



The Right To Privacy And Data Protection Issues In India

Firoz Ansari

Email : aaryavart2013@gmail.com

Received- 26.10.2020,

Revised- 03.11.2020,

Accepted - 08.11.2020

Abstract: *Insights into privacy and data protection concerns can be gained from the ever-changing legal landscape and technological advancements of today. Privacy is a concept that does not interfere with other people's interests. Privacy has become a top priority for individuals thanks to technological advancement, highlighting the importance of information security. Individual autonomy, which is threatened by external intrusion, is emphasized by data protection. By any means necessary, it is essential to end the stranger's influence on the individual's functioning. The right to privacy and data protection are fundamentally at odds. Financial data, health data, company recommendations, intellectual property, and sensitive data are all examples of data that can be protected. Data privacy and security are not adequately addressed in the Information Technology (Amendment) Act of 2008. The IT Act is not enough to protect data, so a separate law needs to be made.*

Key words- Privacy, data protection, personal information, data privacy.

Assistant Professor- Faculty of Law, Agra College, Agra (Dr. B.R. Ambedkar University, Agra) Agra (U.P.), India

Corresponding Author

Privacy is a part of human rights which is within the human since birth. In India, the concept of privacy is relatively new. The Upanishadic literature, which is derived from the ancient Indian epistemology, encourages meditation to be carried out without interruptions from outside sources. The "Arthashastra" and the estates show a great deal of respect for individual privacy. In the Ramayana and other ancient texts, the use of curtains is described and explained in a specific way. While some may consider this irrational, some people must limit their private lives. The quality of public life is significantly impacted by private life, either improving or decreasing it. If you lead a dishonest private life, whether by living in opulence with assets that exceed your declared income or by being discovered spending nights elsewhere, your dedication to the world is meaningless, regardless of your public efforts and devotion. You conclude that there is no privacy because you are constantly scrutinized about your personal and private life. Individuals had few interactions with the government during the laissez-faire era. It is essential to manage administration across multiple contexts in a modern administrative state. The line between a person's public and private lives has blurred. Individuals

are required to provide extensive personal information whenever they interact with the administration. Individual-specific data may be collected by the government in some cases.

Information about people may be crucial for a government in formulating its policies democratically. One fundamental means of social control is government surveillance of its population. The government may need to conduct in-depth social studies and collect data before making welfare payments. For the purpose of combating contemporary organized crime, the collection of personal data is becoming increasingly important. The governments may keep an eye on people who work in the military, international affairs, and nuclear energy industries.

THE CONCEPT OF RIGHT TO PRIVACY- According to the "Duhaime's Law Dictionary" the privacy means an individual's Right to control and access over his/her personal information. This definition is a layman translation to what privacy in simple sense means. It simply indicates that privacy right of an individual is his/her full control and undisrupted access over his/her own personal information. The personal information here includes- his name, address, demographic data, his personal affairs, his private space etc. Gillian Black in his book defines the privacy as Privacy is a desire of an individual to be free from the other's intrusion. The definition states that every individual is having the right of enjoying his



personal choices, his personal affairs free from the interference of other people into it. European Convention on Human Rights in Article 8 defines the privacy as Every individual have the Right to respect for his family and private life, his home and his correspondence. This is a huge effort by the Human Right Convention on the international level to define the importance of privacy in an individual's life. The Article further stated that no Governmental Agency is allowed to intervene the privacy right of a person until and unless, the said intrusion is in accordance to the law and is necessary for the purpose of security of the state, public wellbeing, and essential for the economical wellbeing of the country. Justice Cory of the Canadian Supreme Court in a case defined privacy as Privacy is the situation of being alone, in a case of preferences or freedoms, uninterrupted and independent of government scrutiny; safe from intervention or disturbance. The capacity to exclude anyone from the property is a significant element of privacy. A main aspect of privacy is the right to be free of intrusion or interference."

According to "Justice Dickson is The freedom of a man to ascertain when, how and to what degree he or she will disclose private data, can be characterized as privacy. A sensible idea of privacy requires a person to continue on the belief that the State may only infringe this right by capturing personal communications on a hidden basis if it has determined to the satisfaction of a judicial officer that, an offense

has been performed or is being performed and that monitoring of communications provides proof of the crime."

In "J. K.S Puttaswamy v. Union of India held that The privacy rights is guaranteed in accordance with Article 21 as an inherent component of the right to life and personal liberty and as portion of the rights provided by Part III of the Constitution."

THE RIGHT TO PRIVACY IN INDIAN CONSTITUTION-

The Fundamental Right to Privacy is not explicitly spelled out in India's Constitution. "However, rulings in the courts have established that this right is protected by Part III of the Constitution". The right to privacy includes the following provisions:

* Art. 19: "Freedom of Speech and Expression-Article 19(1) (a) provides that all citizens shall have the right to freedom of speech and expression. However, this is justified by Article 19(2), which says that it will not influence the implementation of any current law or stop the State from creating any law, insofar as such law imposes reasonable constraints on the practice of the right in the interests of India's sovereignty and integrity, state security, friendly ties with foreign countries, public order, decency or morality".

* Art. 21: "Right to Life and Personal Liberty-Article 21 of India's constitution gives citizens and non-citizens the right to privacy. This is not obviously stated in it, but as a statutory justification, the Supreme Court indicated the same.

Article 21 of the Constitution states as follows: No individual shall be denied of his lives or personal freedom except as provided by the procedure established by law. Article 21 is the heart of Indian people's freedom. The terms 'procedure established by law' in this article have been the subject of debate since the Indian constitution was enacted. The right strategy that is needed is that, in the sphere of personal freedom, the significance of the operation created by law is not very distinct from that of the due process clause of the Fifth Amendment to the American Constitution".

* The Indian Judiciary also interpreted privacy right as a fundamental right under Article 21 of Part III of the Constitution. Following were the series of Cases which dealt with right to privacy. MP Sharma v. Satish Chandra, KharakSingh v. The State of UP and Govind v. State of Madhya Pradesh.

* In "Malak Singh Etc v. State of Punjab & Haryana & ors here the Supreme Court held that where there was no illegal interference, State surveillance exercised within its limit and without violating the Right to personal liberty of the citizen, shall be valid and lawful.

* In "R. Rajagopalan v. State of Tamil Nadu, the higher judiciary by declaring right to privacy intrinsic in Article 21 of the Constitution has decided that every Indian citizen has the liberty to safeguard his or her privacy whether it may be related to education of child, giving birth to and raising a child, reproduction,



decision upon the matter of marriage, family etc."

* In "People's Union for Civil Liberty v. Union of India, The Supreme Court held that Right to Privacy includes talking over telephone and such call can be made by sitting in any place of its own office or at home because telephone conversations itself is an essential aspect of man's life. Therefore, tapping of telephone conversations is a violation of Right to privacy under Article 21. With this judicial interpretation, different kinds of privacy arose like privacy of telephone conversation, privacy of medical records etc. However, it has not been declared as fundamental right because majority judges in both Kharak Singh and MP Sharma cases held that Right to privacy is not a Fundamental Right. But in 2012, a petition was filed by K S Puttaswamy before the Honorable Court questioning the Constitutional validity of Aadhar Act on the ground of violation of privacy".

" Thus, in Puttaswamy case, it has been decided by the Supreme judicial authority that Right to Privacy is a fundamental right guaranteed under Part III of the Constitution i.e. intrinsic in Article 21 itself and therein overruled the earlier judgment of Kharak Singh and MP Sharma cases. Thus, from the above discussion of all the cases, it has been concluded that Right to Privacy is now declared as a Fundamental Right of individuals under the Constitution of India.

PRIVILEGES CONNECTED WITH SECURITY IN INFORMATION

ASSURANCE REGULATIONS-

The only piece of legislation in the country that protects an individual's privacy in relation to data and information transactions is the I.T. Act of 2000. In order to increase the effectiveness of their protection, the Indian legislature amended the Act in 2008 and added a number of provisions to the existing Act of 2000. Data privacy is protected by the Information Technology Act and the Amendment Act of 2008, which include the following provisions:

* Section 30 of the Information Technology Act of 2000 mandates that the certifying authority adhere to safety procedures to ensure the confidentiality and privacy of electronic signatures.

* Section 43: The Information Technology Act of 2000's Section 43 makes it possible for the individual in question to be compensated for unauthorized access to his or her personal and private data. Under this section intrusion of one's computer or computer framework amounts to compensation. Several clauses and explanations of this section were amended by the ITAA 2008 which are clause (a), clause (i), clause (j), and explanation (v).

* Section 43A (by ITAA, 2008): The IT Amendment Act of 2008 added this brand-new section to the law. This section provides 'Compensation for inability to safeguard data- where an entity that possesses, distributes or handles any delicate private data or information in a computer resource that it possesses, monitors or works is negligent in applying and retaining

appropriate safety practices and procedures and thus creates any individual unfair loss or unfair benefit, that entity is responsible to pay the losses by the way of compensation to the person who is affected.'

* Section 66: The Information Technology Act of 2000's Section 66 also protects sensitive private information stored in a computer resource by, among other things, penalizing a decrease in the value of information stored in a computer resource with up to three years in prison. Thus, if an attacker is hacking into the computer system and copying and transferring sensitive personal information to a rival that may be of very high utility or of very private nature or business importance to the proprietor, the said act results in a decrease in the amount of data located within a computer resource and thus infringement of privacy.

* Section 72: According to Section 72 of the Information Technology Act of 2000, a government official can be fined if he transfers any digital information or data he has obtained about a person in his formal capacity. There is only a limited implementation of this section. It is confined to the actions and omissions of those individuals who have been given authority under this Act, rules or laws produced under it, i.e. police, certification authorities and officials approved by particular notice.

* Through the ITAA of 2008, "Section 72A was also added to the statute. The section states Any person, including a mediator, who,



while providing services under a legal contract, has obtained access to any material containing information about another person with the intention of causing or knowing that he is ought to cause the unlawful damage or unlawful profit reveals, without the approval of the individual involved or in violation of a legitimate agreement, such work shall be punished with probation for a period of up to three years or a penalty of up to five lakh rupees or both, except as otherwise provided in this Act or any other law".

Additionally, "in accordance with the Supreme Court's decision in the case of Justice K.S. Puttaswamy, the Government of India has established a committee with five members led by Justice (Retd.), a former Supreme Court judge. B.N. Srikrishna for writing a bill regarding data protection. If the bill passes, it will be India's first comprehensive law protecting online users' personal data from misuse by state and non-state intruders. According to the office memo from the Srikrishna Committee, the government is aware of India's growing importance to data protection. It is of the utmost importance to ensure the growth of the digital economy while preserving the privacy of individual information".

The Committee's final study and draft of a data protection law, the Personal Data Protection Bill, 2018, was published in July 2018. The Personal Data Protection Bill establishes a Data Protection Authority to oversee data handling procedures. It also acknowledges the

necessity of developing a mutual culture that safeguards freedom, advancement, and creativity within the context of the fundamental right to privacy, promotes a secure and honest digital economy, and respects the information privacy of citizens.

In addition, the Bill states that it aims to protect individuals' rights to privacy when it comes to their personal data, establish a framework for the implementation of organizational and technical steps in the handling of private information, establish standards for the transmission of private information across borders, guarantee the responsibility of organizations handling information, and offer remedies for processing that is unauthorized or dangerous. It also says that it wants to keep people's privacy and control over their personal data safe.

EFFECTS OF DATA PROTECTION ON SOCIETY-

"The only constant is change." Evolution is the only thing that keeps humans going, according to this proverb. Information is the only thing people rely on in this age, which is the age of information. Through the use of social internet platforms like Facebook, Skype, and Whatsapp, for example, the society of today is connected to one another by a single thread of information. People today share every minute detail of their lives with a variety of people because they are so reliant on these social media platforms. People from all over the world now share their data with one another on these social media platforms, creating a new dimension of the world.

Therefore, enacting effective laws to safeguard data against misuse by individuals or authorities is critical".

In today's world, "data security is of the utmost importance because data is readily available everywhere and it is simple to gain access to the data of an unknown individual without informing him". As a result, there is a significant risk of crimes like identity theft, cybercrime, and hacking. Information security is part of data protection". In the computer system, people have found ways to misuse or exploit information for various purposes.

CONCLUSIONS- The ability of an individual or group to separate or reveal information about them specifically is called privacy. Individuals and cultures differ in the boundaries and substance of what they consider to be personal, but they all share fundamental themes. Sometimes, the desire to remain anonymous or unnoticed in the public domain is associated with privacy. The majority of the time, the expression "private to an individual" refers to something that the individual perceives as intrinsically exceptional or intimate. In this way, the amount of private data that is made public depends on how the public gets this information, which varies from place to place and over time. Most of the time, protection goes beyond privacy and includes things like insurance and ideas about how to use data correctly. In some countries' privacy laws and occasionally in their constitutions, the privilege of not being subjected to unapproved attacks on privacy by



the administration, organizations, or individuals is included. Privacy laws exist in varying degrees in virtually every nation; Tax assessment law, for example, frequently mandates the disclosure of near-home wage or profit data. Particular security in certain countries might battle with the option to talk regulations uninhibitedly, and a few regulations might require open divulgence of information that would be seen in various countries and social orders as private.

SUGGESTIONS- The following recommendations have been derived from the above exchange:

1) The need for a change to the constitution: a safeguarded change is required by which security privileges can be unequivocally ensured by adding another understanding. A change like this is necessary to provide side recognition for protection. At precisely that point, individual freedom, which is guaranteed by the Constitution, may become increasingly important. Creating a National Strategy: To ensure that individuals in India have the right to control their own information collection and transmission, a comprehensive strategy is required. The implementation that combines the essential principles of sensible information practice is an essential component of this strategy.

2) In this manner, the law would restrict individual data customers' access to and use of personal information. Clients of individual data would be required to provide individuals with unambiguous

instruction regarding the collection of individual data and its use. In order to be put into action, individual data clients would need to give people the chance to stop the spread of their own data. Individual information production and accumulation online would be adequately restricted as needed.

3) Even though a comprehensive confidentiality agreement is necessary to guarantee the individual's right to control the collection and transmission of personal data, the parties involved must exercise this control. Regardless, online clients should assume a sense of ownership with their electronic trades. They should be aware of the content of these exchanges and use appropriate security measures, such as encryption, to protect their privacy. When signing up for online communities and participating in business exchanges, individuals will also have to decide how close they are to discovering home data. People will most likely take advantage of the numerous educational, social, and business opportunities offered by the internet in the future if they anticipate the risks associated with using the internet and use the legitimate insurance schemes that have been recently illustrated.

REFERENCES

1. M.C. Pramodan, "Right to Privacy" 14 CULR 6 (1990) Ibid.
2. Available at <http://www.duhaime.org/LegalDictionary/C a t e g o r y / CriminalLawDictionary.aspx>

3. Gillian Black, "Publicity Rights" 2 EPW 8 (2011)

3. Available at <https://www.jus.uio.no/lm/coe.convention.on.human.rights.1950.protocols.to.1966.consolidated/landscape.letter.pdf> (Visited on 22/6/2019)

4. R v. Edward (1996) 1 SCR 128

5. R v. Duarte (1990) 1 SCR 39 (2015) 8 SCC 735

6. HM Seervai, The Constitutional Law in India : A Critical Commentary 43 (Central book publication, New Delhi, 2003)

7. Ibid.

8. JN Pandey, Constitutional Law of India 92 (Central Law Agency, New Delhi, 2007)

9. 1954 AIR 300, 1954 SCR 1077.

10. 1963 AIR 1295, 1964 SCR (1) 332.

11. 1975 AIR 1378, 1975 SCR (3) 946.

12. 1981 AIR 760, 1981 SCR (2) 311.

13. 1995 AIR 264, 1994 SCC (6) 632.

14. 1997 3 SCC 433.

15. Id ; Section 43

16. Id; Section 66

17. Id; Section 72

18. Id; Section 72A

19. Rakesh Chandra , Right to Privacy In India With Reference to Information Technology 98 (YS Book International, New Delhi, 2017)

20. Rahul Mathan, Privacy 3.0 : Unlocking Our Data Driven Future 55 (Harper Collins, Lucknow, 2018)

21. Gaurav Goel, Right To Privacy In India: Concept & Evaluation 26 (Partridge India, New Delhi, 2016)
