VOLUME 26 | SEPTEMBER, 2021 ISSN 2456-9704

NEED OF THE HOUR – A LAW FOR DATA PROTECTION

By Madhumita C
From Sastra Deemed University

Introduction:

The on-going pandemic has altered life as we know it, and the year 2020 saw a rapid transition to digitization of data as it became the means of conducting everyday business affairs. The silver lining under this particular cloud, was that it brought to the table the need for a Data Protection bill and the protection of citizens Right to Privacy in relation to information being shared and stored. The Personal Data Protection Bill was introduced over a decade ago, as early as 2006, but had since then remained covered in cobwebs until 2018. It was only in December 2019, that Mr. Ravi Shankar Prasad, the Minister of Electronics and Information technology introduced it in the Lok Sabha with significant changes that had been made to the 2018 Bill. The Bill sought to provide for protection of personal data of individuals, and provided for the establishment of a Data Protection Authority among other provisions. Drawing parallels to the legislation would highlight the European Union's (EU) proposal for the General Data Protection Regulation (GDPR)[1] which would consolidate its pre-existing data protection framework, which was based on the 1995 European Data Protection Directive[2] for protecting personal data. The GDPR came into force in the year 2018, which triggered the debate for a comprehensive legislation on data protection in India.

India's data protection legislation ought to balance the twin requisites of protecting people's privacy without negatively influencing industrial innovation and growth. The digital economy in India is expected to reach a valuation of $1 trillion dollars by 2022[3] and this reinforces the need for a legislative framework to be put in place, to regulate and protect the citizens' rights in the cyberspace. Geographical boundaries become immaterial where the theft of data is concerned.

Tracing the importance of privacy and data protection.

With the advent of the Information Technological sector in the late 1990s, and the revolutionization of the telecom industry, digital services took prominence in the economy and this led to important consequences. On one hand, due to increasing number of services becoming digitized and a surge in digital platforms, the economy became more interconnected[4] and on the other hand, policy objectives like cash

[1] European Union, "REGULATION (EU) 2016/ 679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 27 April 2016 - on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/ 46/ EC (General Data Protection Regulation)" (n.d.).

[2] European Parliament, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," Pub. L. No. Official Journal L 281, 0031 (1995), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[3] https://hbr.org/2019/12/how-india-plans-to-protect-consumer-data

[4] "Users in India to Reach 627 Million in 2019," Economic Times, https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-to-reach-627-million-in-2019-report/articleshow/68288868.cms?from=mdr.

transfers could easily be achieved through the online service delivery. The implementation of the Aadhaar scheme sought to facilitate this objective, but was subject to criticism due to several reasons. One major criticism was that this scheme was being utilised to benefit private firms for customer onboarding, which went against social-welfare. It was alleged that the storage of Aadhaar-related customer information, such as metadata about the place of authentication, constituted a serious breach of privacy.[5] Another significant point of criticism was that the scheme would vest extensive powers with the state in terms of surveillance due to the proposed ubiquitous nature of the Aadhar. It was this Aadhar debate that highlighted the privacy concerns, which manifested itself before the Supreme Court by way of several petitions challenging the validity of the impugned Act. Upon hearing the case, the five-judge bench of the Supreme Court stated that, before ruling on the infringement of privacy, there was a need to determine if there was a Right to Privacy that is guaranteed by the Constitution in the first place. Thus, the case was referred to a bench of nine judges of the Supreme Court, which resulted in the landmark ruling of ***Justice K. S. Puttaswamy and Anr. v. Union Of India And Ors***[6] in August 2017 that a right to privacy did exist under Article 21, and overturned the earlier judgement given in Kharak Singh.

The Supreme Court had, on earlier occasions protected facets of privacy in cases such as *Kharak Singh*[7] (Privacy from Police visits at night) and *PUCL v. Union of India*[8] (Telephone tapping case). However, the Puttaswamy judgement stood out in conceptualizing the concept of Privacy as a right in itself that was fundamental in nature. This perception of privacy was already in line with the principle of privacy existent in other countries, that had a framework which included data protection under its ambit.

The B.N. Srikrishna Committee Report

Around the same time, the Union Government constituted a committee to be headed by retired Supreme Court Judge, **Justice BN Srikrishna**, in July 2017, to deliberate on a data protection framework. The committee published its report in 2018, Justice Srikrishna said data privacy is a burning issue and there are three parts to the triangle. "The citizen's rights have to be protected, the responsibilities of the states have to be defined but the data protection can't be at the cost of trade and industry."[9]

In its report, a draft for the Personal Data Protection Bill 2018 was provided which eventually formed the basis for the bill that was tabled in the Lok Sabha.[10]

[5] Madhav Khosla and Ananth Padmanabhan, "The Aadhaar Challenge: 3 Features That Put Constitutional Rights at Risk," ThePrint, June 27, 2018, https://theprint.in/opinion/the-aadhaar-challenge-3-features-that-put-constitutional-rights-at-risk/75576/.

[6] WRIT PETITION (CIVIL) NO 494 OF 2012

[7] AIR 1963 SC 1295

[8] (1997) 1 SCC 301.

[9] https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-committee-submits-report-on-data-protection-herere-the-highlights/articleshow/65164663.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppstwhich provided for the rationale behind a legal framework

[10] Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, "Draft Personal Data Protection Bill, 2018," https://www.thehinducentre.com/resources/article245

Analysing Informational Privacy in light of Puttaswamy Judgement:

The landmark ruling in the *Puttaswamy* judgment, spanning 547 pages, contains six opinions and a lot of interesting observations. The judgement, in its plurality opinion recognizes "Informational privacy" as a part of the right to privacy guaranteed under Art. 21. The Supreme Court held that information about a person and the right to access that information also needed to be given the protection of privacy. It stated that every person should have the right to control commercial use of his or her identity and that the "right of individuals to exclusively commercially exploit their identity and personal information, to control the information that is available about them on the internet and to disseminate certain personal information for limited purposes alone" emanates from this right.

This was the first time that the Supreme Court had expressly recognised the right of individuals over their personal data.

Hon'ble Justice Chandrachud, in his plurality opinion, opined that, "the right to privacy is not independent of the other freedoms guaranteed by Part III of the Constitution. It is an element of human dignity and is an inalienable natural right."

He further argued for the importance of the informational aspect of privacy and its connection with human dignity and autonomy, and rejected the argument of privacy as an elitist construct. During the course of his opinion, Chandrachud J. made several observations about privacy in the digital economy, dangers of data mining, positive obligations on the State, and the need for a data protection law.

Nariman J. too endorsed Gary Bostwick's conceptual understanding of privacy as encompassing "repose, sanctuary, and intimate decision". He classified the right into three categories of which one highlights the information privacy which captures unauthorised uses of personal information.[11] Considering the potential of Social media and World Wide Web, Justice Kaul identified the need for the "right to be forgotten".[12] He was of the view that, "the right to be forgotten refers to the ability of individuals to limit, de-link, delete, or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant, or anachronistic".[13] The Right to privacy must allow for an individual to have control over his personal information, which meant that if he wishes to delete his information then it must get erased from the cyberspace. However, the data protection laws across the world only go so far as to recognize the right to be forgotten but do not recognize the right to be deleted from cyberspace. The line of distinction lies at the point where "right to be forgotten" only goes so far as not appearing as the "top result" on cyberspace, whereas the "right to be deleted" extends to providing an

61526.ece/binary/Personal_Data_Protection_bill,2018_0.

[11] An Analysis of Puttaswamy, https://www.ssoar.info/ssoar/bitstream/handle/document/54766/ssoar-indrastraglobal-2017-11-bhandari_et_al-An_Analysis_of_Puttaswamy_The.pdf?sequence=1#:~:text=On%2024th%20August%202017%2C%20a,the%20constitutional%20right%20to%20privacy.

