Page 252 - 260 **DOI:** *https://doij.org/10.10000/IJLMH.11461*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

Privacy and Cyberspace in India: A critical analysis of Justice Srikrishna Committee Report and The Personal Data Protection Bill, 2018

MAYUR CHOUDHARY[1] AND PERI PRATIMA[2]

ABSTRACT

Privacy has two facets, first is privacy in the real world which can be defined as preventing a person from intruding into one's physical space or solitude; the second is, privacy in the virtual world also known as cyber space which relates to the collection of user information from a variety of sources including the internet. Privacy in the virtual realm consists of information collection, information processing, information dissemination and invasion on private data.

However, the very technology that offers so many benefits can also expose valuable information to third parties resulting in loss and unwanted use of private and confidential data. Facebook data breach controversy which saw the sale of personal data of 50 million Facebook profiles and the Aadhar data breach, where there were allegations that one could buy personal data stored on the UIDAI's database for as less as ₹500 are the major examples of the threats that Social media poses. Platforms like facebook, instagram, snapchat are seeing ever increasing user base; real-time location check-in, user tracking, selling user data for profiling are some of the few emerging issues. These crimes are evolving at a very fast pace and yet India lacks stringent cyber regulations especially for data protection. There is an imbalance between the age-old laws and the advancement society has made. Information Technology Act 2000 was drafted with major focus to facilitate e-commerce and cyber privacy was not seen as a major concern.

This research paper aims to point out the lacunae in the present laws and stresses the need for robust laws in line with the landmark judgement of Supreme Court which recognised Right to privacy as a fundamental right flowing from Article 21 of the Constitution of India. The researchers have also analysed Justice B.N. Srikrishna Committee report on Data Protection Law and the Personal Data Protection Bill, 2018 and have made comparisons with Europe's General Data Protection Regulation and India's take away from it.

[1] Author is a PhD Candidate at National Law Institute University, Bhopal, India.
[2] Author is a LLM Student at MATS University, Raipur, India

 [ISSN 2581-5369]

I. INTRODUCTION

Privacy is defined as an individual's right to control his or her personal activities or intimate personal decisions without outside interference, observation and intrusion.[3] In present scenario privacy have two facets, first is privacy in *the real world* which can be defined as preventing a person from intrusion into one's physical space or solitude; the second is, privacy in the *virtual world* also known as *cyber space* which relates to the collection of user information from a variety of sources including the internet. Privacy in the virtual realm consists of information collection, information processing, information dissemination and invasion on private data.

With the advent of technology we have moved away from conventional modes of communication to the modern means of communication; telegram, telephone and camera are replaced by mobile phones;computer and mobile phone are readily replacing television; from reading newspapers and magazines to reading articles on internet, we have come a long way. The 21st century is also known as information age, which is associated with digital revolution.[4] Everyone and everything is interconnected and information is readily available.

With the fast-paced technological advancements and ever-increasing use of internet, people are seemingly more indulged in the virtual world, also known as cyber world. Social networking platforms are serving as a tool to facilitate this indulgence. Websites such as Facebook, Twitter, Instagram, and YouTube collectively have a user base of nearly 2 Billion monthly active users[5] having applications and functions such as chatting, photo and video uploading and sharing. These websites collects, retain and process a lot of private information on their servers, which are often maintained outside the territorial jurisdiction of India. An Indian user of these websites has little to no protection against the theft or unauthorized access of this data by a third party. With respect to the liability of these companies for use of these data by third parties without the user's consent, law is silent and the Information Technology Act[6] does not contain any provision and was mainly meant to give legal recognition of e-commerce in India. Cybercrime as a term is defined nowhere in the act.[7]Due to the inefficiency of this Act, some academicians call it toothless legislation[8], which has not been completely effective in issuing penalties, or sanctions against perpetrators who choose to misuse the reach of cyber space.

[3]*Privacy, Black's Law Dictionary* (10th ed. 2014).
[4]Castells Manuel, *The Rise of the Network Society*, Oxford, Blackwell Publishers, 2000.
[5]*State of Social Report*, 2019 https://buffer.com/state-of-social-2019 (Last visited: 23rdFebruary 2021).
[6] Information Technology Act, 2000.
[7] Soumik Chakraborty, *Critical Appraisal of Information Technology Act*, https://www.lawctopus.com/academike/critical-appraisal-information-technology-act-2000/ (Last visited: 23 Feb 2021).
[8]Zargar, Haris, *India's Information Technology Act has not been effective in checking cybercrime*, DNA India, April 3, 2013.

