

Lecture- 24



Right to information vs right to privacy

Introduction

Right to privacy and right to information in India are the two most important rights to ensure that people can live their lives with dignity and integrity. These two rights are fundamental in maintaining the quality of life of an individual. While the right to privacy allows people privacy to their personal issues/affairs, the latter allows citizens to hold various government departments accountable for important public affairs. Most of the time, these two rights complement each other in holding the government accountable to individuals. But there is a conflict between these rights when there is a demand for access to personal information held by government bodies.

The relationship between right to privacy and right to information laws is currently considered the most important subject of debate around the world as various countries are adopting different types of concepts in relation to these laws and are making different legislations.

In India, in August 2017 the Supreme Court of India issued a landmark judgment recognizing the basic rights guaranteed by the Constitution of India as the right to privacy. The right to privacy was considered to be inherent in the right to life as stated in Article 21 of the Constitution of India. On the other hand, the right to information acquires the constitutional right of freedom of expression guaranteed to all citizens under Article 19(1)(a) of the Constitution. A bill stipulating various provisions for exercising this right was passed in 2005 and named the Right to Information Act, 2005.

What is known as the right to privacy?

If we try to understand privacy in the layman's terms it can be stated as "No unwarranted public interference" it generally means to be free and alone without unnecessary public interference as one's personal information is considered to be his personal property and he/she has the right to not disclose any such personal information. It may be said that privacy is the reversal of being public, if any private letter of one's friend is published by anyone without his/her express or implied permission then his/her privacy would be violated.

The right to privacy is recognized internationally as well and the concept is present under various declarations and conventions which can be seen as:

Article – 12 of the UDHR (Universal Declaration of Human Rights):

There should not be any arbitrary interference in anyone's privacy, family, home or correspondence nor should there be an attack upon the reputation and honour of any individual.

Article – 17 of ICCPR (International Covenant on Civil and Political Rights):

There should be no arbitrary interference in anybody's privacy, family or home.

Article – 8 of the European Convention on Human Rights:

Every individual has a right to respect, his private and family life.

In India, earlier right to privacy was not granted as a fundamental right to its citizens, the sole credit goes to the judiciary for interpreting the concept of right to privacy because neither the Constitution nor any other legislation defined this concept. We can see the evolution of this concept through different cases which made it a fundamental right after several years of interpretation.

The first case was;

M.P. Sharma vs. Satish Chandra was, before the Supreme Court of India, this case was in relation to search and seizure of documents of Dalmia group of companies, a search was carried out in 34 places belonging to the group and some of the private documents were also searched and evaluated due to which a writ petition was filed before the Supreme Court that the aggrieved parties' fundamental rights were violated, here the court had the opportunity of considering the constitutional status of the right to privacy in the context of state's power of search and seizure, but a very narrow view of constitutional provisions was taken in the case. The Supreme Court stated that the right to privacy is not a fundamental right and cannot be put into the domain of public law.

Furthermore in the case of;

Kharak Singh vs. State of Uttar Pradesh The petitioner was charged and tried for committing dacoity and he was subjected to domiciliary visits and surveillance by the police. The Petitioner filed a writ petition claiming that his fundamental rights under Articles 19 and 21 were violated, while determining the validity, the Supreme court also examined whether the right to privacy formed a part of Article 21 under personal liberty. Here the apex court while giving its judgment made the domiciliary visits unconstitutional and also stated that the right to privacy is not a fundamental right and right to movement under Article 19 infringes with physical restrictions.

Then a phase of cases came up where the Courts started recognizing the right to privacy and a judgment in the case of PUCL vs. Union of India, where the Supreme Court held that right to life and personal liberty includes the right to privacy and right to privacy includes telephone conversations as private at home or office and thus telephone tapping would be violative of Article 21.

In the year 2017, the Supreme Court in the landmark judgment of **Justice K.S. Puttaswamy vs. Union of India**, also known as the Aadhar case. It was in this case that the Right to privacy was first recognised as a fundamental right given under the constitution of India. The court held that the right to privacy is an integral part of the right to life and personal liberty as guaranteed under Article 21 of the Constitution. Due to this judgment, the Supreme Court interpreted that Aadhar is not violative of right to privacy and this judgment overruled the above other judgments where it was said that right to privacy is not a fundamental right.

Right to privacy has now be granted the status of fundamental right but is not an absolute right overall and is subject to certain restrictions or limitations that are:

- National Security and Public Safety.
- Public Interest.
- Scientific or Historic Research.
- Criminal Offences, etc.

Concept of data protection

Data protection generally is a set of policies and procedures that you can use to ensure the privacy, availability and integrity of data, sometimes known as data security or information privacy. In the digital age, data plays a huge role in our everyday lives, it's present in lots of obvious ways. When we are shopping online for example and have to type in our name and address. Data collection can also be less visible, for example, take data brokers, we have probably never heard of them, but these businesses specialize in creating in-depth profiles of individuals for advertisers. A single profile may draw on up to 1,500 data points, this can include a person's sexuality, browsing history, political affiliation and even medical records. Data protection is concerned with the ways in which third parties handle the information they hold about the public as to how it is collected, processed, shared, stored and used.

We can say that privacy and data protection are connected to each other, whereas data protection can also be termed as a part of privacy that holds a bigger place in an individual's life. Data protection is defined more specifically than privacy but however, it depends on the legal structure of different countries and how it is applied in consonance with the privacy laws prevailing in the countries.

In India, the right to privacy was recognized after the Aadhar judgment under which the concept of data protection also came up. As India does not have a particular data protection law to protect data and information shared or received in any form, they can be interpreted through a mixture of legislations, rules or guidelines. The most important and prominent is the Information Technology Act, 2000 which is considered as the primary law dealing with cybercrime and electronic commerce, under this legislation and rules only the information exchanged through an electronic form is governed and not the non-electronic forms. However, the scope of this law is limited and majorly protects the sensitive personal data and information collected through computer resources through corporate entities. There is no legislation on data localization which is the major concern and reason for the ban of Chinese applications, in order to address this a comprehensive data protection law is needed. This has been brought up in the discussions related to the Personal Data Protection Bill, 2019 which was presented in the Lok Sabha and after some

debates were given to a Joint Parliamentary Committee to examine the bill and give its report.

The Salient features of the bill are:

- Application of the Act to processing of personal data.
- Categorizing the kinds of personal data into three major heads – Personal Data, Sensitive Personal Data and Critical Personal Data.
- Obligations and limitations of the data collectors.
- Restrictions on the transfer of Personal data outside India.
- Exemptions or safeguards to Government agencies and other laws in relation to the processing of personal data.
- Offences and penalties against the prohibited acts under the law.
- Amendments to other laws as needed.
- New legal draft