A UNIT OF
LAW LABORATORY

MAY 2022

Law Laboratory Research Journal of Law & Socio-Economic Issues

ISSN: 2583-0783

VOLUME 1 | ISSUE 3

WWW.LAWLABJOURNAL.IN

RIGHT TO PRIVACY AND DATA PROTECTION IN INDIA

- *Shirin*[1]

ABSTRACT

The Constitution recognizes an inherent right to privacy under Article 21. This fundamental right throws a long shadow on Indian law, affects legislative and judicial activity, and serves as a check on legislative and executive action. In addition to its consequences for public law, this right has inspired the establishment of a tortious right against the breach of privacy and the interpretation of rights inherent in laws governing consumer protection, health, information technology, and telecom licenses. With the advent of technology into our daily lives, this right has gained much more importance than before. The world of internet and social media has given rise to data privacy issues since the nature of medium is such that it is a child's play to exploit personal data. Despite the formal recognition of right to privacy as a fundamental right, we lack a wholesome statute on same. Data protection is not a total grey area in India, however the fact that the law is scattered in various statutes makes it largely ineffective. Hence, this research paper goes on to analyze the need for such a law in India and as to how the bills with regard to same have been received over time.

Keywords: Constitution, Rights, Data, Protection, Fundamental Right

INTRODUCTION

The concept of privacy dates back to the dawn of human civilization. However, the idea of privacy is difficult to grasp. The term "privacy" has taken on a variety of meanings for different academics, and those definitions shift as society itself does. It is possible to trace back its history by looking at arguments in the Constituent Assembly, when privacy and secrecy were debated. It is clear from the debates in the Constituent Assembly that the right to privacy was purposefully omitted from the Constitution. Legislators' motivations for doing this remain a mystery. Post-independence India's Constitution does not explicitly acknowledge the right to privacy, but

[1] SRM University, Sonipat, Delhi

precedents in the courts have allowed it to develop. In the instance of Kharak Singh[2], it was acknowledged for the first time. The "Indian Evidence Act, the Information Technology Act, the Indian Penal Code, Criminal Law, Indian Telegraph Act, Indian Easement Act, and Family Law" are all examples of legislation that include provisions that pertain to privacy. In this article, we've explored these laws in great length. There are many different types of privacy that have developed through time: the privacy of one's physical space, one's bodily identity and information, and the privacy of one's personal preferences. And this right is even more important to safeguard in the digital age we live in today. There has been some discussion over the impact of social media on privacy rights in today's digital age. To that end, we'll take a close look at the laws in place to safeguard individuals' privacy, and whether or not they go far enough to address concerns like invasions of privacy, which are protected by Article 21[3].

DEFINITION OF PRIVACY RIGHTS

When discussing its definition, the term "privacy" is difficult to comprehend. It has been interpreted in several ways. "Right to privacy," according to Black's Law Dictionary[4], includes "various rights recognized as inherent in the concept of ordered liberty." These freedoms protect people's right to fundamentally choose how they want to live their lives and interact with their families, other people, and their interpersonal connections and activities. It's also been said that privacy is about a person's lawful claim to decide how much of himself he wants to disclose with others, as well as his control over when, where, and under what conditions he does so. It refers to his unrestricted ability to engage or not participate in whatever way he chooses. It also refers to the freedom of the individual to decide what information about him or her is made public; he or she is the exclusive owner of that information. A person's "right to be left alone," on the other hand, signifies that he or she is entitled to privacy. All the rights that have been recognized as inherent in the idea of ordered liberty fall under the umbrella phrase "right to privacy." Freedom of assembly and free speech may be seen as essential components of the right to privacy, since they allow people to do both.

[2] *Kharak Singh* v. *State Of UP*, 1964 SCR (1) 332.
[3] The Constitution of India, 1950.
[4] "Privacy" Black's Law Dictionary.

RIGHT TO PRIVACY: CONSTITUTIONAL ESSENCE

According to Article 21[5], which covers our essential rights, the right to privacy is one of those rights. This was supported by a 9-j SC bench in *Justice K.S. Puttaswamy* v. *UOI*[6], which issued a landmark decision on August 24, 2017, stating that "the right to privacy" is an essential component of our Constitution.

One may be forgiven for wondering why a bench of nine judges was tasked with deciding whether or not the “right to privacy” falls within Art 21 of our Constitution. In 2017, a 5-j bench of SC made the announcement that they wanted a 9-j panel to first assess whether “the right to privacy” is a fundamental right before deciding on the primary issue regarding Aadhaar. The case that included the Aadhaar card and “right to privacy” was being considered by the court. The A.G. in Aadhaar matter stated that even though previous rulings had acknowledged the “right to privacy”, they did not explicitly recognize it like in Kharak Singh[7] and MP Sharma rulings[8]. As a result, a 9-j bench must be constituted to analyze whether “the right to privacy” qualifies as a basic freedom. A flurry of legislative initiatives to pass Personal Data Protection laws were triggered by the SC's broad interpretation.

STATUTORY PROVISIONS ON DATA PRIVACY IN INDIA

The sharing or receiving of personal information in spoken, writing, or electronic form is not protected by a stand-alone legislation in India. Although there are safeguards, they are spread over a variety of laws, regulations, and policies.

IT (Amendment Act of 2008) and IT (Sensitive Personal Data or Information) Rules of 2011 include the most significant clauses. For online trade and cybercrime, this is India's most important law in the country. Because of their name, SPDI Rules only cover data and information sent electronically; they do not cover data and information obtained via non-digital methods.[9]

All rules and regulations pertaining to the IT Act, 2000 were devoid of the safeguards and restrictions necessary to secure sensitive personal information submitted electronically when it first went into effect on October 17, 2000. The Information Technology Bill, 2006 was finally

[5] The Constitution of India, 1950.
[6] (2017) 10 SCC 1.
[7] *Supra note* 1.
[8] *MP Sharma* v *Satish Chandra*, (1954) 1 SCR 1077.
[9] “Puttaswamy v. Union of India (I)”, Global Freedom Express (July 13, 2022) https://globalfreedomofexpression.columbia.edu/cases/puttaswamy-v-india/

introduced as a result, and the IT (Amendment) Act, 2008 followed, with its provisions taking effect on Oct 27, 2009. It inserted Sec 43A in IT Act, as per which, if: "a corporate body possesses or deals with any sensitive personal data or information, and is negligent in maintaining reasonable security to protect such data or information, which thereby causes wrongful loss or wrongful gain to any person, then such body corporate shall be liable to pay damages to the person(s) so affected."

Also, Sec 72A, as per which: "the punishment for disclosure of information in breach of lawful contract and any person may be punished with imprisonment for a term not exceeding three years, or with a fine not exceeding up to five lakh rupees, or with both, in case disclosure of the information is made in breach of lawful contract." Punishment for it is stated in Sec 72. It says that: "any person who, in pursuance of any of the powers conferred under the IT Act Rules or Regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned, discloses such electronic record, book, register, correspondence, information, document or other material to any other person, shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Rs 1,00,000, (approx. US$ 3,000) or with both." Anyone who commits an offense or violation outside of India shall be held to the same standards as anyone who commits an offense or violation in India. This is stated in Section 75 of the Act.[10]

The IT Act and Rules' reach and breadth, however, are constrained. Most of the rules only cover "sensitive personal data and information" that is gathered using "computer resources." Only a tiny portion of the restrictions may be enforced by consumers, and the provisions are only applicable to business organizations that carry out automated data processing. Data localization is not covered, which was the main worry and the basis for the Indian government's decision to prohibit Chinese applications. India needs a thorough data privacy legislation to overcome these restrictions.

PERSONAL DATA PROTECTION BILL, 2019

The SC's 9-judge bench upheld the "right to privacy" in *K.S. Puttaswamy v. UOI*[11] "right to privacy case" in August 2017. According to Art 21[12], the Court highlighted the rights to life and

[10] Ibid.

[11] *Supra note* 5.

