific standards for anonymity for non-personal data. In their plea, the bill states that this is to refine the services provided by the government which again leaves a cloud of doubt of how and where the data will be shares.

The stance on cross-border sharing and localization of data has been unclear although this provision will lay down major consequences on business in India. Therefore, India is in dire need of a strong set of regulations pertaining to industrial data as well as enhanced drone laws which possesses a major cyber security threat.

[13] (2017) 10 SCC 1

For sharing of personal data across the border, the bill has laid down provisions similar to those of GDPR but has made it crystal clear that the data can only be sent for processing and cannot be stored outside. However, it is silent on the dilemma it will cause for what kind of data has to fall under this category ultimately creating technical issues.

Overall, the bill does not set a noteworthy example to nations who are in line to figure out their Data Protection policies which should be a perfect blend between the right to privacy and data security. The bill requires crucial revisions if the government upholds its constitutional responsibility to its citizens and economic welfare.

CONCLUSION

As the Preamble of the bill suggests, the data protection bill provides for the protection of the privacy of individuals relating to their personal data, specifies the flow and usage of personal data, creates a relationship of trust between persons and entities processing the personal data, protecting the rights of individuals whose personal data are processed in order to create a framework for organizational and technical measures in the processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing such personal data.[14]

However, the bill in many ways lacks specific regulations which safeguard the individual's right to privacy and increases the power of the state to have access to all the data without any particular checks and balances.

While this legislation can be perceived as light at the end of a dark tunnel regarding data protection and privacy in India, there are many more adaptations which India will have to face in the coming years. Also, the Judiciary is more aware and conscious about privacy and security which will certainly lead to robust regulations regarding data protection.

But the government will have to speed up its legislative process to keep up with the pace of technological advancements happening rapidly. The policymakers would also have to be acquainted with the technical know-how to regulate cyber security.

[14] Preamble of The Personal Data Protection Bill, 2019

However, it is the duty of the judiciary to uphold the constitutional sovereignty and since this bill gives disproportionate powers to the government which puts privacy at great risk, in the words of Justice BN Krishna, the intervention of the judiciary becomes mandatory.
