

DE JURE NEXUS LAW JOURNAL

Author:

Muskan Dadia

Student, Government Law College, Mumbai

STATUS OF DATA PROTECTION AND PRIVACY IN INDIA

Today's world is called the 'Digital World' because hordes of information is largely available to everyone, mainly through computer technology. Terms such as artificial intelligence, machine learning, internet of things etc. are more prevalent now than ever. Data surrounds us everywhere. Section 2(1)(o) of the Information Technology Act, 2000 (the "IT Act") has defined "data" to mean "a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized 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." ⁱ Data is of two types, one that we voluntarily share and the second that is generated every time we utilize services online, like ordering food or calling for a cab . In such a scenario, one's privacy and safety online, enters a vulnerable position.

Mainly companies and governments collect and integrate information for their perusal. Companies do so to understand the behaviors and preferences of their customers online, to analyze the market conditions, strategize their sale policy etc. On the other hand, governments collect data to monitor suspicious activities and to maintain national security and social control.

Data protection and data privacy are often confused with each other. However, there is a significant difference between the two. Data privacy stands for who has access to the data, while data protection signifies the mechanisms and strategies to control who accesses this data.

Jurists in India are struggling to make laws that maintain a balance between one's individual rights and the overall security of a nation. This has proven to be a cumbersome task. The dilemma has further deepened after the Supreme Court declared on 24th August, 2017, that the 'right to privacy' is a fundamental right guaranteed to the citizens under part III of the constitution.

As of today, India does not have an expressed legislation on data protection. Unfortunately, The Personal Data Protection Bill (PDP), that was introduced in the parliament in 2006, has still not taken the shape of a law. However, the Information Technology act (2000), has been amended to incorporate rules on proper disclosure of information.

THE INFORMATION TECHNOLOGY ACT (2000)

The Information Technology Act, 2000 is the chief law in India that deals with cybercrime and electronic commerce. Pramod Mahajan, the then Minister of Information Technology, and a group of officials played an important role in nailing down the act. The bill received assent from President K.R.Narayan on May 9th, 2000. ⁱⁱ

The act played a pivotal role in changing the status of data privacy and protection in the following ways :-

- Recognized electronic records and digital signatures, thereby, facilitating a legal framework for electronic governance.
- Provided a definition for cyber crimes and laid down penalties for the same.
- Directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures.
- Established a cyber crime tribunal to resolve disputes.
- Amended the following acts to make them compliant with new technology: -
 - Indian Penal Code, 1860
 - The Indian Evidence Act, 1872
 - The Banker's Book Evidence Act, 1891
 - Reserve Bank Of India Act, 1934. ⁱⁱⁱ

Following sections were amended to deal with the rules on proper disclosure of personal data:-

- 43A. Compensation for failure to protect data—'Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.'^{iv}
- 72A. Punishment for disclosure of information in breach of lawful contract. –'Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.'^v

The government further issued the Rules, 2011 (guidelines) under section 43A of the Information Technology Act, 2000. These rules added numerous other requirements for the collection and disclosure of personal information in the commercial sector. Although, these rules resembled much of the greatly lauded - 'General Data Protection Rules '(GDPR) of the European Union, much was not seen to have been implemented under them.

Justice K. S. Puttuswamy Vs The Union Of India

In this landmark judgement, a nine-judge bench held that the right to privacy was protected as a fundamental constitutional right under the articles 14, 19 and 21 of the Indian Constitution.

Background

In the year 2012, Justice K. S. Puttuswamy filed a petition in the Supreme Court challenging the constitutional validity of the Aadhar system. Under the Aadhar system, a database

of the personal identity and biometric information of citizens was made. More than a billion Indians had already registered themselves under this scheme. A 12 digit code was allotted to each registered Indian. A comprehensive record of their biometric information and finger prints was maintained. In order to open a bank account, file returns, borrow loans, it was mandatory to be registered under this program.

Justice Puttuswamy (retired) held this to be an infringement of one's privacy. The biometric information could be misused in the absence of adequate safeguards and the state could not possibly turn a blind eye to the same.

The government defended by stating that an eight judge bench in the case of M. P. Sharma Vs Satish Chandra and a majority of four judges in the case of Kharak Singh Vs State Of Uttar Pradesh had already held that the right to privacy was not a constitutional right.

On 11th August, 2015, a three-judge bench held that the case be referred to a larger bench of five judges, who further ordered a bench of nine judges to adjudicate the case. While, the clarification on the right to privacy was not touched upon, the bench did pass an interim order restricting mandatory linking of Aadhar in order to avail benefits.

JUDGEMENT

Six different opinions were given by the nine judges, forming one of the longest judgements in the history of India. The coup de maître was Dr. D.Y. Chandrachud's judgement on behalf of four judges, covering about 266 pages^{vi}. Its mainly contained the following three insights :-

- Domestic laws in India dealing with privacy and nature of constitutional rights
- Comparative law on privacy (from England, United States, South Africa, Canada, The European Court Of Human Rights and the Inter- American Court of Human Rights)
- Several criticisms of the privacy doctrine. ^{vii}

Article 21 of the constitution played a crucial role in the delivering of this judgement. It states that, " No person shall be deprived of his life or personal liberty except according to procedure established by law."^{viii} Dr, Chandrachud threw light upon the fact that article 21 has been interpreted to encompass, inter alia, the rights to a speedy trial, legal aid , a healthy environment,

shelter, freedom from torture, right to reputation and earning a livelihood. Privacy too is included in fundamental freedom or liberty.

In one of the most significant sections of the joint judgement, titled 'Essential Nature Of Privacy', Dr. Chandrachud deeply brought out the important co-relation between dignity and privacy.

"Dignity cannot exist without privacy. Both reside within the inalienable values of life, liberty and freedom which the Constitution has recognized. Privacy is the ultimate expression of the sanctity of the individual. It is a constitutional value which straddles across the spectrum of fundamental rights and protects for the individual a zone of choice and self-determination" [169]^{ix}

While the right to privacy is not an absolute right, infringement must meet the following three parameters:-

- Legality
- Need for legitimate aim
- Proportionality

The judgement paved way for the decriminalization of homosexuality and abolishing provisions of adultery as a crime in the cases of Navtej Singh Johar (2018) Vs The Union Of India and Joseph Shine Vs The Union Of India (27th September, 2018) respectively.

Current Issues And Concerns Surrounding Data Privacy

- ✓ Jurists want to transform the 'consent' based approach to a 'rights' based one. While the consent-based approach allows the data controller to use, share and process information with third parties after obtaining the consent of the user, the rights based approach bestows the user with superior rights over the information, culminating in increased autonomy over personal data.
- ✓ The IT Rules, 2011 defines 'personal and sensitive data' as information related to
 - ❖ Passwords
 - ❖ Financial information like debit card, credit card and bank account numbers.
 - ❖ Sexual orientation
 - ❖ Physical, physiological and mental health conditions

- ❖ Medical history and records
- ❖ Biometric information

However, these provisions apply only to the information collected by corporate bodies. Moreover, the information available freely in public is not considered to come under the definition of 'sensitive personal data.'^x

- ✓ Section 69 of The Information Technology Act states the exceptions to the maintenance of data privacy by the government where it feels necessary to protect:-
 - ❖ The sovereignty or integrity of India
 - ❖ Defence of India
 - ❖ Security of State
 - ❖ Friendly relations with foreign states
 - ❖ Public order
 - ❖ Prevention of incitement to the commission of a cognizable offence related to above
 - ❖ For investigating an offence^{xi}
- ✓ Obligations of employers towards their employees in relation to the information collected by them are not clearly stated.
- ✓ No clear limits have been set on the extent to which personal information can be shared with external third parties.
- ✓ There is still ambiguity about the duration for which the information can be retained by the corporate bodies.

CONCLUSION

Privacy is a basic human right that is protected by the constitution. With globalization and emergence in new technologies, personal information is easily accessible and is in a vulnerable position. Although the constitution recognizes the right to privacy, its growth and development has been fully left with the judiciary to deal with. The Information Technology Act alone is not sufficient to protect data and a wholly comprehensive policy on data privacy is the need of the hour. The law should be able to strike the correct balance between an individual's personal rights and the over all security of the nation.



De Jure Nexus

LAW JOURNAL

ⁱ Available at :- <https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf>, last accessed on 30th March, 2021.

ⁱⁱ Available at :-

https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfv_sbdihbgfGhdfgFHtyhRtMjk4NzY=, last accessed on 30th march 2021.

ⁱⁱⁱ Available at :- <https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf>, last accessed on 30th march, 2021.

^{iv} Available at :- <https://indiankanoon.org/doc/39800/>, last accessed on 30th March, 2021.

^v Available at :-

<https://indiankanoon.org/doc/1480903/#:~:text=%2DSave%20as%20otherwise%20provided%20in,information%2C%20document%20or%20other%20material>, last accessed on 30th March, 2021.

^{vi} Available at :- <https://inform.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/>, last accessed on 31st March, 2021.

^{vii} Available at :- <https://inform.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/>, last accessed on 31st March, 2021.

^{viii} Available at :- <https://inform.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/>, last accessed on 31st March, 2021.

^{ix} Available at :- <https://inform.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/>, last accessed on 31st March, 2021.

^x Available at :- <https://elplaw.in/wp-content/uploads/2018/08/Data-Protection-26-Privacy-Issues-in-India.pdf>, last accessed on 31st March, 2021.

^{xi} Available at :- <https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india-everything-you-must-know>, last accessed on 31st March, 2021.