



Right to privacy and data protection under Indian legal regime

Kuldeep Yadav

Research Scholar, Mahatma Gandhi Kasha Vidyapeeth University, Varanasi, Uttar Pradesh, India

Abstract

Around the world, the right to privacy has become widely acknowledged as a fundamental human right. In India Article 21 of the Indian Constitution recognizes privacy as a Fundamental Right. The security of data has become particularly challenging to achieve. Further, the lack of legal protection for this Right has made it easy for the ruling majority to violate private rights through discriminatory legislation. This Right was not initially acknowledged in India as a Fundamental Right, nor was any special data protection legislation passed to protect citizens' Rights to Privacy. At the same time, there were several claims that the Indian government and private commercial entities occasionally violated citizens' rights to privacy. Such claims were also brought before the courts of law, where the judges rendered important judgments that included rules and norms. In order to comprehend the level of security provided to Indian individuals regarding their right to privacy by the legal system, it is crucial to study all of these legislative changes connected to the right to privacy and data protection. However, it has been determined that the Indian Legal System has adequately recognized the Right to Privacy and significant steps have been taken to prevent data theft and the improper use of sensitive information.

Keywords: data protection, personal information, confidentiality, right to privacy

Introduction

“Privacy is not something that I am merely entitled to, it is an absolute prerequisite.”

These are "Marlon Brando's" exact words. In addition to not disclosing personal information, original work, trade secrets, corporate secrets, personal relationships and life, etc., privacy encompasses a wide range of topics. A person's right is violated if his letters to another person are publicized without his consent. There is a greater danger of technology being misused as we go closer to its advancement. India is seeing an increase in cybercrime on a daily basis because there aren't any particular or strict rules for data protection. The purpose of data protection is to safeguard a person's private information.

The idea of privacy has a long history and is a fundamental component of human rights, which are ingrained in every person from birth. They cannot be divided or considered sacred. It covers things like the right to private communication, the right to one's body's privacy, the right to one's sexual orientation, the right to have children, etc. The private right, information of public interest, or information in the form of a public record are not included inside it.

Concerns over the security of personal information and data basically, the right to one's privacy is already at an all-time high. The unique right of an individual to manage the acquisition, use, and disclosure of personal information is referred to as the right to privacy. Personal information can include, among other things, details about your hobbies, routines, and activities, as well as information about your family, your education, your communications (including phone and mail records), your health, and your finances. The fusion of technology has also given rise to new concerns around data protection and privacy rights.

The 1948 Universal Declaration of Human Rights ("UDHR") enshrined this fundamental right to private protection. No one may be subjected to arbitrary interference with their family, home, or correspondence, or to attacks on their character or honour, as stated in Article 12 of the constitution. Everyone has a right to legal protection from these types of intrusions or assaults. The 1976 International Covenant on Civil and Political Rights ("ICCPR") also outlines this human right. The State must implement legislative and other measures to give effect to the ban against such interferences and attacks as well as the protection of this right in order to fulfil its duties under the ICCPR. As a signatory to both the UDHR and the ICCPR, India is immediately bound by both international agreements. To safeguard this valued right, however, no corresponding legislation has been enacted in India.

Research Methodology

This research makes use of a number of different methodologies used in legal research. The most crucial component of legal research is the sources of legal materials because without them, it is impossible to find solutions to the legal problems that have been raised. As a result, legal materials are used as sources of legal research in order to address the problems that have been raised. The writers of this study used both primary and secondary legal sources.

Indian Legal Scenario

According to Article 21 of the Indian Constitution, which outlines our essential rights, the right to privacy is one of those rights. This was supported by a nine-judge Supreme Court panel in Justice K.S. Puttaswamy v. Union of India, which issued a landmark decision on August 24, 2017, stating that "the right to privacy" is an essential component of Part III of the Indian Constitution.

We are aware that there is currently no clear regulation in India that might deal with privacy and data protection. In the lack of such laws, there is nonetheless a legal structure that, although not directly addressing privacy and data protection, does so indirectly. In addition to statutory protection, the Indian Constitution also guarantees privacy protection. The sharing or receiving of personal information in spoken, written, or electronic form is not protected by a stand-alone law in India. Although there are protections, they are spread over a variety of laws, regulations, and policies.

Constitution of India: The Indian Constitution ("Constitution") has been construed to include the right to privacy as an unstated fundamental right. The Indian Judiciary was inspired to take a proactive role in defending this right as a result of the growing number of occasions when the State violated it on justifications (that were not always legitimate). *Kharak Singh v. State of U.P.* is a significant ruling on this subject. The Supreme Court determined that because the right to privacy is protected by Article 21 of the Constitution, it is against the individual's personal liberty to enter his or her home without permission and disturb them. The Supreme Court, however, limited the right to privacy in *Gobind v. State of Madhya Pradesh* and ruled that a violation of privacy can be permitted by the law. In the case *R. Rajagopal v. State of T.N.*, which was heard in 1994, the Supreme Court was asked to weigh in on the extent and boundaries of the right to privacy or the right to be left alone. In this instance, a condemned prisoner's right to privacy was in question. Justice B.P. Jeevan Reddy held that even though the right to privacy was not listed as a basic right, it may be deduced from Article 21 of the Constitution by applying case law from the United States and the United Kingdom to the Constitution. *People's Union of Civil Liberties v. the Union of India* was a landmark case involving the right to privacy. The case largely dealt with the subject of "telephone tapping," and it was decided that doing so would violate someone's right to privacy unless it was very necessary, like in the case of a public emergency. Although it may appear that the right to privacy is sufficiently safeguarded as a fundamental right, it is important to remember that, with a few notable exceptions, fundamental rights given to the individual only serve as restrictions on State activity. Therefore, a person will not be shielded from private parties' acts by such a reading.