[12] Per Kaul at Para 64, Puttaswamy v. UOI (2017) 10 SCC 1

[13] Government of India, Report: Committee on A Free and Fair Digital Economy Protecting Privacy, Empowering Indians (Union Ministry of Electronics & Information Technology, 2017).

individual with the control over permanent deletion of information from the cyberspace. The inclusion of the aspect of informational privacy by the Court paves the way for a variety of claims that could arise. However, without a legal framework in place that allows for data protection, the efforts to protect this right will remain futile. Although the exact boundaries of this right will continue to develop on a case-by-case basis, it is undisputed that there is a need for a legislation. In the absence of a defined legislation, decisions of cases will differ based on the factual circumstances at hand and the judicial interpretation. For instance, does the efficiency of having a meta-database of information on all citizens trump the autonomy of those who resist its adoption? Can an individual's "right to be forgotten" on the Internet override the open information needs of many others? An answer to these questions would only be good in law if a Data Protection Act is in place.

Scope and Major Features of the proposed Data Protection Bill:

The bill provides a legal framework for the collection and use of personal information. It governs the processing of personal data by the Government, Companies in India and Foreign companies dealing with processing of data of individuals in India.

The Bill categorises certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the government, in consultation with the Authority and the concerned sectoral regulator.

It imposes certain obligations upon data fiduciaries in the way they process the data available to them, in a transparent and accountable manner. It is ensured through implementing security safeguards, instituting grievance redressal mechanisms to address complaints of individuals. Additionally, mechanisms for parental consent and age verification are mandated when processing personal data of children that are sensitive.

The Bill creates a set of rights and responsibilities for individuals including the right to obtain confirmation from fiduciaries on processing of their data, seek correction of inaccurate, incomplete, or out-of-date personal data; have personal data transferred to any other data fiduciary in certain circumstances, and restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn.

- It lays down grounds for processing of personal data, which is possible only if an individual consents to it, except under certain circumstances which include instances where the State requires it for providing benefits to an individual, or for legal proceedings, or to respond to a medical emergency.

  It allows for Social Media Intermediaries to facilitate online interaction between users and allow for sharing of information. These intermediaries have a notified threshold, and those who would have an impact on electoral democracy or public order also have obligations thrust upon them including making a provision of a voluntary user verification mechanism for users in India.
- The bill proposes to create a Data Protection Authority (DPA) for making regulations and enforcing the legal framework, which may take steps to protect individuals' interests,

prevent the misuse of any personal data and to ensure complying with the Bill.

- The DPA would consist of a chairperson and six members, with at least 10 years' expertise in the field of data protection and information technology. It also provides appeal provisions for the orders provided by the DPA, which would be directed to the Appellate Tribunal, and appeals upon orders of the Appellate Tribunal would be heard by the Supreme Court.
- The bill also vests substantive standard-setting powers with the central government and tasks the DPA with enforcing the same.
- While the Bill allows for transferring of data for processing outside of India, if explicitly consented to by individuals, these are restricted to a certain extent by way of conditions. Such sensitive personal data would, however, continue to be stored in India.

- **Exemptions from the Bill:** The union government can exempt any of its agencies from the provisions of the Act:

(i) in interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states

(ii) for preventing incitement to commission of any cognisable offence (i.e. arrest without warrant) relating to the above matters. Processing of personal data is also exempted from provisions of the Bill for certain other purposes such as:

➔ prevention, investigation, or prosecution of any offence, or

➔ personal, domestic, journalistic purposes.

➔ However, such processing must be for a specific, clear and lawful purpose, with certain security safeguards.

- Offences under the Bill would incur monetary penalties, for instance, processing or transferring personal data in violation of the Bill is punishable with a fine of Rs 15 crore or 4% of the annual turnover of the fiduciary, whichever is higher. A failure to conduct a data audit, is punishable with a fine of five crore rupees or 2% of the annual turnover of the fiduciary, whichever is higher. This offense is cognizable, i.e., an offense in which an arrest can be made without a warrant and nonbailable.
- Re-identification and processing of de-identified personal data without consent is punishable with imprisonment of up to three years, or fine, or both.

- The Bill amends the Information Technology Act, 2000 to delete the provisions related to compensation payable by companies for failure to protect personal data.[14]

Impact of the proposed Bill on the Indian Economy:

The proposed data protection bill would therefore provide a preventive framework that would apply to existing methods of data collection and the practices of usage currently being followed. It imposes obligations upon businesses that collect and use data of its consumers while providing a higher threshold of consumer-rights in relation to their data that is stored. Since the provisions of the legislation mandates the meeting of the outlined requirements to collect any sort of personal data, it would require even the small grocery stores and mom-and-pop stores that have been following simple data collection methods, and the erstwhile larger business complexes using a more sophisticated range of data

[14] https://prsindia.org/billtrack/the-personal-data-protection-bill-2019

collection involving algorithms and datasets to re-evaluate their methodologies.

The legislation would thus have a notable impact on the country's economy. Although India is home to a myriad of multinational corporations, and houses several national and international companies, the majority of the business sector is comprised of small businesses and entrepreneurial start-ups that are small in scale. As per an annual report of the Ministry of Micro, Small and Medium Enterprises, "of the estimated number of 633.92 lakh [63.39 million] enterprises, only 4000 enterprises were large and thereby out of the MSME [micro, small, and medium enterprise] Sector."[15] Therefore the major impact of the proposed legislation would affect small businesses.

It is therefore pertinent that personal data protection does not negatively influence industrial innovation and growth. Further, the Indian landscape is predominantly rural, in the sense that digital connectivity still a novel concept for a large section of the populace as against the urban metropolitans who have adapted to the digital ecosystem. Rural population (% of total population) in India was reported at 65.53 % in 2019, according to the World Bank collection of development indicators, compiled from officially recognized sources.[16]

The remotest corners of India still do not have basic infrastructural facilities including proper roads, hospitals or schools, and sanitation facilities. Under such circumstances, a well-laid out plan to implement the existing digitization plans should be closely followed up with bringing awareness and educating the rural population of importance of Data Privacy and protection and the online hazards that could likely occur and in such cases, of the remedies available to them.

As with most legislations, the main problem that could hinder the efficiency of the proposed legislation would arise during the process of implementation. Implementing a uniform legislation protecting the rights of such a diverse and dense population with contrasting economic and social backgrounds would be a challenge in itself. Furthermore, the threat to data privacy of citizens could occur from both state as well as non-state actors. When the State joins with private entities, in the absence of such a protection law, people would fall prey to more serious concerns than mere target advertising.

Conclusion:

At this time and age, in order to assess a country's governance, the threshold includes how well a State is able to empower its citizens digitally while providing them effective remedies in case their privacy is violated and their data is threatened.

From an economic and trade standpoint, India is a developing country that is rapidly digitizing its economic affairs, and requires a legal framework needs to be set in place that is at par with foreign jurisdictions. India's law has to be suitable enough to be considered adequate in the EU's directory in terms of its Data Protection Directive. If India succeeds, trade would become much

[15] Ministry of Micro, Small and Medium Enterprises, Government of India, "Annual Report 2017-18 - Ministry of Micro, Small and Medium Enterprises," (New Delhi, India, 2018), https://msme.gov.in/sites/default/files/MSME-AR-2017-18-Eng.pdf., 23.

[16] https://tradingeconomics.com/india/rural-population-percent-of-total-population-wb-data.html

easier with the EU and its member states and otherwise cumbersome procedures that are mandated could be avoided completely.

It is acknowledged that there are several challenges that are existing with regards to the digital cyberspace, and they continue to grow as the world becomes increasingly digital. Governments, Private entities, terrorist organizations and other anti-social elements tend to continuously scrutinize the online realm. In this era, the most powerful weapon in the hands of your enemy would be your personal data that is made available to them through the cyberspace. Without proper protection, not just individuals but an entire economy could be in danger.

Therefore, while implementing the data protection bill, these factors ought to be kept in mind and the implementation process should consider and evaluate all forms of loopholes and lacunae in the law and strategize mechanisms to make the law as watertight as possible to protect its citizens data privacy.

*****