[12] The Constitution of India, 1950.

personal freedom. The Indian government established a Committee of Experts, headed by Justice B.N. Sri Krishna, to investigate data privacy problems in India during the case. This report and draft Personal Data Protection Bill were given to Ministry of Electronics and Information Technology in July 2018 after the white paper's open consultation. Expert Committee suggestions and stakeholder input were used to draft Personal Data Protection Bill 2019. A further set of three critical elements is outlined in the text:[13]

- Personal data protection is a crucial component of "informational privacy and right to privacy."
- As the digital economy has grown, people are increasingly using data as a vital form of interpersonal connection.
- The establishment of a collective culture that promotes a free and equitable digital economy, respects the privacy of individuals' personal information, and ensures these things is necessary to ensure empowerment, advancement, and innovation through digital governance and inclusion, as well as matters related or incidental to those.

The above-mentioned bill was developed following extensive engagement and consultation with a variety of stakeholders, including Indian law enforcement, which opposes "data colonialism" by significant Western technology companies like Google and Facebook and wants access to data stored in the US for national security investigations. As a replacement for Sec. 43-A of the IT Act of 2000, this bill would eliminate all provisions pertaining to company liability for data breaches and privacy violations.

Before processing personal data, data fiduciaries and processors are obliged by law to get permission from data principals. Regardless of whether they are representatives of the State, a corporation, a government agency, or an individual, whomever decides the reason for and the method of processing personal data. An individual who administers personal data on behalf of a data fiduciary is known as a data processor. This includes the government, corporations, people, and other legal bodies. Data collectors must now comply with new reporting standards, such as the obligation to get parental or guardian consent before collecting children's data. The persons whose data is being gathered, or the "data principals," are also given rights under the law.

In the event that the legislation is passed, data fiduciaries and data processors will need to:[14]

- Inform the data principals of the collecting of their data.

[13] ORF Technology and Media Initiative, "The Personal Data Protection Bill 2019: Recommendations to the Joint Parliamentary Committee" (ORF Special Report No. 102, March 2020).

[14] *Supra note* 12.

- Request permission before processing a data subject's personal information.
- Gather and maintain proof that a notification was made and permission was obtained.
- Enable users to access, amend, and delete their data as well as withdraw their permission.
- Permit customers to transmit their data to other firms, including any conclusions drawn by such businesses from that data.
- alter organizational procedures to safeguard data, such as by adhering to privacy
- by-design principles and putting in place security measures

Additionally, the law stipulates that all "sensitive personal data" must be kept in India and that "essential personal data" cannot be sent outside. As it would disrupt market-driven choices and compel businesses to utilize local data storage service providers, this has been condemned as being protectionist.

CRITICISM OF THE BILL

Since its inception, the Bill has come under scrutiny for being skewed in favor of the company collecting the data and for potentially having serious problems with user rights. Globally, data privacy laws have properly given users primary control over data gathering and permission. The laws provide users the freedom to choose how and when their data may be gathered, processed, kept, and shared by providing them with the necessary rights and ability to do so. Despite explicitly granting people certain rights and safeguards, the DP Bill makes it near impossible for users to exercise their rights.

The DP Bill makes it more difficult for users to exercise their right to withdraw permission by declaring that if the withdrawal is made without a "valid cause," the data subject would be responsible for any resulting legal ramifications. This eliminates the individual's ability to exercise a right to withdraw consent by making it prohibitively difficult to exercise, as well as unnecessary demanding and burdensome. This is complicated further by the fact that the legislation doesn't specify what constitutes a "good cause" or the nature and scope of the legal repercussions that are intended by the provision. In addition, the legislation establishes circumstances in which it permits the processing of data without the data principals' permission. Given the many layers and complexities that technological processes and products currently have, the regulations that allow for these grey zones simply make things worse for unwary consumers.

CONCLUSION

In the current era of globalization, it has become much easier than it was ever earlier to save and transfer data. However, this has had not only positive results but also several negative implications like the infamous WhatsApp data leak case. It has become easier to exploit data and breach the privacy of the masses. Since it is a relatively new concern, there is no concrete law on the topic. The Personal Data Protection Bill of 2019 was introduced in Parliament as an attempt to bring in a comprehensive Centre level law on the issue but the same has not yet become a reality. Data privacy is extremely important in all spheres of life but most importantly in the corporate world. India needs to take the issue seriously as it is not at par with other leading nations of the world when it comes to data privacy issues.