Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 6, 1734-1738

Data Protection And Privacy Laws: An Indian Perspective

Dr. Shraddha Pandey

Associate Professor & HoD School of Law ITM University Raipur.

Abstract

In India, a number of measures are being adopted in order to work on the privacy and data protection concerns of the individuals. In this regard, the Data Protection Bills are a noteworthy contribution, which were brought forth post the landmark ruling of 2017 case given by the Supreme Court of India that made the right to privacy a fundamental right of any person. This discussion embarks upon the journey of development of Indian privacy and data protection legislation post this ruling, with a focus on the recent amendments.

Keywords: Data protection, privacy law, privacy, right to privacy, data protection bill

1. Introduction

In the present digital world, there is a lot of discussion undertaken on the terms like privacy and data protection. This is because of the growing concerns across the globe with regards to the protection of privacy and that of data, for both the public and private individuals, including the companies, entities, and other such bodies[1]. From the files of a company that are put on a network, to the social media profile of a person, even when the same is locked, everything is prone to an attack, as long as it is digitally connected. There have even been concerns of the auto-driven cars having a possibility of being hacked[2], or the surveillance cameras being gained an unauthorized access of[3].

To put this in perspective, one can refer to the statistical data. In the first half of 2020, the data breaches across the globe, exposed nearly thirty-six billion records. The cybersecurity risks were deemed to be noticing an upward trend, as per 68% of the business leaders. The common causes of data breach involved financial motivation, in 86% cases, and espionage, in 10% cases. To understand the costs of such instances, one can look at the average cost of data beach as of 2020, which stood at $3.86 million. And to identify a breach, the average time taken was 207 days[4].

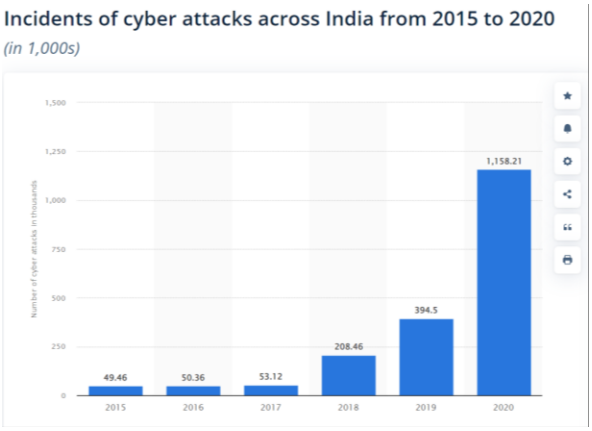
The figures are staggering and depicts the need of strong privacy and data protection laws, which have been put forth in majority jurisdictions, including India. The present discussion attempts to highlight these very laws, particularly in context of their evolution, to understand the manner in which attempts are made to curtail the acts of privacy and data breach in the nation.

2. Understanding the Indian Privacy and Data Protection concerns

2.1. The Problem: Data

In comparison to 2019, where 400 thousand cyber-attacks were noted in India, the year 2020 saw over 1.1 million cyberattacks being reported in the nation. The chart given below shows the growth in incidents of cyber-attacks in the nation from 2015 to 2020[5].

Figure 1: Incidents of Cyber Attacks



As per one of the recent reports, there was four times increment in the data theft in a year, where nearly 87 million Indian users stated that their personal information had been stolen. This report was provided by Surfshark, a Netherlands based VPN provider. The figures were presented for 2021, where the comparison was drawn from 2020. As per this report, the nation held the third position in the number of users that had their data compromised, on a nation-based data breach statistics, and stood just after the US and Iran. The big data breaches covered the Air India and Domino's India cases. The user accounts theft witnessed in the nation stood at 19.2 million, which is a very concerning figure[6].

The latest statistics are also worrisome. The cybersecurity incidents that were noted till February 2022 stood at over 2.12 lakhs. These numbers were presented in the Lok Sabha by Rajeev Chandrasekhar, the Minister of State for Electronics and Information Technology. This was given by the Indian Computer Emergency Response Team, which reported similar cases at 14.02 lakhs for 2021. The need for ensuring safety, openness, accountability, and trustworthiness of internet was deemed crucial by the government, for all the users. There has been a noted surge in the cyber security related attacks on the critical infrastructure of India. For instance, Mumbai, the nation's financial capital, saw a massive power outage in October 2020 that resulted in the train services being cancelled, which essentially brought the entire city to its knees[7]. Some of the other noteworthy cases includes the COVID-19 Results Database incident, and the data breach incidents of MobiKwik, Upstox, and Unacademy[8].

2.2. The Solution: Laws

2.2.1. Rights to Privacy Case

Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors (2017) 10 SCC 1[9] is deemed as the landmark case in Indian privacy law sphere as this is the case that declared right to privacy as being the fundamental right of any person. This case was decided by the Hon'ble Supreme Court of India and has often been referred to as the Right to Privacy Case. This case strengthened the need for bringing more conclusive legislation within the Indian jurisdiction for protection of the privacy and personal data of the individuals[10]. This led to the Central Government appointing a data protection committee in August 2017 that was chaired by Justice Srikrishna, who is the retired judge of Supreme Court of India. The committee put forth an extensive white paper on 27th July 2018 that highlighted the significance of data protection. July 2018 saw the release of the Personal Data Protection Bill 2018 by the committee. On the basis of the recommendations that were presented by the industry stakeholders, the Personal Data Protection Bill, 2019 (the Bill) was brought forth a year later, with few modifications, in the lower house of Indian Parliament[11].

2.2.2. Data Protection Bill, 2019

On 12th December 2019, the Bill was referred for further debate and examination to the Joint Parliamentary Committee. Nearly two years after deliberating on this Bill, on 16th December 2021, the Committee presented its report on this Bill, covering changes to the Bill and recommendations as well. Some of the key recommendations that were presented in this report need to be looked into to understand the

manner in which a change was brought in the Indian privacy and data protection law, or an attempt for which was at least put forth. This would also help the stakeholders in understanding the impact these suggestions have on the privacy of an individual, particularly the rights pertaining to it[12].

2.2.2.1. Personal Data

The first and foremost one in this regard was related to brining a change in the name and scope of the Bill. The Bill covered the regulation of personal data of the individuals only. This is the reason that the recommendations covered the need for changing the name of the Bill so as to cover the non-personal data as well. The Bill empowered the Central government to get access to non-personal or anonymised data from any data fiduciary so as to allow itself to get a better targeted delivery of services and/or to formulate evidence based policies. Yet, concerns were raised by the stakeholders regarding the same legislation covering personal and non-personal data having the possibility of dilution of goals of the proposed bill, which meant to protect the personal data of an individual only[13].

2.2.2.2. Localized Data

The provisions of the data localization were present in the Bill, which were recommended upon by the committee regarding the data to be stored in India being a crucial aspect, as it was significant from security and national reasons. The suggestions also provided that the Government had to bring in mirror copies for the critical and sensitive personal data that had been stored abroad, along with the Indian operating entities to gradually shift towards the data to be localized. Apart from the provisions pertaining to localisation of data, the proposal was put forth in the Report for the Central Government to prepare a comprehensive data localization policy that had the goal of developing a proper infrastructure for local data storage, along with assisting the start-ups in compliance with the localization requirements. At the same time, the goal of the government was set to ease of doing business for such start-ups[14].

2.2.2.3. Data Protection Authority

The next one was related to the selection of Data Protection Authority, the selection of which covered limited stakeholders, and had to be the members of the Ministry of Electronics and Information Technology, and the Ministry of Legal Affairs. The recommendations were put forth for the selection of committee to have a wider representation from academic experts, along with technical and legal ones, along with the bureaucrat officers covering this selection committee. The reason behind this was to ensure that the control was not solely in hands of the Central Government, and involved the members that were appointed on their behest[15].

2.2.2.4. Data Protection Officer

Even though the Bill made it obligatory for the appointment of a Data Protection officer as a significant data fiduciary, the Report proposed that such an officer should be appointed to have an important role in operations and management of the important data fiduciaries, along with such an officer being a key managerial personnel or senior level officer that has technical knowledge in operations field of the relevant significant data fiduciary[16].

2.2.2.5. Government Exemption

The government had been provided with exemption from compliance based on this draft legislation so as to protect the national interest. There were certain conditions put forth for this exemption where the recommendations were given that the Government could exempt itself from the provisions where it was a just, fair, proportionate, and reasonable procedure. This was parallel to the Supreme Court judgement given in Right to Privacy Case pertaining to the tests of proportionality, procedural safeguards, legitimate aim, and legality tests being put forth in that case. These tests had to be met in order for the right of privacy of a person being proven to have been breached by the Government so as to

pursue the exemptions that were made available to it[17].

2.2.2.6. Regulating social media

The social media intermediaries, as per the report, had to be subjected to a higher level of scrutiny. For curbing the problems associated with the fake accounts and fake news, the suggestion was for verification of all user accounts on such social media intermediaries. The failure of the Information Technology Act, 2000 in context of intermediary framework was deemed to have been failed in attaining its goals, leading to the recommendations for the social media intermediaries to be deemed as publishers of certain specified content, particularly when it was coming from the unverified accounts. Apart from this, recommendations were put forth that none of the social media platforms should be permitted to have their operations in the nation, so long as the parent company that handled that technology, had an office set up in the nation. In addition to this, on lines of Press Council of India, a statutory media regulatory authority had to be set up for regulating the content on all of the social media platforms, regardless of the platform in which the content was published, be it offline, online, print or otherwise[18].

2.2.2.7. Breach of Data

The companies were required to report any kind of personal data breaches under this bill, where such a breach resulted in harm being caused to the data principal. Though, apart from this, the report mandated a log to be maintained that covered all kinds of data breaches, irrespective of the fact whether such a breach was related to the non-personal or personal data, even when the chances of harm to the data principal were present or not. Furthermore, a timeline of seventy two hours was also put forth for reporting such breaches. This meant that not only there was a need to report the breaches, but a mandatory log had to be maintained for personal and non-personal data, that was not contingent to the data principal being harmed, within a proper timeline[19].

2.2.2.8. Data of Children

There had been pertinent provisions with regards to the data of children being protected under the Bill. The concept of guardian data fiduciary was defined under this Bill as data fiduciary, which operated on online services or commercial websites that were directed at the children, or that processed large volume of personal data of children. The bill exempted the guardian data fiduciary from attaining the parent's or guardian's consent, which is required by the other data fiduciaries. The recommendations put through this report required the deletion of guardian concept as being a separate class of data fiduciary, since there was a possibility of the goal of protecting children being diluted. Apart from this, the recommendations were put forth regarding the data fiduciaries being barred from undertaking tracking, targeted advertising, profiling, or behavioural targeting of children, along with processing the personal data that could have the possibility of causing a major harm to the children. Earlier, only the guardian data fiduciaries had this bar applicable[20].

3. Conclusion

In conclusion, it is clear that the data protection and privacy areas are a focal point of discussion in the present legal discussions taking place in the nation. These were started post the 2017 ruling that was given by the Hon'ble Court, giving the right of privacy as a fundamental right for all the individuals. This led to the different versions of Data Protection Bill being put forth and recommendations being given on it. This has been done with the goal of bringing a comprehensive data protection legislation in the nation, which is presently missing, leaving the individuals prone to cyber security concerns. The previous parts highlighted the statistical data on the growing cyberattacks in the nation, which highlight the necessity of such measures to be adopted at the earliest. It remains to be seen what the final legislation would be and the provisions that are adopted in the finally drafted Act. However, it is crucial for the suggestions put forth by the various scholars to be considered in order to reach the goal of bringing a comprehensive data protection legislation in India.

