SSRG International Journal of Humanities and Social Science
ISSN: 2394-2703/ https://doi.org/10.14445/23942703/IJHSS-V11I2P101

Volume 11 Issue 2, 1-4, Mar-Apr 2024

Review Article

Evolution of Data Protection Regime in India: An Analysis

Arjun Arya

Bellarmine College Preparatory, California, United States of America.

Corresponding Author : arya.arjun183@gmail.com

Received: 02 February 2024 Revised: 10 March 2024 Accepted: 20 March 2024 Published: 03 April 2024

Abstract *- With the increasing relevance and significance of protecting sensitive data, whether relating to an individual or a business entity, an analysis of the safeguards proposed by the existing data protection regime in India becomes essential. This policy paper sheds light on the shortcomings of The Digital Personal Data Protection Bill 2022, alongside tracing the evolution of the data protection bill in India, along with its several iterations and modifications, and proposes to seek inspiration from the best practices pertaining to the data protection laws from countries such as the U.S.*

Keywords *- Data Protection, India, Privacy, Security, Data Protection Authority.*

1. Introduction

India's approach to data protection and privacy has been evolving as priorities of India and the world have been. India is known as the world's largest democracy, but its data policies need some more democratic elements to it. The latest bill, the Digital Personal Data Protection Bill (2022), on the issue of data policy introduced in India has many glaring issues in it, such as the non-consensual usage of CCTV cameras, as well as the data held by the Data Protection Agency ("DPA") established under the bill not being subject to the bill and its fines/penalties.

The latest edition of India's bill imposes penalties of up to INR 500 crore. However, this bill does have certain loopholes that allow international companies to export the data of Indian citizens for profit, as well as allow the federal government to give state agencies exemptions from these laws. The bill is also being referred to as a move that is seen as a win for tech companies but a loss for the citizens. (Singh 2022)[1]

In August of 2017, the Supreme Court of India, in the case of KS Puttaswamy vs Union of India, ruled that personal privacy is a fundamental right under the framework of the right to life under Article 21 of the Constitution of India. This judgment was a breakthrough in India's nonexistent data protection policy. In this case, a nine-judge bench of the Supreme Court overruled its two previous judgments passed in the case of Kharak Singh vs State of U.P. and M.P Sharma vs Union of India, wherein the court had earlier held that privacy was not a fundamental right under the Constitution of India.

The Puttaswamy decision created a need for more strict laws governing the issue of privacy, specifically related to data. A month previous to the Puttaswamy decision, a committee headed by Justice B.N. Srikrishna and consisting of nine members had been created to examine issues related to data protection in India, which had been proportional in growth to the growth of information technologies in India and the rest of the world.

2. Results and Discussion

2.1. Addressing the Problem

The current bill has many problems with it. The bill does not provide detailed specifications on various elements, such as the use of CCTV footage, the timeline for destruction of data, et cetera. Further, the current bill does not provide a time-bound limit for fiduciaries (any entity holding or using data) to destroy data, along with the associated procedure for destroying such data or retaining the data. This is important because if a time or deadline is not given, companies will not assign people to destroy data, as there is no harm in procrastinating and not doing it if a company says it will eventually. Additionally, this bill does not allow for prosecution against the DPA itself or any employee connected with it, so data stored by the DPA is not protected under this bill. The bill is strangely quiet on the non-consensual recording of CCTV cameras in India, and it is not clear whether the bill will fine misuse of CCTV data recordings under the INR 500 crore limit. These issues are important because citizens should be made aware of whether any of these issues are subject to this bill so that they are aware of whether their privacy is protected or not.

2.2. Personal Data Protection Bill, 2018

The Committee of Experts on a Data Protection Framework for India submitted both its report and a drafted Personal Data Protection Bill in 2018. Section 2(13) of this bill defined "personal data" as any information that renders an individual identifiable. The said bill made for personal data being allowed to be processed if the individual gave consent, in a medical emergency, or if the state could, provide benefits to the individual person. It allowed exemptions for certain kinds of data processing relating to journalism, national security, and legal proceedings. The fiduciary must store a serving copy of the data in India. The fiduciary must notify and inform the user of how their data will be used and the purpose of the data, among other things. If there were to be a data breach, the fiduciary must notify the DPA if it will be harmful to the individual. The state is not required to ask for the individual's consent when providing any government benefits, as it takes data to find where you are a citizen. The DPA can arrest and detain violators of the bill in prison without any approval or order needed from the court.