Hence, there exists a void of law, which needs to fillimmediately.

II. TRACES OF USER DATA AND EXPOSURE TO RISK

Every internet user leaves a digital footprint (A trail of data a person creates while using the internet. This includes websites visited, emails sent, information submitted online) some data is collected every moment when one goes though internet, this data collection can be happening with or without the person's knowledge. Based on this, digital footprint can be divided in two categories:

1. Active digital footprint: it consists of publicly traceable information that you share on web, which includes data uploaded on Facebook, Instagram or other social media platforms or any other information, which the user posts online for public viewing.
2. Passive digital footprint: it is made up of the information that a private company reaps behind the scenes which includes IP address, purchasing history, browsing details, location data etc.

Now this digital footprint along with other data of users is often used by companies without the user's consent or knowledge to identify and predict patterns of a user's activity, this data can also be used by a private person to do some unlawful or immoral acts, for example morphing was the most prevalent cybercrime against women a few years back wherein publicly available photograph of females were changed to that of an obscene picture.

Year 2017 saw the biggest data misuse event of all times known as Facebook-Cambridge analytica scandal where Facebook profile data of 50 million people was collected by the use of a third party application named '*thisisyourdigitallife'* which required Facebook login. This data was used by Cambridge analytica to attempt to influence public opinion for various political organizations.

III. REASONS FOR REALIZATION OF CYBER PRIVACY

According to Privacy international[9] few things have contributed to the ever-increasing privacy invasion on internet. They include:

1. Globalization, due to which geographical limitation to the flow of data is eliminated.
2. Convergence and integration is leading to the removal of technological barriers connecting systems, which is resulting in generation of easily exchangeable and

[9] Privacy International (PI) is a registered charity based in London that works at the intersection of modern technologies and rights. https://privacyinternational.org/about (Last Visited 20th February 2021).

interoperable information.

3. Availability of information in multimedia making it easier to translate it in other forms.

These factors make it very easy to gain access of a person's virtual data. This unlawful harvesting of data or illegal access of data is the major cause of rise in cybercrimes. According to National Crime Records Bureau's data, 11,592 cases of cybercrimes were registered in 2015, which rose to 12,317 in 2016.[10]These cases also include breach of confidentiality/privacy.

Most companies and business hire firms specializing in information processing for marketing purposes. Malicious acts like spreading malware and exploitation of bugs is also one such use of breach of privacy. Not only adults but also children and adolescents are at a greater risk as they tend to be ignorant about privacy and its implications and in turn become easy prey for private intruders. Pedophiles can exploit this vulnerability and scammers can rob a person of their money.

IV. CONSEQUENCES OF BREACH OF PRIVACY

Breach of privacy in the form of unauthorized use user data can lead to various general as well as criminal consequences, which may be as follows:

1. Based on the information processed, a user is delivered a curated content, which restricts not only his freedom of choice but also restricts the right to be informed.
2. A user is not free to choose the extent of his exposure of his personal data and is not guaranteed against its potential misuse.
3. Due to external location of the servers, fixing liability of companies becomes a problem.
4. A user may be exposed to criminals in the form of cyber stalker, spammer, hacker etc.
5. The physical life of a user is exposed to strangers especially of children and women. There have been cases where images of women were morphed to portray them in an indecent manner, private chats and images of users are leaked and used for blackmail, children lured by abusers through Facebook.
6. The intermediaries hosting this data have no accountability.

Abovementioned are some of the consequences of data breach, which may result in serious violation of fundamental rights of a user. In the recent case of *Justice. K. S. Puttaswamy (Retd.)*

[10] Shaswati Das, *11,592 cases of cybercrime registered in India in 2015: NCRB*, 06 Apr 2017 https://www.livemint.com/Politics/ayV9OMPCiNs60cRD0Jv75I/11592-cases-of-cyber-crime-registered-in-India-in-2015-NCR.html (Last Visited 20th February 2021).

v. Union of India,[11] right to privacy has been recognized as a fundamental right flowing from Article 21 of the Constitution. To realize the privacy spirited in this judgment the government setup a committee under the chairmanship of retired Supreme Court judge B.N. Srikrishna in August 2017 on *Data Privacy and Protection*[12], its essential objects were:

a) to study various issues relating to data protection in India;

b) to make specific suggestions for consideration of the central government on principles to be considered for data protection in India and suggest a draft data protection Bill.

The committee gave its report on July 2018. The committee in its report[13] observed that data privacy is a burning issue and immediate attention is required on three issues, which are:

- The citizen's rights have to be protected,
- the responsibilities of the states have to be defined,
- the data protection can't be at the cost of trade and industry.

V. HIGHLIGHTS OF THE REPORT

- The law will have jurisdiction over the processing of personal data if such data has been used, shared, disclosed, collected or otherwise processed in India.
- Personal data collected, used, shared, disclosed or otherwise processed by companies incorporated under Indian law will be covered, irrespective of where it is actually processed in India. However, Central Government may be empowered to exempt such companies, which only process the personal data of foreign nationals not present in India.
- No retrospective effect of law. The need of Aadhaar Act to be amended for bolstering data protection.
- The data protection law will set up a Data Protection Authority[14], which will be an independent regulatory body responsible for the enforcement and effective implementation of the law. The Central Government shall establish an appellate

[11] Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
[12] *Justice Krishna to head expert group on Data Protection Framework for India*, Press Information Bureau Government of India, 01-August-2017 http://pib.nic.in/newsite/PrintRelease.aspx?relid=169420 (Last Visited 20th February 2019).
[13] Data Protection Committee Report, Available at, https://www.gov.in%2Fwritereaddata%2Ffiles%2FData_Protection_Committee_Report.pdf&usg=AOvVaw3mOpJmTrJWckd2j_RkcnvJ169420 (Last Visited 21 Feb, 2021)
[14] Hereinafter referred to as DPA.

tribunal or grant powers to an existing appellate tribunal to hear and dispose of any appeal against an order of the DPA.

- Suggesting penalties imposed for violations of the data protection law. The penalties imposed would be an amount up to the fixed upper limit or a percentage of the total worldwide turnover of the preceding financial year, whichever is higher.
- The state can process data without consent of the user on ground of public welfare, law and order, emergencies where the individual is incapable of providing consent, employment, and Reasonable purpose.
- The law will cover processing of personal data by both public and private entities.
- The definition of '*sensitive data*' which includes passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data, and data that reveals transgender status, intersex status, caste, tribe, religious or political beliefs or affiliations of an individual. However, the DPA will be given the residuary power to notify further categories in accordance with the criteria set by law.
- Consent will be a lawful basis for processing of personal data. However, the law will adopt a modified consent framework which will apply a product liability regime to consent thereby making the data fiduciary liable for harms caused to the data principal.
- Cross border data transfers of personal data, other than critical personal data, will be through model contract clauses containing key obligations with the transferor being liable for harms caused to the principal due to any violations committed by the transferee. Personal data determined to be critical will be subject to the requirement to process only in India (there will be a prohibition against cross border transfer for such data).

Based on these recommendations, the Government of India proposed Draft Personal Data Protection Bill, 2018. Meanwhile, European Union, known for its robust and comprehensive laws for regulation of cyber space and democratic control of corporate entities, implemented ***General Data Protection Regulation.***[15]The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the European Union whereas the Personal Data Protection Bill, 2018is aimed at securing the rights of data subjects and overhauling completely the present

[15] *General Data Protection Regulation*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Last Visited 22nd February, 2021).

data privacy and protection regime in India or rather the lack of it.

VI. BRIEF OVERVIEW OF THE DATA PROTECTION BILL, 2018

The Bill has provided a wide definition of sensitive personal data[16] , which includes data revealing or relating to password, financial data, health data, official identifier, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe. International data protection laws have provided a much narrower scope of definition for sensitive personal data. This wider scope would result in companies facing higher compliance requirements.

Every entity processing data is required to store one serving copy of the personal data on a server or data centre that is located within the territory of India[17]. This obligation is likely to increase operational costs for them and may work as a trade barrier hindering the ability of companies to transfer and process data globally. The Bill does not define the term 'critical personal data' or provide any guidelines to determine the same. It states that critical personal data shall be only processed in a server or data centre located in India[18]. This implies that such data cannot be transferred to any country outside India. The Bill imposes draconian measures such as liability on the directors of a company or the officers in charge, for the conduct of the business of the company at the time of commission of the cyber offence.[19]

The Bill provides the data fiduciaries, an obligation to conduct periodic review of the personal data stored with them so that it is not retained beyond the period necessary for processing.[20] However, the Bill does not specify the time intervals at which such review has to be done. This would impliedly increase the operational costs for the companies.

The Bill provides that the data fiduciary have to provide the data principal with adequate notice before collection of personal data.[21]The Bill has establishes Data Protection Authority[22] and has granted it a wide range of discretionary, administrative, quasi-judicial and quasi-legislative powers.

Under the current personal data protection regime in India, which is governed by the IT Rules, all government bodies and related organizations have been excluded from its purview. However, in contrast to this, The Bill has been drafted in such a way to make it applicable to

[16] Sec. 3(35), The Data Protection Bill, 2018.
[17] Sec. 40(1), The Data Protection Bill, 2018.
[18] Sec. 40(2), The Data Protection Bill, 2018.
[19] Sec. 95(3), The Data Protection Bill, 2018.
[20] Sec. 10(3), The Data Protection Bill, 2018.
[21] Sec. 8, The Data Protection Bill, 2018.
[22] Sec. 49, The Data Protection Bill, 2018.

 [ISSN 2581-5369]

all entities, whether or not they are controlled or owned by the government.

VII. MAJOR DIFFERENCES BETWEEN GENERAL DATA PROTECTION REGULATION AND THE PERSONAL DATA PROTECTION BILL, 2018.

General Data Protection Regulation is based the premise that the ownership of data belongs to the entity whose personal date it is. However, the The Personal Data Protection Bill, 2018 fails to provide that. The Personal Data Protection Bill, 2018 brings out a diluted version of General Data Protection Regulation and provides much lesser powers to the citizens.

- The Personal Data Protection Bill, 2018 does not require entities that process the personal data to share the names and other information about the recipient of such personal data with those whose personal data is being processed, which is not the case[23] with General Data Protection Regulation.
- There is no obligation on entities, which process the data to provide information regarding the duration for which the data will be stored while collecting, or at any time, as has been provided[24] in the General Data Protection Regulation.
- The entity processing the data does not need to share the source of the personal data with the entity whose data is being collected, in case the data has not been collected from him/her, which is a mandatory requirement in case of General Data Protection Regulation.
- There is no requirement that the data processing entity share with the data principal the existence of automated decision-making[25], including profiling, which is not the case with General Data Protection Regulation.
- General Data Protection Regulation requires that the entity whose date is being processed, is provided with a copy of data undergoing processing, however, the Indian data protection bill provides a summary[26] of the data to be shared, but has failed to state the scope of that summary.
- General Data Protection Regulation provides right to data erasure[27], however The Personal Data Protection Bill does not provide such a right.

[23]Art. 13 (1)(e), General Data Protection Regulation.
[24] Art. 13(2), General Data Protection Regulation.
[25] Art.22, General Data Protection Regulation.
[26] Sec. 24, The Personal Data Protection Bill, 2018.
[27] Art.17, General Data Protection Regulation.

 [ISSN 2581-5369]

- In case of a breach, there is no requirement by The Personal Data Protection Bill to share it with the entity whose information has been processed but the data protection authority shall determine whether such breach should be reported to that entity[28], which is not the case with General Data Protection Regulation.[29]
- The entities whose personal data is being processed are called 'data subjects' under General Data Protection Regulation and 'data principals' by The Personal Data Protection Bill. In addition, entities that process the personal data are called 'data controllers' under General Data Protection Regulation terminology while being referred to as 'data fiduciaries' by the Indian bill.

VIII. CONCLUSION

Having regard to changing times and increased reliance on technology and internet, a person's life has expanded in the virtual dimension known as cyber world. This exposure is capable of bringing threats to the physical life of person and may hamper the enjoyment of his rights. To protect the individuals against this there is an immediate need to recognize and protect the virtual privacy of individuals. The General Data Protection Regulations of European Union provides comprehensive rules and will serve as a benchmark for data protection laws of future.

The Personal Data Protection Bill is heavily loaded with compliance, which may serve as a good start for regulating companies have control of user data in India. The Act also provides for penalty scheme to serve as a deterrent for non-compliance. For balancing compliance and penalties the economic and trade, interests should also be taken into consideration along with the integrity a person's virtual life.

Legislation of other countries especially on the matter of cross border transfer data should be considered to make the law harmonious and interoperable. The PDP Bill is the most prominent step towards a comprehensive law on personal data protection in India.

*****

[28] Sec.32, The Personal Data Protection Bill, 2018.
[29] Art. 34, General Data Protection Regulation.

 [ISSN 2581-5369]