

**INTERNATIONAL JOURNAL OF LAW  
MANAGEMENT & HUMANITIES**  
**[ISSN 2581-5369]**

---

**Volume 4 | Issue 1**

**2021**

---

© 2021 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com>)

---

This Article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in International Journal of Law Management & Humanities after due review.

In case of **any suggestion or complaint**, please contact [Gyan@vidhiaagaz.com](mailto:Gyan@vidhiaagaz.com).

---

**To submit your Manuscript** for Publication at **International Journal of Law Management & Humanities**, kindly email your Manuscript at [submission@ijlmh.com](mailto:submission@ijlmh.com).

---

# An Analysis of Data Protection and Privacy Laws in India

---

NIVEDITA BARAILY<sup>1</sup>

## ABSTRACT

*Data Protection and Privacy are two interrelated issues regarding internet governance. Data Protection is a legal instrument to ensure the privacy of citizens. Privacy can be defined as a right to control one's personal information and data and disseminate the same according to their will and choice. Right to privacy has been recognised as a fundamental right in India with the help of various judicial decisions and a legal right with the help of statutes. It has also been recognised in international instruments such as the Universal Declaration of Human Rights, 1948 and the International Covenant on Civil and Political Rights, 1976 among many other international and regional human rights conventions. The UN Special Rapporteur was appointed in July 2015 for the Right of Privacy in Digital Age which reflects the increasing importance of privacy in global digital policy and the need for recognising and addressing privacy rights issues in both international and national levels. India as of 2020 does not have a dedicated law on data protection and privacy and hasn't adopted any international instrument on the same. Specific provisions of the Information Technology Act, 2000 (IT Act) can be applied to data protection and privacy, however, they are in no way exhaustive. The Personal Data Protection Bill, 2019 was introduced in the Lok Sabha on December 11, 2019 by the Minister of Electronics and Information Technology, Mr. Ravi Kumar. The Bill not only seeks to ensure protection of personal data but also to establish a Data Protection Authority for the same.*

**Keywords:** *Data Protection, Privacy, Information Technology, Personal Data Protection Bill*

## I. DATA PROTECTION AND PRIVACY UNDER THE CONSTITUTION OF INDIA

The Constitution of India is the most supreme law of the land. It is an undisputed fact that our Constitution is a living document and it moulds itself with the changing environment. Amongst various other rights, it recognises the right to privacy as a fundamental right falling under the canopy of Article 21. Article 21 states that “no person shall be deprived of his life

---

<sup>1</sup> Author is a student at University of North Bengal, India.

and personal liberty except according to the procedure established by law.”<sup>2</sup> Right to privacy is related to one’s life and liberty, hence, it is protected by Article 21.

In *R. Rajagopal v. State of Tamil Nadu*,<sup>3</sup> also known as “Auto Shanker Case”, the Supreme Court has expressly held that the right to privacy or the right to be let alone is guaranteed under Article 21 of the Constitution. A citizen has the right to safeguard the privacy of his own, his family, education, marriage, procreation and motherhood among other matters.

In *State of Maharashtra v. Madhulkar Narain*,<sup>4</sup> it has been held that the right to privacy is available even to a woman of easy virtue and no one can invade her privacy.

In *People’s Union for Civil Liberties v. Union of India*,<sup>5</sup> popularly known as “Phone Tapping Case”, the Supreme Court held that telephone tapping is a serious invasion of an individual’s right to privacy which is part of right to life and personal liberty under Article 21 of the Constitution and it should not be resorted to by the State unless there is an interest or public emergency or public safety. The Indian Telegraph Act 1885 and the Information Technology Act 2000 allow the government to conduct surveillance activities based on certain criteria that is in the interests of the sovereignty and integrity of India, security of the state, friendly relations with foreign states, public order or for prevention of incitement of the commission of an offence. These grounds are based on reasonable restrictions to free speech contained in the Constitution of India.

Eventually, the right to privacy has been recognised as a fundamental right in the year 2017. *Justice K. S. Puttaswamy (Retired.) and another. v Union of India and others*<sup>6</sup>, is a landmark judgment of the Supreme Court of India, which holds that the right to privacy is protected as a fundamental constitutional right under Articles 14, 19 and 21 of the Constitution of India. It was held that protection of privacy can not only be held against the state but also against the non-state entities in this age of technological development. However, just like any other fundamental right, the right to privacy is also not an absolute right and any invasion of the same by any state or non-state actor must satisfy the triple test of legitimate aim, proportionality and legality.

The Supreme Court, therefore, facilitated in making legal framework for privacy protections in India. The judgment of this case establishes that right to privacy is a fundamental right, inalienable and intrinsic to human liberty and dignity protected under Article 21 of the

---

<sup>2</sup> Constitution of India, art.21.

<sup>3</sup> *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.

<sup>4</sup> *State of Maharashtra v. Madhulkar Narain*, (1991) AIR 207.

<sup>5</sup> *People’s Union for Civil Liberties v. Union of India*, (1997) AIR 568.

<sup>6</sup> *Justice K. S. Puttaswamy (Retired.) and another. v Union of India and others*, (2017) 1 SCC 10.

Constitution.

## **II. DATA PROTECTION, PRIVACY AND THE INFORMATION TECHNOLOGY ACT, 2000**

The Information Act, 2000 is based on United Nations Model Law on Electronic Commerce. It contains the following provisions regarding data protection and privacy. **Section 43A** provides for compensation in the event one is negligent in using reasonable security practices and procedures (RSPP) in protecting sensitive personal data and information (SPDI) and this results in a wrongful gain or wrongful loss.<sup>7</sup>

'Reasonable security practices and procedures' mean security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices as may be prescribed by the Central Government. This means that if the parties, for instance, an employer and an employee - agree on the RSPP to be adopted, the rules of the government would not apply.

**Section 2(o)** defines data as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.<sup>8</sup> **Section 2(v)** defines information as any data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer-generated micro fiche.<sup>9</sup>

**Section 72A** provides for criminal punishment if, in the course of performing a contract, a service provider discloses personal information without the consent of the person concerned or in breach of a lawful contract and he or she does so with the intention to cause, or knowing he or she is likely to cause, wrongful loss or wrongful gain.<sup>10</sup>

**Section 72** prescribes criminal punishment if a government official discloses records and information accessed by him or her in the course of his or her duties without the consent of

---

<sup>7</sup> Information Technology Act, 2000, § 43A.

<sup>8</sup> Information Technology Act, 2000, § 2.

<sup>9</sup> Information Technology Act, 2000, § 2.

<sup>10</sup> Information Technology Act, 2000, § 72A.

the concerned person or unless permitted by other laws.<sup>11</sup>

**The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011** list the type of personal information which may be construed as sensitive personal data or information, and includes: (i) password; (ii) financial information; (iii) health parameters (including physical, physiological and mental health conditions and medical records or history); (iv) sexual orientation; and (v) biometric information.

The IT Rules has also defined the termed ‘personal information’ as any such information that relates to a natural person capable of identifying such person.

**Section 75** provides that this Act shall apply to an offence or contravention committed by any person outside India if the act or conduct constituting an offence or contravention involves a computer, computer system or computer network located in India.

### **III. PERSONAL DATA PROTECTION BILL, 2019<sup>12</sup>**

This Bill seeks to govern **personal data processing** by government and companies whether Indian or foreign that deals with personal information of individuals in India. Personal data is the data, character traits and attributes that help to identify a person. The Bill has classified some of the personal data as sensitive personal data. Some of the sensitive personal data are financial data, biometric data, religious beliefs and any other category as specified by the Government.

There are various types of **rights** sought by this Bill that are conferred on the individual. Every individual has the right to obtain information regarding the confirmation from the fiduciary on whether their data has been processed. It also gives the right to correct their incomplete, inaccurate or obsolete personal data. In certain circumstances, the individuals can also transfer their personal data from one fiduciary to another. A fiduciary’s right to disclose personal data can be restricted if it is no longer necessary or if the consent has been withdrawn.

A **data fiduciary** is any entity or individual who decides the means and purpose of processing personal data. Such processing will be subject to certain purpose, collection and storage limitations. For instance, personal data can be processed only for specific, clear and lawful purpose. In order to ensure the rights of the individuals, all data fiduciaries are entitled

---

<sup>11</sup> Information Technology Act, 2000, § 72.

<sup>12</sup> The Personal Data Protection Bill, PRS LEGISLATIVE RESEARCH, (January 29, 2021, 12:52 pm) <https://www.prsindia.org/billtrack/personal-data-protection-bill-2019>

take transparency and accountability measures such as implementing security measures to prevent the misuse of personal data; constituting a redress mechanism to tackle the complaints of the individuals; also take extra measures to process sensitive personal information of children such as age verification and parental consent.

Certain sensitive personal data of individuals can be transferred outside India if explicitly consented by the concerned individual subject to certain conditions. However, it will continue to be stored in India. Some data that are categorised as critical data can only be processed in India.

The Bill also seeks to establish a **Data Protection Authority** to take protective measures regarding the personal data of the individuals, prevent misuse of the same and to ensure that this bill is complied with. The Authority is sought to comprise of a Chairperson and six other members with a minimum of 10 years' experience in the field of data protection and information technology. Orders made by the Authority can be appealed to the Appellate Tribunal and appeals from the Appellate Tribunal shall lie to the Supreme Court.

This Bill empowers the Central Government to provide certain exemptions to any of its agencies from the provisions the proposed Act in the interests of nation's sovereignty, security and integrity, and friendly relations with other nations or to prevent incitement of commission of a cognisable offence regarding the aforementioned interests.

If any data fiduciary processes or transfers any personal data in contravention of this Bill, shall be punishable with a fine of Rs. 15 crores or 4% of the annual turnover of the fiduciary, whichever is higher. In case of failure to conduct an audit of data, the data fiduciary shall be punishable with a fine of Rs. 5 crores or 2% of the annual turnover of the data fiduciary, whichever is higher. 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 seeks to amend the provisions of the Information Technology Act, 2000 that relates to the compensation payable by companies for failure to protect personal data.

#### **IV. CONCLUSION**

India as of today does not have any exhaustive legislation in the field of Data Protection and Privacy. The Constitution of India has always been a living entity and a dynamic body of rules and regulations. It has always been amended in the manner that facilitates development and change in tandem with the changing mentality and technological advancement. Being the protector of the Constitution, the Supreme Court via its landmark and relevant judgments has

made the right to privacy a fundamental right. In this digital age, protecting one's personal data is of paramount significance, therefore, the right to privacy also extends to protection of personal data and information.

The Information Technology Act, 2000 and the IT Rules, 2011 together have provided legal protection to data and privacy. Although, the Act does not sufficiently deal with data protection and privacy, the Rules that have been supplemented to the Act in order to extend protection, as far as possible, to data protection and privacy.

The proposed Bill aims at protecting personal data and information of the citizens of India. It also aims at protecting critical personal information of the citizens of India by allowing its process to be only in India. However, the exemptions of this Bill provide immunity to the agencies of the Central Government as per the discretion of the latter. This provision has a tendency to give arbitrary powers to the Central Government.

\*\*\*\*\*