Law of Torts: Direct legal recourse for invasions of privacy is not permitted by common law tort rules. By using civil wrongs like defamation, trespass, and breach of confidence, tort law aims to protect people. However, with the introduction of new technology, such common law appears blatantly inappropriate for this new setting. To address difficulties with privacy and data protection, a separate law is required.

Indian Penal Code, 1860: The penal code does not explicitly address violations of data privacy. Nevertheless, there are some offences from which it can be inferred that a penalty for invasion of privacy exists, for instance, under Article 408 of the IPC culpability results from dishonest misappropriation of movable property.

The Information Technology Act, 2000: To create a comprehensive regulatory framework for e-commerce, the ITA was passed. Examining Sections 69 and 75 of the Act is important in relation to the right to privacy on the Internet. Similar to Section 5(2) of the Indian Telegraph Act of 1885, Section 69 gives the Controller the authority to direct any government agency to intercept any information transmitted through any computer resource and mandates that users disclose encryption keys or face up to a seven-year prison sentence. On the other hand, the sole express clause in the statute dealing with privacy and breach of confidentiality is Section 72. It states that anyone who divulges the contents of an electronic record, for example, without the owner's agreement may be penalized with up to two years in prison, a fine up to one lakh rupees, or a combination of the two. However, both clauses in the Information Technology Act of 2000 deal particularly with the government's authority over people's privacy. The protection of privacy rights, which can be construed in the context of transactions between persons and companies or between two individuals over the Internet, are not covered by Indian legislation, it can be inferred from an awareness of the Indian legal circumstances.

Intellectual Property Law: The Copyright Act of 1957 in India addresses issues involving copyrighted infringement and imposes mandatory punishment that is proportionate to the gravity of the offence. According to Section 65 of the Act, anyone found using a computer or a copy of a computer software that violates the law faces up to three years in prison or a fine. Furthermore, an author's copyright is protected when they create records or broadcast programmes using information obtained from another source and by investing time, money, labour, and talent that counts as work within the definition of the Copyright Act. As a result, any violation of the Copyright Act involving such database may give rise to legal action against the outsourcing parent company.

Indian Contract Act, 1872: The Indian Contract Act, 1872 is the Indian law that controls the terms of contracts and agreements made between parties. As a result, if the parties engage into a contract, they must include a confidential or privacy provision, which states that personal information about individuals may only be disclosed

with their permission and consent, and only for purposes or in a manner agreed upon by the parties. Therefore, a person who divulged information without authorization and in violation of the terms of the agreement would be in breach of contract and subject to legal action for damages. Additionally, an insurance proposal containing a secret clause regarding the customers of the insurer is issued by the insurer as part of an insurance contract. Any release of this information without agreement will result in legal action for damages on the grounds of breach of the contract the parties had previously agreed upon.

Conclusion and Suggestions

As a result of various judicial interpretations, the Right to Privacy has become a Fundamental Right in India. However, if we look at the current situation, we will see that globalization has led to significant technological advancement and given the advancement of technology, the question of whether or not we have privacy in our daily lives arises. This right is crucial for living a life of dignity, for being able to make our own decisions, and for personal growth, hence it is crucial. As we can see, technology is a big part of our lives today. It has greatly benefited us, but it has also turned into a threat since as technology advanced, so did a number of issues like cybercrimes, data theft, abuse of data, etc., which are directly related to our privacy. We all know that in order to receive any type of service, we must share our personal information or data with a third party, whether it is a government agency or a private company. However, doing so increases the risk of data theft or misuse because India does not have sufficient data protection laws, despite having other laws that indirectly deal with data protection. There are still certain gaps that need to be addressed even though India is attempting to establish and create legislation for data protection and privacy. Due to the critical importance of this new area of law in the modern day, our Indian legislature must take into account the benefits of data protection and privacy legislation from around the globe and advance its implementation and development. There are numerous data protection regulations in other countries that, if adopted and effectively enforced in India, might help to reduce problems with data protection.

References

1. AIR 1963 SC 1295.
2. (1975) SCC (Cri) 468.
3. Bijan Brahmhatt. "Position and perspective of privacy laws in India", available at: <http://www.lawctopus.com/acadomike/postion-perspective-laws-India/> (Visited on October 23, 2019).
4. Bijan Brahmhatt. "Position and perspective of privacy laws in India", available at: <http://www.lawctopus.com/acadomike/postion-perspective-laws-India/> (Visited on October 23, 2019).
5. Reserve Bank of India
6. Ministry of Communication and Information Technology
7. Latha R Nair. "Data Protection Efforts in India. Blind leading the blind", 4, IJLT1, 2018, 23-27.
8. Personal Data Protection Bill, 2019.
9. The National Association of Software and Services Companies, available at: <https://www.britanica.com/topic/National-Association-of-softwae-and-service-companies>
10. Rana SS. Co. advocates, "India: Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011."