IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Right To Privacy In India: Understanding Data Protection

Ajay Kumar, Research Scholar, Ch.Charan Singh University, Meerut(INDIA)

Abstract

The Honorable Supreme Court of India under the judgment in KS Puttaswamy vs Union of India declared the right to privacy as a fundamental right guaranteed by the constitution of India. Data protection is the backbone of the right to privacy. The government introduced the data protection bill in the parliament and which has been withdrawn. Now the government is planning to make a new comprehensive law of global standards regarding data security. Data is information. It may be of many types like financial data, health data, personal data, etc. there are various types of data protection mechanisms available like encryption, data masking, tokenization, etc. data protection is an essential step towards securing the right to privacy in India. There are various processes of data protection like encryption, tokenization, and data masking.

Introduction

Union minister, Ashwini Vaishnav has withdrawn the data protection bill, 2021 from the Lok Sabha after four years of deliberations. The minister said that 81 amendments were proposed regarding the bill and 12 recommendations were made. So, under the changed circumstances and to tackle future challenges the government decided to withdraw it and promised to make a new law. Concerning the above step, there is a need to understand data and data protection. How it is related to the right to privacy which is a fundamental right in India? All these issues have been discussed in this article.

The right to privacy is an important human right that has been recognized globally. **Article 12** of the universal declaration of human rights, says that no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence… Everyone has the right to the protection of the law against such interference or attacks."[1]

In the year 2017, the Honorable Supreme Court of India in the case of ***Justice K.S. Puttaswamy vs. Union of India*** recognized the right to privacy of every individual, guaranteed by the constitution within article 21 in particular and part III on the whole. In the same judgment, the supreme court also instructed the government to legislate a law for data protection. Following this, the union government set up a committee under the retired supreme court justice BN Srikrishna. Later in 2019, the committee tabled the bill named Personal Data Protection Bill 2019. This bill then went for review by the Joint Committee of the Parliament. Then a revised draft came in November 2021. This revised draft now has been withdrawn from the parliament by the government due to various reasons which have been discussed in the later part of the article.

Fundamental rights and Privacy

The fundamental rights are important to both citizens and the state. People develop themselves with fundamental rights and the nation stays dynamic and alive when its citizens have these. The fundamental rights are placed in part third (article 12-35) of the Indian constitution. The makers of the Indian constitution derived inspiration from the constitution of the USA i.e. Bill of Rights.[2] The fundamental rights promote the ideal of political democracy as they prevent the establishment of an authoritarian and despotic rule in the country. They also protect the liberties and freedom of the people against the invasion of the state. They provide equality for all individuals, the dignity of the individual, support for a larger public interest, and unity of the nation. These rights are justiciable in nature. It means that one can ask for the protection of these rights from the Supreme Court. The fundamental rights are most essential for the wholistic development of the individual. Presently there are only six fundamental rights available to individuals in India. These are

[1] https://privacyinternational.org/sites/default/files/2018-09/Part%201%20-%20Data%20Protection%2C%20Explained.pdf
[2] Laxmikant, M., Indian Polity, Fifth Edition, McGraw Hill Education(India) Private Limited, page-7.1

right to equality(art14-18), right to freedom (19-22), right against exploitation (23-24), right to freedom of religion(art.25-28), cultural and educational rights(art.29-30) and right to constitutional remedies(art.32).

Among these fundamental rights, article 21 is about the protection of life and personal liberty. And it declares that no person shall be deprived of his life or personal liberty except according to procedure established by law. The judgment of KS Puttaswamy vs. Union of India,2017 declares that privacy is an intrinsic part of human personality and it is an essential part of the life of any human being. According to the judgment, the right to privacy is a fundamental right under article 21 i.e. the right to life and personal liberty.

Privacy and information

Now when we say protection of privacy the question came to our mind what it is? The term privacy is very comprehensive and it includes lots of meanings according to different authors.

Like Adam Carlyle Breckenridge has defined 'privacy' in his book "The Right to Privacy" as the rightful claim of the individual to determine the extent to which he wishes to share himself with others and his control over time, place, and circumstances to communicate to others. It means his right to withdraw or to participate as he sees fit. It is also the individual's right to control the dissemination of information about himself; it is his own personal possession."[3]

Judge Cooley says that "privacy is synonymous with the right to be left alone."[4]

Arthur R. Miller defines privacy as the "individual's ability to control the circulation of information relating to him- a power that often is essential to maintaining the social relationship and personal freedom.[5]

The term 'privacy' is mostly defined in terms of 'information'. This useful information about a person is called data. Thus, we can say that the protection of data is the protection of the privacy of a person. It means that to secure the right to privacy of the citizens, we need to protect the data of the citizens. Thus, data protection is an essential and fundamental step towards securing the right to privacy of the citizens.

Data

Now to understand data protection, we need to learn about data, types of data, collection of data, and processing of data.

[3] Carlyle, Adam,1971, The Right to privacy,
[4] Thomas M. Cooley, A Treatise on the law of Torts, 2nd ed. (Chicago: Callaghan and co.1888), p.29
[5] Goyal, Gaurav and kumar, Ravinder; the right to privacy in India: concept and evolution, Partridge publication, p.10

The **personal data protection bill 2019** expressed the data as a representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means.

In India government and non-government agencies both collect data from the citizens to provide services. People provide data through employment advertisements, Simcard purchases, LPG connections, bank Accounts, National Census, social media, online shopping, market shopping, health checkups, during toll centers, admissions in educational and skill institutions, etc. this sharing of information with the agencies or institutions is necessary for getting the better services but when the use of this data done for another purpose then it may affect the privacy of the people.

Types of data

Based on the different nature of the information, data can be classified as-

Financial data means data related to users' bank account details. The financial data is used to identify accounts in a bank, debit/credit card, or a payment instrument issued by a financial institution. it is data of the relationship between data principal and financial institution including financial status and credit or transaction history.

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioral characteristics, physiology, or health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

Health data means the data related to the state of physical or mental health of the data principal and includes records regarding the past, present, or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services;

Personal data means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute, or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for profiling;

Data protection

Now understand data protection. Data protection is the whole process to secure the data. It is the process of safeguarding crucial information from corruption, sharing, or loss.

It protects the data from unauthorized access and provides a technical mechanism to safeguard the data so that, that data can be used only for the intended purpose and not for another purpose. It is concerned with safeguarding the information from hackers. It ensured that someone's data is protected from unethical intervention and access.[6]

In this process, there are some players which we need to understand like data principals, data fiduciaries, and data processors. The Data Protection Bill 2019 explained these terms as-

data principle- "data principal" means the natural person to whom the personal data relates;

data fiduciary means any person, including the State, a company, any juristic entity, or any individual who alone or in conjunction with others determines the purpose and means of the processing of personal data; example- google, Flipkart, Amazon, etc.

data processor means any person, including the State, a company, any juristic entity, or any individual, who processes personal data on behalf of a data fiduciary;

The whole process of data protection can be broadly classified into three categories.

- Traditional data protection
- Data security
- Data privacy

[6] https://blog.ipleaders.in/difference-between-data-protection-and-data-privacy/

Traditional data protection: this category includes steps like backup or restoring data, archiving of data, data retention replication of data, and physical infrastructure.

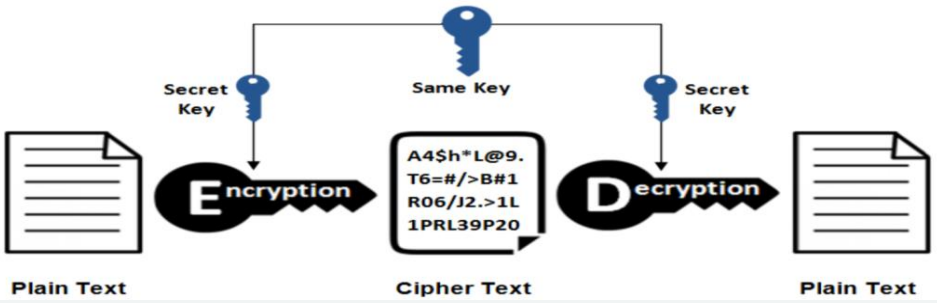
Data security includes processes like encryption, threat monitoring, authentication, access control, breach access and recovery, and data loss prevention.

Data privacy includes legislation, policies, data governance, etc.

There are five protection methods that we are going to discuss here.

- **Encryption**- this method makes the data unreadable to unauthorized users. It converts that data into an unreadable form, with the help of mathematical tools and provides a password or a key to decrypt the data for the authorized user.

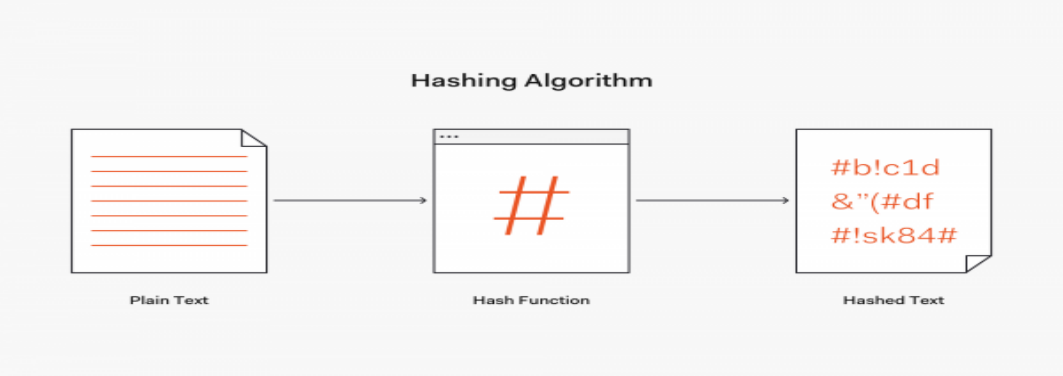
  It is the process of translating a text message or email into an unreadable or coded format, this unreadable format is called 'cipher text'. When the intended authorized user opens the message, with the help of a password the coded information is translated back to its original form. This reverse process is called decryption. The sender and the recipient both use a secret encryption key to unlock the data. This encryption key is a collection of algorithms that scramble and unscramble data back to a readable format.



Data encryption mechanism

- **Hashing** -it is the process of transforming any given key or a string of characters into another value. This is usually represented by a shorter fixed-length value or key that represents and makes it easier to find or employ the original string. The most popular use for hashing is the implementation of hash

tables. A hash table stores key and value pairs in a list that is accessible through its index.



Hashing mechanism

- **Data masking**—It uses data masking software that hides that data by obscuring letters and numbers with proxy characters. The data is still there, behind the masking. The software changes the data back to its original form only when an authorized user receives that data.
- **Tokenization**- It is a reversible protection mechanism. In this process, the data is substituted by a so-called token. This token itself maps back to the original data element but does not expose any sensitive data.

Conclusion.

The right to privacy is a fundamental right in India as declared by the judgment of KS Puttaswamy vs Union of India case (2017) of the supreme court. And it must be protected. Private companies and government should maintain the security of information of the people so that people do not suffer from the invasion of privacy. The government has withdrawn the data protection bill 2021 from the parliament and now the government is planning to make a comprehensive data protection law that will be of global standards. Despite the data protection laws, awareness among the people regarding privacy, data protection, and cyber security is a must. Government should include this step in the upcoming legislation.

References

1. [1]Data Protection Explained, https://privacyinternational.org/sites/default/files/2018-09/Part%201%20-%20Data%20Protection%2C%20Explained.pdf
2. [1] Laxmikant, M., Indian Polity, Fifth Edition, McGraw Hill Education (India) Private Limited, page-7.1
3. [1] Carlyle, Adam,1971, The Right to privacy,
4. [1] Thomas M. Cooley, A Treatise on the law of Torts, 2nd ed. (Chicago: Callaghan and co.1888), p.29
5. [1] Goyal, Gaurav & Kumar, Ravinder; the right to privacy in India: concept and evolution, Partridge publication, p.10