In 2019, the bill was tabled, and finally, 2 years later, the Joint Parliamentary Committee adopted a final set of recommendations, which required stricter compliance from Informational Technology companies. This bill, unfortunately placed economic interests at least on the same level as personal data privacy. The economic interests being placed above the data vulnerability of Indians is very against the decision of the Supreme Court in the case of KS Puttaswamy vs Union of India.

2.3. Data Protection Bill, 2021

The 2021 bill was renamed to the "Data Protection Bill 2021" since the bill will regulate non-personal data as well if put into action. The user rights were weakened, including places in the new bill using vague language implying that data fiduciaries would be allowed to reject requests from users to erase, update, and correct their data. The reason given for this was "technical infeasibility," which therefore gives the fiduciaries more power, as seen through Section 18(3) of the bill. There is a little bit of hope provided for the common citizen through Section 62 of the bill, which enables any ordinary citizen to file a complaint with the DPA and allows for compensation. Social media companies, such as Meta and Twitter, are not treated as publishers, and the verification method for these platforms falls under scrutiny. Social media platforms will hold personal data about verified users on these platforms to indicate an actual user, although this is a deviation from laws in other European countries. According to the Information Technology Act of 2000 (IT Act), social media platforms are known as "intermediaries," which basically enhance access to data for the common man; this bill recognizes that the IT Act has not been able to regulate the platforms well. The bill also extends the provision to foreign-based entities in case Indians are subjected to their data processing activities (Wadhwa 2022)[2]. This bill introduces the term, "significant data fiduciary," which means that if a platform has above a certain number of users, then the platform becomes a fiduciary like any other data company under the bill. This seems well, but because of the verification process in the bill, this bill is a net loss for data privacy.

2.4. Digital Personal Data Protection Bill, 2022

In 2022, the Digital Personal Data Protection Bill was proposed by India's Ministry of Electronics and Information Technology, which made for a Data Protection Board to oversee compliance and impose financial penalties amounting to up to INR 500 crore. (Baldin 2022)[3] The bill will allow companies to transfer some users' data abroad while giving the federal government powers to exempt state agencies from the law in the interests of "national security." (Vengatill 2022)[4] This latest bill makes more clear statements about consent taken from a user, including having the data fiduciary ask for consent before using any trackers on personal data, such as cookies. Another provision made by the bill is regarding children. Data fiduciaries are not allowed to process personal data about children without verifiable parental consent, and data fiduciaries are also not allowed to show personalized ads to children in India, according to Sections 10(1) and 10(3), respectively. In terms of the penalties specified in this bill, INR 500 crore amount would do a lot of damage to India's growing digital ecosystem. Hence, the bill recommends a ramp-based penalty system.

2.5. Data Policy in the US

The data policy in the US is very jumbled at the federal level, mainly derived from the Federal Trade Commission Act, which bars unfair and deceptive business practices from companies. An example of this could be a company stating that it does not sell a user's personal data and then selling it anyway. Children under the age of thirteen are more specifically protected under COPPA (Children's Online Privacy Protection Act), which bars the collection of personal data of any person under the age of thirteen digitally. If information is being collected from children, then the publication of privacy policies, as well as parental consent, is required. Another example of data protection policy in the US is the law on video and audio recording, which is restricted for sale, and this includes online streaming. The Cable Communications Policy includes provisions dedicated to the protection of a subscriber's privacy. These are all at the federal level, and most, if not all, states have more extensive laws on data protection.

When it comes to data protection, some states are more actively making laws protecting their citizens than others. Massachusetts has relatively strong data laws in its state legislation, including a law requiring any entity that has access to personal data to maintain a comprehensive written information security plan and to establish and maintain a formal information security program. (Pittman 2022)[5] New York is also establishing more safe practices in the interest of

its citizens, requiring companies to perform periodic risk assessments and file annual compliance certificates. A big surprise on this list of forward states is Illinois, which is the most modern state in terms of its privacy laws. This is seen through it being the first state to regulate companies that collect biometrics or calculations related to human characteristics, and data and allowing people whose biometric data has been violated to sue the company without having to show they suffered harm. Lastly, California enacted the California Consumer Privacy Act ("CCPA"), which included a clause requiring businesses to specify the category of personal information they were taking from the user. It gave California residents two new rights. These were the right to access and delete personal information given to a business, as well as the right to opt out of having personal information sold to third parties.

