VOLUME 1 ISSUE 1

"The Indian Data Protection Irony: Potential Shortcomings of Personal Data Protection Bill, 2019"

Pascal Sasil R
School of Law, Christ University, Bengaluru.
pascal.sasil@law.christuniversity.in

----------***----------

ABSTRACT

"*The concept of Privacy is founded on the autonomy of the individual. The ability of the individual to make choices lies at the core of human personality."*

- K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1

Analyzing the simple word privacy, through a legal lens might end up giving different interpretations and implorations. Here, we are concerned about information privacy ranging from contact details given to a retailer to buy a good to giving your iris capture print to the Government for Aadhar Scheme. As the Information Age dawns about us, the baseline has indeed become 'Information is Wealth'. From the Wiki Leaks to the Cambridge Analytica- Facebook Data Scandal, time and again we understand the value of data and information. India has been a late runner in Data Privacy and Protection as it was not until the Landmark Justice Puttuswamy case, The Right to Privacy of Information was even recognized and thereafter the Personal Data Protection Bill, following the footprints of European GDPR. The move is one that must be welcomed, considering the fact that only now people are conscious of how unsafe their data is with no legislations to prevent the free reign of access to personal data. Having said this, there are some serious loopholes and flaws in the bill which may hamper the effectiveness of the bill, defeating its very reason. Clauses talking about law enforcement agencies processing personal data of users without consent for so called 'reasonable purposes', raise serious concerns. Further, the architect of the Bill, Justice Sri Krishna himself has slammed the Bill as one which could well turn free India into an Orwellian state, without the essential safeguards that was proposed in the draft bill.

Thus, this article will analyze the irony, of a bill that seeks to ensure privacy and is instead is criticized for its potential ability to breach a citizen's data. Further, the article will contain a comparative analysis of the bill with other data protection legislations of the world to highlight the possible anomalies.

Keywords: *Data Protection, Right to Privacy, Data Fiduciaries, Global Legislations.*

1. INTRODUCTION

Figures from e-database Statista, estimate the digital population of India to be a whopping 687.6 million[1]. The responsibility to protect such an enormous volume of data of its citizens from all possible vulnerabilities and threats falls on the Indian State. As far as The Republic of India is concerned, the evolution of right to privacy has been a measured progress. Notable landmark cases include Govind v. State of Madhya Pradesh, 1975[2], where the right to privacy was located in Article 19 and 21 of the Indian Constitution. Kharak Singh v. State of Uttar Pradesh,1963[3] had a minority judgement which spoke about the continuous surveillance of police and it being a violation of privacy. R. Rajagopal v. State of Tamil Nadu[4] against advanced the fact that Right to Privacy was in Article 21. Selvi v. State of Karnataka[5] held that any citizen had the right to fair interrogation without use of any techniques that exposes his/her identity as a part of right to privacy. The Information Technology Act, 2000[6] and the SPDI Rules of 2011 were the only active legislations dealing with certain ambits of Data Protection until 2017, when the Landmark Justice Puttaswamy case[7] changed the course of Data Protection Regime in India. The judgement recognized The Right to Privacy of Information as a fundamental right and hence, The Personal Data Protection Bill[8], the nation's first of its kind data protection bill came into existence as a result of the endeavors of Justice Sri Krishna Committee, tasked with the humongous responsibility to draft the exclusive data protection legislation of the country.

[1] Sanika Diwanji, 2020. *Digital population across India as of 2020,* STATISTA [last accessed 30 April 2020]. Available at: https://www.statista.com/statistics/309866/india-digital-population/
[2] Govind v. State Of Madhya Pradesh, (1975) SCR (3) 946
[3] Kharak Singh v. The State Of Uttar Pradesh & Others, (1964) SCR (1) 332
[4] R. Rajagopal v. State Of Tamil Nadu, (1994) SCC (6) 632
[5] Selvi and Others v. State of Karnataka, (2010) 7 SCC 263
[6] Information Technology Act, 2000 (No. 21 of 2000 dated 9th June 2000).
[7] *K.S. Puttaswamy v. Union of India, (2019) 1 SCC 1.*
[8] Personal Data Protection Bill 2019 (Pending).

1.1 Backdrop of the controversy:

However, ever since the bill was made public, it has come under severe criticism from the legal fraternity and the general audience alike[9]. The bill has been termed as a poor rip-off from the European General Data Protection Regulations, 2017. Further, several corporations and tech bodies accused the Indian version of the Bill of improbable expectations and regulations. Amidst all confusions and chaos, the bill was tabled in the Parliament in the month of December, last year. The bill further sent shock waves across the nation as critical parts of the Bill contrasted the draft bill submitted to the central government by the Justice BN SriKrishna Committee[10]. This time around, The Central Government faced severe backlash with Justice Sri Krishna himself as he slamming this version of the bill[11]. The Government was forced to look at other alternatives and hence among various other controversies, the controversial Bill was forwarded to a Joint Parliamentary Committee to analyse the bill and revert back[12].

2. COMPARATIVE ANALYSIS WITH GDPR AND CCPA

With the backdrop now clear, is the bill really obsolete? Does it pose a threat? If so, what are the potential issues? Is it truly a poor rip off from other Data Protection Regimes? Let us analyze the same in a constructive manner. Starting off, let us analyze the issues that have resulted in ripples globally followed by those concerns exclusive to the Indian Front and compare the Bill with global data protection regimes like the European Union's General Data Protection Regulation (GDPR)[13] and California Consumer Protection Act (CCPA)[14].

2.1 Data Localization:

One of the key defects that global pioneers have pointed out are the Data Localization norms located in the bill. Data localization is the practice in which there is a ban or restriction on the

[9] Bailey, R., Bhandari, V., Parsheera, S. and Rahman, F., 2018. Comments on the (Draft) Personal Data Protection Bill, 2018. *Available at SSRN 3269735*.

[10] Sonam Saigal, *Data Protection Bill not in line with draft: Justice Srikrishna*, THE HINDU, (Dec. 18, 2019), <https://www.thehindu.com/news/national/data-protection-bill-not-in-line-with-draft/article30307560.ece>, last accessed on 09 May, 2020

[11] *Final Privacy Bill Could Turn India into 'Orwellian State': Justice Srikrishna,* THE WIRE, (Dec. 12, 2019), <https://thewire.in/law/privacy-bill-india-orwellian-state-justice-bn-srikrishna>, last accessed on 09 May, 2020

[12] *Govt Decides to Send Privacy Bill to Joint Committee, not Shashi Tharoor-Headed Panel on IT*, THE WIRE, (Dec. 11, 2019), <https://thewire.in/law/government-introduces-data-protection-bill-in-ls-to-send-it-to-joint-select-committee>, last accessed on 09 May, 2020

[13] General Data Protection Regulation (EU) 2016/679, Official Journal L 119, 4 May 2016, p. 1-88.

[14] California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.198(a) (2018)

citizen's information from leaving one's home country for processing, storage and collection before/instead of being transferred internationally. Data Localization Norms are a key concept in Global Data Protection with the debate between trade barriers due to the same and cybersecurity risks, a never ending one[15]. The current version of the Act talks about the same in Sections 40 and 41 dealing with Restrictions on Cross-Border Transfer of Personal Data and Conditions for Cross-Border Transfer of Personal Data, respectively. The Act mandates for data localization and cross-border transfer of data only in case of an adequacy decision by the Central Government, or in case of Standard Contractual clauses between companies, which is again subject to approval from the Data Protection Authority that is to be established under the Act. Now, let us compare these norms with the GDPR[16] and CCPA. GDPR has more relaxed norms which require only the Data Protection Commission's intervention and in case of binding corporate rules, a free hand is given to cross border data transfer. One step ahead, the CCPA has no active restrictions on Cross Border Data Transfer! Thus, the Indian norms are indeed very stringent and pose a threat to multinationals which might want to expand their base in India. Though it might be argued that countries like China and Russia already have Data Localization as a concept in their Legislations, we ought to understand the fact that India is still a developing hub for digitalization and it takes millions of dollars as investment for global companies to set up local servers. The issue has become a polarizing concept day by day. While Reliance Chairman Mukesh Ambani, has openly voiced out that Indian data should be owned exclusively by Indians[17], Facebook CEO Mark Zuckerberg called data localization a dangerous entity[18]. Thus, all the concerns voiced out must be investigated before coming to a consensus on this issue.

2.2 Non- Compliance Penalties:

The second issue that global experts have identified with the bill is its non-compliance penalties. The Bill has proposed for fines up to $727,450 or 2% of its Global turnover, whichever is higher, similar to the GDPR, which fines companies $2,184,525 or 4% of turnover. Most global

[15] Selby, J., 2017. Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? *International Journal of Law and Information Technology*, *25*(3), pp.213-232.

[17] Mukesh Adhikary, *'Data is the new oil': Mukesh Ambani says global firms should not control India's data,* BUSINESS TODAY, (Jan. 18, 2019), <https://www.businesstoday.in/current/economy-politics/data-new-oil-mukesh-ambani-says-global-firms-should-not-control-india-data/story/311244.html>, last accessed on 09 May, 2020

[18] *Why Mark Zuckerberg Is Not Happy With India's Data Localisation Demands,* GADGETS 360 NDTV, (Apr. 27, 2019), <https://gadgets.ndtv.com/social-networking/news/why-mark-zuckerberg-is-not-happy-with-india-s-data-localisation-demands-2029546>, last accessed on 09 May, 2020

companies and Indian techs have only just established their bases and many more global firms have been counting on the Digital India Scheme to make their foothold in India. In such a scenario, such stringent norms to deal with non-compliance comes as nothing but a deterrent to these establishments. The addition of criminal liabilities making the offences cognizable and non-bailable under the bill further worsens the situation. Grave concerns have been raised about India's e-commerce sector which is the second largest in the world and the imposing of such stringent norms might potentially strangle it in a situation where the market has already experienced a huge lull courtesy of the COVID-19 pandemic.

2.3 The Right To Be Forgotten:

Moving forward, the 'Right to be Forgotten' is one more aspect of the bill that has been surrounded by various ambiguities. The Act pushes only for a stay on the access and usage of existing data, in case of any requests made from the side of the user. This is undoubtedly not enough as the possibility of Data Breach is highly likely in case of such unattended data. As far as European GDPR is concerned, they are miles ahead, in mandating firms to delete all existing data in case of requests and thus preventing the likelihood of any misuse or breach in stored data. On the land, the transparency of the proposed Data Protection Authority has also come under the scanner of several critics. While the bill intends to improve transparency and accountability, the Data Protection Authority that is proposed under the bill, comprising of a chairperson and six other members appointed by the Central Government is extremely limited in its scope and number. Further, the Bill does not mandate any limitation period for reporting a potential breach to the authority and thus raises several questions over the effectiveness of the proposed Authority.

2.4 Absent Automated Technology Regulations:

There exist some fatal flaws dealing with automated technology in the bill. With the advent of technology, most companies are making a calculated approach towards the use of automated systems in data collection and processing. European GDPR recognizes the need to protect individuals from automated decision making and hence it vouches for the right to not be subjected to automated decision making. The Indian PDPB is not progressive when it comes to this and doesn't mention about any such explicit right, raising ambiguities over its effectivity in case of future legal issues surrounding the same.

3. DATA PRIVACY CONCERNS – THE UNIQUE INDIAN IRONY

Having discussed about the major global concerns, let us jump to the Indian front and investigate the concerns raised about individual data privacy. It is indeed a huge irony that a Bill intended to protect Personal Data of citizens is in turn criticized for the potential risks it poses to individual data. The primary concerns raised by the Indian legal fraternity surround the principle of categorization of user data and unregulated access to this data by law enforcement agencies. The latest version of the bill allows Blanket Governmental access to data of users in some cases, especially when national security is involved. Further, the bill has provisions that empowers the government to ask companies for anonymized personal data and non-personal data. While it broadly categorizes data of individuals into three categories, critical, sensitive and general the government can, at any point, bypass restrictions to give complete access to itself or any agency under it. Thus, several exemptions have been allowed in the bill for the Government to access data in an unaccounted manner. Having said all this, the whole crux of this criticism lies in the fact that the original draft version of the bill had no such mention of providing any such exemptions or powers to the government or its agencies. On the contrast, the draft bill contained provisions that required for proper authorization by law for accessing and processing data of citizens, even if it entails national security. The final bill clearly roots out any such procedure that the government would have to follow. Justice BN Srikrishna himself has slammed this particular controversial aspect of the Bill. He went on to express concerns that this particular unregulated governmental access to personal data could well turn Free India into an Orwellian State[19]. The term Orwellian state is used to describe a system of governance that has draconian control over its people, as described in the novel Nineteen Eighty-Four by George Orwell. *"They have removed the safeguards. That is the most dangerous. The government can at any time access private data or government agency data on grounds of sovereignty or public order. This has dangerous implications."* quoted Justice Sri Krishna. This criticism is indeed justified as the bill might make the going tough for the common man and such a sensitive aspect must have its safeguards in place to prevent misuse.

CONCLUSION

Thus, these are some of the many potential issues in the Bill which might end up defeating the very aim of the bill, to uphold and ensure 'The Right To Privacy' of every citizen. We, 1.3 billion

[19] *Supra* at note 6.

citizens of India, have a right to this privacy and any entity, sovereign or non-sovereign ought to be denied the chance to interfere with the same. Certain asks like the restriction on the blanket powers given to government ought to be looked into in an unbiased manner. On the other hand, from a global perspective, we are looking at potential losses to the Indian frontier courtesy of certain flaws and many other stringent provisions. Addressing these issues without any bias is the only solution at our hands to give India the vital push in Data Protection. The legal and legislative fraternity must understand the implications of the same in this ever evolving 21st Century. The issue is still afresh with the Joint Parliamentary Committee reviewing the bill and various parties have been sending across their fair concerns before the committee[20]. The Joint Parliamentary Committee has a huge responsibility on its shoulders to investigate upon the same to prevent any further shortcomings arising out of the same. With high hopes pinned on the Joint Parliamentary Committee, on an endnote, we as members of the legal fraternity have a greater responsibility to look at both sides of the coin to ensure that any right instilled by law, for that matter of fact, is preserved.

[20] Surabhi Agarwal, *Tech bodies to take Data Bill worries to house committee*, THE ECONOMIC TIMES, (Feb. 20, 2020), <https://economictimes.indiatimes.com/tech/ites/tech-bodies-to-take-data-bill-worries-to-house-committee/articleshow/74217942.cms>, last accessed on 09 May, 2020

REFERENCES

Journals and Scholarly Articles:

1. Bhandari, V. and Sane, R., 2018. Protecting citizens from the state post Puttaswamy: analysing the privacy implications of the Justice SriKrishna committee report and the data protection bill, 2018. *Socio-Legal Rev.*, *14*, p.143.
2. PUTTASWAMY, P., IMPLICATIONS OF THE JUSTICE SRIKRISHNA.
3. Rosen, J., 2011. The right to be forgotten. *Stan. L. Rev. Online*, *64*, p.88.
4. Weber, R.H., 2011. The right to be forgotten: More than a Pandora's box. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, *2*, p.120.