References

1. "Comparing Draft Data Protection Bill, 2021 With Its Predecessors", Internet Freedom Foundation (Webpage, 2021) <https://internetfreedom.in/comparing-pdpb/>
2. "Law In India - DLA Piper Global Data Protection Laws of The World", Dlapiperdataprotection.Com (Webpage, 2022) <https://www.dlapiperdataprotection.com/index.html?t=law&c=IN>
3. "Ten Compelling Features of India's Proposed Data Privacy Law | JD Supra", JD Supra (Webpage, 2022) <https://www.jdsupra.com/legalnews/ten-compelling-features-of-india-s-6127498/>
4. "Update On Data Protection Law - Privacy Protection - India", Mondaq.Com (Webpage, 2022) <https://www.mondaq.com/india/privacy-protection/1146570/update-on-data-protection-law>
5. "Update On Data Protection Law", Alpha Rajan & Partners (Webpage, 2021) <https://alpha-partners.org/2021/12/29/update-on-data-protection-law/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=LinkedIn-integration>
6. Basuroy, Tanushree, "India: Number of Cyber Attacks 2020 | Statista", Statista (Webpage, 2022) <https://www.statista.com/statistics/1201177/india-number-of-cyber-attacks/>
7. Boehme-Neßler, Volker, "Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection" (2016) 6(3) International Data Privacy Law
8. Bose, Abanti, "Top 10 Data Breaches That Have Occurred in India in 2020-21 - Ipleaders", Ipleaders (Webpage, 2021) <https://blog.ipleaders.in/top-10-data-breaches-that-have-occurred-in-india-in-2020-21/>
9. Gokhale, Gowree, Aaron Kamath and Purushotham Kittane, "Privacy &Amp; Data Protection Capsule: India&Amp;#039;S Turn on The World Stage", The National Law Review (Webpage, 2022) <https://www.natlawreview.com/article/privacy-data-protection-capsule-india-s-turn-world-stage>
10. Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors (2017) 10 SCC 1
11. Kaiser, E., "Monitoring Employees with Hidden Surveillance Cameras Breaches Their Right to Privacy" (2018) 4(3) European Data Protection Law Review
12. Lee, Chasel, "Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars" (2018) 69 Fed. Comm. LJ
13. Manohar Lal Sharma v Union of India (2021) SCC OnLine SC 985, decided on 27.10.2021
14. Mihindukulasuriya, Regina, "4-Fold Rise in Data Theft in A Year, 86.6 Mn Indian Users Had Personal Info Stolen, Says Report", The Print (Webpage, 2021) <https://theprint.in/tech/4-fold-rise-in-data-theft-in-a-year-86-6-mn-indian-users-had-personal-info-stolen-says-report/782707/>
15. Sobers, Rob, "134 Cybersecurity Statistics and Trends For 2021", Varonis.Com (Webpage, 2021) <https://www.varonis.com/blog/cybersecurity-statistics>
16. Sodhi, Shruti Dvivedi, Bansari Samant and Tushar Sinha, "The Journey of India's Data Protection Jurisprudence", Lexology (Webpage, 2022) <https://www.lexology.com/library/detail.aspx?g=57720842-f709-4dd4-947b-44c3c6e4ed10>
17. Thathoo, Chetan, "2.12 Lakh Cybersecurity Incidents Reported In 2022: Indian Govt", Inc42 Media (Webpage, 2022) <https://inc42.com/buzz/2-12-lakh-cybersecurity-incidents-reported-in-2022-indian-govt/>
18. Wadhwa, Rishi and Grace Bains, "The Evolution of India's Data Privacy Regime In 2021", Iapp.Org (Webpage,2022) <https://iapp.org/news/a/the-evolution-of-indias-data-privacy-regime-in-2021/#:~:text=In%202017%2C%20the%20Supreme%20Court,does%20not%20exist%20in%20India.>