There are many sector-specific laws, or laws governing data policy in different fields. For example, the Gramm Leach Bliley Act (also known as the Financial Services Modernization Act of 1999) governs the protection of personal information held by banks, insurance companies, and others in the financial service sector, imposing requirements on securing NPI, or healthcare numbers, restricting disclosure of and use of NPI, notifying customers when NPI is being used.

All of these laws in the US are not managed by a single entity but are instead managed through their respective sector managers. The CCPA established the first dedicated privacy regulator in the US, and its responsibilities included reinforcement of the CPRA, working with the Attorney General, rulemaking under the CPRA, and, lastly, promoting public awareness of issues relating to data privacy.

2.6. US Inspirations Visible for India

India may consider adopting the US sector-specific strategy in protecting data. What this means is that each business sector can have different laws governing data privacy and protection, which would allow for more clear-cut laws for any scenario and less confusion over what laws govern which case. This would also eliminate the confusion over CCTV cameras, as security would be a different sector from others and should, therefore, have different laws than other things, since it is not related to, say, Facebook data tracking. Such a sector-specific approach has the potential to ensure that citizens understand the laws and whether a specific case is applicable to that law. There are only so many specific cases one can mention in a bill, and the US approach has the advantage of having many different bills forming the base of data protection policy. There are concerns that if a singular bill is employed, it can only go into so much detail before the common person cannot process it. Many people have questions about specific things that cannot be answered just through one bill.

This is where the US-adapted data policies, pushing for a sector-specific approach, would come in. For example, having a separate regulation governing CCTV footage would provide more clarity to citizens about which of their data is protected by what law and what is not protected or policed. This would lead to shortening the length of trials as well, since many cases would just be open and shut about which law was violated, and doling out the punishment, instead of taking many weeks, months, and years to settle which provision was violated, which is detrimental to the Indian Judicial System and wastes precious time for judges who could be heard for other criminal cases.

2.7. Action Plan

A way to implement the aforementioned would be to begin by solving specifically those issues that have many non-open-and-shut cases, such as data infringement and children's data being leaked, both of which are damaging issues that take a long time to prove. Stricter regulation of both of these issues would result in better data protection. Further, issues addressed above with the Digital Personal Data Protection Bill, such as CCTV footage, would be filed under the government/police data sector because the police mainly use CCTV footage, so there would be separate laws made for the same. In addition, the DPA established by the bill would be regulated according to the provisions of the bill, and prosecuted the same as any other entity or business.

3. Conclusion

In conclusion, India has made strides in data policy after the Puttaswamy case. However, because of vague language and issues being unaddressed, such as CCTV being unaddressed and timelines not being provided for fiduciaries to destroy data, the bill in its current form should not be implemented. This is where the US adopted sector-specific approach may come in to provide India with inspiration on how to address these problems with specifics and provide concrete steps for actions that need to be taken by fiduciaries.

References

[1] Jagmeet Singh, and Manish Singh, India Proposes Permitting Cross-Border Data Transfers with Certain Countries in New Privacy Bill, TechCrunch, 2022. [Online]. Available: https://techcrunch.com/2022/11/18/india-digital-data-protection-bill-2022-draft/?guccounter=1

[2] Rishi Wadhwa, and Grace Bains, The Evolution of India's Data Privacy Regime in 2021, IAPP, 2022. [Online]. Available: https://iapp.org/news/a/the-evolution-of-indias-data-privacy-regime-in-2021/

[3] Anna Baldin, India: Digital Personal Data Protection Bill, 2022 - What You Need to Know, DataGuidance, 2022. [Online]. Available: https://www.dataguidance.com/opinion/india-digital-personal-data-protection-bill-2022

[4] Munsif Vengattil, and Aditya Kalra, India Proposes Easier Cross-Border Data Transfers Under New Privacy Law, Reuters, 2022. [Online]. Available: https://www.reuters.com/world/india/india-releases-draft-new-data-protection-bill-2022-11-18/

[5] F. Paul Pittman, Abdul Hafiz, and Andrew Hamm, Data Protection Laws and Regulations Report 2022-2023 USA, ICLG. Com, 2022. [Online]. Available: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa