LEGALFOXES LAW TIMES

# Right to Privacy and Data Protection Bill, 2019

By: Aditya Narayan Bej & Gyaninee Pattnaik, Purbasha Pattnaik

## Introduction

The right of individuals to decide the precise context and scenario where they should disclose peculiar private data is considered confidential. Known throughout the development of a long history, the term, Privacy comes from the Latin word "privates", meaning separate, limited, personal, or otherwise. However, the main grip on the definition lies in the context, the community, and the individual that is what is considered to be confidential and what is legally protected as confidential.

**Legal Viewpoints on Privacy:**

This right to privacy means the management of information or activities relating to you. In India, most people understand Privacy only in terms of gender, wealth, and sometimes passwords as well. Privacy is considered a tort. Until 1960 the privacy was not considered a fundamental right under the Constitution of India nor a legal right under any other law. The Constitutional right to privacy prevents unauthorized search and fainting. The idea that privacy is not a basic requirement in our society was maintained in 1954 by an eight-judge bench in the case of *M. Sharma v. Satish Chandra*[1]. Privacy was not considered a fundamental right, the case of while working with the power to search and retrieve documents from the Dalmia group, has revoked the existence of a right to privacy on the grounds that the founders of the Constitution did not make a concerted effort to include the right to privacy in the Constitution. In the case *of Kharak Singh v. State of Uttar Pradesh*[2] wherein Justice Subbarao, after a night-long house search ban, declared that the "Right to Privacy was still an essential human right in that provision was not enshrined or declared a fundamental right under the Indian Constitution.

**Elucidation of Right to Privacy via Case laws**.

- In *R. Rajagopal v. The State of Tamil Nadu*[3] The apex Court, in its very first instance, directly linked the right to privacy to Article 21 of the Constitution and went on to say: "

[1] AIR 1954 SCR 1077
[2] AIR 1964(1) SCR 332
[3] 1995 AIR 264, 1994 SCC (6) 632

including family, marriage, childbearing, motherhood, childbearing, education, and much more".

- In *Ram Jethmalani & Ors v. Union of India & Ors*[4] Supreme Court categorically held the requirement of the state not to make public any private information about an individual, which would violate the person's privacy. A nine-judge panel of the Supreme Court on 24 August 2017 declared privacy as an integral part of Part III of the Indian Constitution, which shall include our basic rights, ranging from rights related to equality (Articles 14 to 18); freedom of speech and Article 19 (1) (a)); freedom of movement (Section 19 (1) (d)); protection of health and personal freedom (Article 21) and others. These fundamental rights are inalienable and may not be granted or revoked by law. In addition, all administrative rules and regulations must be complied with.
- Government proposed biometrics-based ID system was challenged by retired High Court Judge Puttaswamy making the biometrics responsible for access to government services and benefits. The government has requested that the Constitution does not provide any direct protection of the right to privacy. Confidentiality is considered by the court, as in the case of essential freedoms or freedoms guaranteed under Article 21 which states: "No one shall be arbitrarily deprived of his life or freedom except by the law established by law".
- In 2017 after the passing of *K.S Puttaswamy v. The Union of India*[5], which overturned Khakak Singh's case, ruled that privacy rights were a fundamental right.

**Privacy as Control over Information and Data Protection:**

Only the information owner decides the disclosure of the information. For example, confidentiality can be considered critical if an employee working for a government tax office looks at the records of anyone other than his or her own interest as there is no data protection authority in India. In addition, the IT Act of 2000 contains various provisions that allow for the termination, employment and removal of digital definitions. It also provides the collection and monitoring of traffic data. It also allows governments to set national encryption standards. Projects such as the Central Monitoring System, NATGRID, Phone & Internet Interception used by the police make State employment very high.



**The Personal Data Protection Bill, 2019**

The Minister of Technology and Information Technology, Mr Ravi Shankar Prasad, on December 11, 2019, introduced the Personal Data Protection Bill, 2019 in Lok Sabha. The Bill strives to provide for the protection of personal information and establishes the respective Data Protection Authority respectively. The framework of the Personal Data Protection Bill is currently being considered. To date, the current data protection framework is enshrined in the Information

[4] WRIT PETITION (CIVIL) NO. 176 OF 2009
[5] WRIT PETITION (CIVIL) NO. 494 OF 2012

Technology Act, 2000 ("IT Act") and its subordinate laws, most importantly Information Technology with sound security procedures and strict personal data and information laws, 2011 (" IT Rules "). The bill is a mirror and seems to allow for parts of the Federal data privacy mechanisms integrated with the data management system in the United States. This perhaps demonstrates a completely different understanding of how human rights are related to the protection of online speech and data privacy. The U.S, it views online data protection and information as less of a burden on the government than, for example, many European Union counterparts. India as a global leader in democratic data management has high levels of international internet policy participation - that is, work in the UN General Assembly and elsewhere.

**Applicability and Provisions of the Bill**

To avoid any important data to be copied to a country, the target country must use it to protect adequate privacy of the data and not to prevent access to Indian law from that data. The Bill regulates the processing of personal data based on character traits, personal attributes, biometrics, gender status, religious beliefs, etc.

a) government,

b) companies based in India, and

c) Foreign companies that process personal information of Indian people.

Data relating to features, or proprietary features, which can be used to identify a person, is called Personal Data. The bill excludes certain particular data such as delicate personal data, including financial data, biometric data, caste, religious or political beliefs, or any other category of information defined in consultation with relevant authorities and the sector director, by. In addition to retaliation, stipulating what needs to be done with regard to data retention, the evidence of compliance with the bill is not yet clear in its determination whether such retention will exceed the objective requirements under Section 4 of the Bill.



**Compliance with Data Protection and Fiduciary Data:**

A business or person that determines the main purpose or agenda behind processing of such personal information. This processing proceeds according to purpose, collection, and final limits. Fiduciary controls how data is processed and why it is processed personally by a third party, data processor. All credible information is expected to undergo specific disclosure and culpability measures such as (i) the use of safety measures (such as data encryption and data protection), and (ii) the development of instruments for resolving criticisms against individuals. The procedures should also include verification of age and age of consent of parents when considering sensitive personal information of children. Such data processing has become an important source of revenue for large companies (depending on your online and preferred practices, but without prior knowledge).

The Bill sets out certain individual rights (or principal data). This includes the right to (i) receive automatic validation from a person who knows whether their information has been used, (ii) to seek redress for incorrect, incomplete, or outdated personal data, (iii) In some cases, personal

information may be transported to any other data affidavit in some cases, and (iv) prevent further disclosure of its information by your spouse if it is no longer required or else upon the revocation of the permit.

**Reasons to process personal information:**

The Bill allows for the processing of information by fraudulent persons as long as the consent is granted by each individual. However, in some cases, personal information is processed without permission. These include: (i) whether the State requires it to provide benefits to individuals, (ii) legal action, (iii) response to an emergency medical emergency.

- **Social media mediators:**
  The Bill provides for the sharing of information and will include mediators who make online communications between the user and. Mediators, who have certain responsibilities for their actions that are guaranteed to affect the democracy or social structure, provide a secure consumer authentication instrument for consumers in India. Consumers over the notified threshold, too.
- **Data Protection Officer:**
  The Information Officer recognized by the Bill may: (i) take steps to ensure protection of the public interest, (ii) prevent the misuse of personal data, and (iii) ensure compliance with the Bill. It will be chaired by 6 members, with 10 years of expertise in information protection and information technology. The instructions of the Authority are usually submitted to the Appeal Tribunal. Appeals from the Tribunal will go to the Supreme Court.
- **Data Transfer Outside India:**
  Upon unequivocally being approved by a person, sensitive personal information may be transferred outside India for processing, and subject to certain additional conditions. However, such sensitive personal information will still be stockpiled in India. Personal information required as sensitive personal data by the government can only be processed in India.

**Exceptions**

The central administration may relieve any of its organs from the provisions of the Act: (i) for the purpose of state security, public order, monarchy and integrity of India and foreign relations, and (ii) to prevent the promotion of such criminal offense (eg detention without a permit) in this regard the above items. For definite purposes, the processing of personal data is also excused from provisions of the Bill such as (i) the protection, investigation, or prosecution of any offense, or (ii) personal, internal, or (iii) reporting commitments. However, such analysis must be clear, concise, and legitimate, with safeguards.[6]

**Offences**

Offences under the Bill include: and (ii) failure to conduct data business, data analysis, fined by five crore rupees or 2% of annual fiduciary[7] profit, whichever is higher. Re-identification and

[6]Indian Personal Data Protection Bill 2019 – Key Highlights, (February 8, 2020), https://previewtech.net/data-protection-bill-2019

[7] Personal Data Protection bill proposes jail term for executives, up to Rs 15 crore penalty for data misuse, (Dec 04, 2019), https://economictimes.indiatimes.com/tech/internet/personal-data-protection-bill-proposes-jail-term-for-

processing of personally identifiable personal data is punishable by imprisonment for up to three years, with a fine, or both.

- **Sharing non-personal information with government:**
  The Central Government may further the data management process by providing it with any: (i) non-personal information (ii) anonymous personal information for better service management.
- **Amendment of other laws:**
  In order to amend the provisions of the Information Technology Act, 2000 relating to reimbursement, payable by companies for failing to protect personal information was passed.

**Conclusion:**

Privacy is one of the most important ingredients in a healthy lifestyle. The right to privacy is recognized in the Indian Constitution but its growth and development are left in the hands of the law. In the present era, it is very difficult to thwart data from accessing a public domain if someone intends to delete it without using much pressure. In a fast-paced world, data is a new force, a data controller can control how people think, decide, and view others. Therefore, the privacy or security of personal information is a serious matter for the government. The new data protection bill seeks to fill in the blanks but is not entirely successful in preventing violations of privacy or personal information. Data protection may include financial data, personal information, business proposals, intellectual property, and sensitive data. Chapters IX and XI of the Information Technology Act describe infringement of privacy and confidentiality related to unauthorized access to a computer, computer system, computer network or resources, unauthorized modification, removal, addition, modification, destruction, duplication, or data transfer, computer database, etc. No, full details are provided in the Data Protection and Privacy Act processed within the Information Technology Act, 2000. IT legislation requires establishing a set of specific standards related to the methods and purposes of copyright and personal data information. We can conclude that IT law addresses the issue of data protection and alternative laws are very much needed in data protection which strikes an operative balance between human freedom and privacy.

executives-up-to-rs-15-crore-penalty-for-data-misuse/articleshow/72370222.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst