**The Legislative and Administrative Framework on Protection of Right to Privacy in Digital India**

**Dr. Manpreet Kaur Rajpal[[1]](#footnote-1)**

# Abstract

*The need for solitude is inherent in all humans. In truth, establishing different borders with virtually total isolation is a natural need for an individual. In its widest meaning, privacy covers a wide range of potential outcomes, including non-disclosure of information, sexual affairs, business secrets, and non-observance by others. It might be claimed that privacy is the polar opposite of publicity; if anybody publishes intimate letters to a friend without his express or implied agreement, his privacy will be violated. Similarly, peering into one’s neighbor’s house from the outside is a violation of one’s right to privacy. Privacy is recognized in many places and cultures across the world, and it is guaranteed in the Universal Declaration of Human Rights and several other International and Regional Human Rights Treaties. The 1948 Universal Declaration of Human Rights, which specifically guarantees geographical and communication privacy, is the global norm for modern privacy. No one should be subjected to arbitrary interference with his privacy, family, home, or communications, or to attacks on his honor or reputation, according to Article 12. Everyone has a legal right to be protected from such interference or violence. In India, we want a robust legal framework as well as clear concepts of privacy. The right to privacy was first established via judicial activism. It is not a fundamental right, but it is an essential component of one. Numerous court rulings, starting back to Kharak Singh and continuing to the present day, mention such a privilege in Article 21. The Criminal Procedure Code of 1973, the Indian Penal Code of 1860, the Hindu Marriage Act of 1955, the Children Acts of 1960, the Indian Easement Act of 1882, the Indian Contract Act of 1872, the Information Technology Act of 2000, the Right to Information Act of 2005, the Indian Post Office Act of 1898, the Credit Information Companies Act of 2005, and the Copy Right Act of 1957 all mention the right to privacy.*

**Keywords:**Right to Privacy, Legislative Framework, Judicial Response, Pre & Post Independence Development.

# Introduction

In India, law and social order are inextricably linked. The law as a regulator of all the societal relationships must, therefore, be sensitive to the evolving social needs, as it is the primary duty of the law to serve society. Our ancient and classical heritage is our legal heritage.[[2]](#footnote-2)Though the law has in great measure been transformed, it is based on its old heritage, as a part of its development our social values have made a considerable progress in the process of modernization. Though the law in general and the right to privacy in particular, has evolved, there are some elements which have remained unchanged, or as it were, embedded in our ancient and traditional legal structure. The law and values of our tradition, being the basic elements in the evolution of our legal system, have a strong influence on the formulation of the new ideas, concepts, and rules. This traditional Indian legal system had been subject to the influences of Islamic law, the law of the ancient Greeks, and Roman law, and it can be said that the Indian legal tradition has been enriched and modified to a considerable extent by foreign influences. However, even the influences of the British civil law on the Indian law have given it a particular flavor and character.

The history of the law in India dates back to very remote antiquity, and traces of our legal system appear in the ancient Hindu texts. The law was the part of our society even before it was reflected in the Vedas. Even in these ancient texts, some of our legal ideas, social values, and customs have been preserved. The earliest Hindu law books which include rules and regulations were codified in the first millennium BCE. Since then the legal philosophy has undergone various modifications. In the last millennium, there was a strong influence from Arabic law on India, and the legal philosophy was modified and influenced by the religious and philosophical principles which had spread in India, especially with the growth of Islam in India.[[3]](#footnote-3)

# The Right to Privacy: The Development in India

In terms of the growth of privacy, India lags significantly behind both the United States and the United Kingdom. In India, the lack of active judicial enforcement, clear legislative enactments, and public debate on the topic has resulted in the growth and development of the Right to Privacy in a negative direction. Surprisingly, India has a rich historical foundation and a well-developed privacy legislation dating back to the ancient times. The origins of privacy in India may be traced in ancient Hindu Jurisprudence, namely in the descriptions of homes in the Grihya-Sutras, Kautilya’sArthashastra, and the epics of Ramayana and Mahabharata. During the medieval period, Muslim women were observed to observe ‘purdah’ in order to avoid public display of their faces. The Quranic injunctions also established privacy standards for both men and women. As a result, it was only in the contemporary time that this right’s development experienced some deterioration and underdevelopment.

Unlike in the United States and the United Kingdom, India’s privacy laws are not founded on the Law of Confidentiality; rather, it has been regarded as a Customary Right from ancient times. The current development of the Right to Privacy in India was characterized by a very ancient case, Nuth Mull vs. Zuka-Oollah Beg and KureemOollah Beg, in 1855. It was the first Indian case determined by the SadarDiwaniAdalat of the Northwestern Provinces in 1855 that raised the issue of the right to privacy. This case demonstrates that the Right to Privacy was widely acknowledged in India at least a half-century before it was introduced in the United States of America in 1890. The Court ruled in this case that the building of a home should not be done in such a way that the other premises may be seen from the roof of the new house, infringing on their right to privacy. As a result, the Customary Right to Privacy has existed in India from ancient times.

Though the growth of privacy in India in the contemporary time has suffered from some deterioration, this does not imply that there has been no privacy legislation in India. During this time, it was regarded a customary privilege and an easement right. Furthermore, several British Indian legislations include specific legal provisions pertaining to privacy. The courts of British India have also issued a number of judgements in support of privacy protection based on either a customary right or an easement right. In addition, since independence, the Indian judiciary has actively promoted the establishment of privacy as a constitutional right as well as acknowledgment of it as a basic right. As a result, while the process of developing privacy in India throughout the contemporary period has slowed, it has never been static. However, the evolution of privacy in contemporary India may be split into two distinct periods: -

## The Development of Privacy in the Pre-Independence Period

The social structure of pre-independence or British India was modernized via urbanization and industrialization. Furthermore, the expansion of knowledge has improved Indians’ awareness of privacy, while technological developments have brought new dangers to privacy. All of these incidents, taken together, have prompted the British government to take efforts to safeguard privacy through legislative and judicial initiatives. As a result, the process of developing Privacy in India has begun. Section 26 of the Indian Post Act of 1898[[4]](#footnote-4), for example, enables the Central and State Governments to intercept mail items during public crises and for the protection of public safety or calm, but only by written order. Furthermore, several sections of the Telegraph Act of 1885 and the Post Office Act of 1898 violate individual privacy through telephone monitoring and mail censorship. As a result, changes are necessary to modify the legislation. As a result, the pre-independence period in India was exposed to numerous legislative changes on the Right to Privacy, demonstrating that Indian legislators have always attempted to protect privacy rights.

## The Development of Privacy in the Post-Independence Period

The post-independence period in India has been characterized as a period of substantial progress in the realm of the Right to Privacy. However, the independent India did not consider the Right to Privacy from the outset. Furthermore, no measures for the preservation of privacy were done at the time the Indian Constitution was drafted in 1950. In reality, the need for this right’s protection only became apparent later on. After 1950, vestiges of privacy were discovered in several Indian statutes, such as the provisions for In Camera procedures in various marital acts, such as the Hindu Marriage Act, 1955 and the Special Marriage Act, 1954. These are the major advancements in the field of privacy in India.

Though the Indian Constitution does not specifically mention the preservation of privacy in India, there are a few times in the Constituent Assembly Debates where privacy is discussed. In the Constituent Assembly, for example, Mr. Karimuddin offered an amendment to a clause to the draft Article 14,196 that was comparable to the protection of the Right to Privacy from search and seizure as described in the 4th Amendment to the United States Constitution. Dr. B. R. Ambedkar advocated this viewpoint during the creation of the Indian Constitution, although it was ultimately futile owing to disagreements among the other Constituent Assembly members. In reality, the Indian Constitution’s drafters failed to see the need of include the right to privacy as a basic right in the Indian Constitution. The legislative history of the Constitution clearly demonstrates this.[[5]](#footnote-5)

Due to the greater influence of the British legal system than the American legal system at the time of the drafting of the Indian Constitution in 1950, the Right to Privacy was not proclaimed as a basic right or other constitutional right. Furthermore, because the Indian legal system is founded on English common law, the Indian judiciary has never acknowledged the right to privacy. However, the Indian judiciary has steadily become more liberal, and with the extension of Article 21 of the Indian Constitution in the Maneka Gandhi case in 1978, the right to life and personal liberty has taken on new significance. When the concept of ‘Personal Liberty’ was broadened to cover many additional rights, the Right to Privacy was incorporated. As a result, a new age of judicial growth of the Right to Privacy has begun in accordance with Article 21 of the Indian Constitution. The first case for privacy protection in this age wasKharak Singh vs. State of U.P.[[6]](#footnote-6) Since then, the right to privacy has been evolved in India on a case-by-case basis, and it is continuously evolving to include many new areas of privacy.

As a result, the Indian judiciary’s actions have enhanced the process of developing the Right to Privacy in India. However, several legislations, such as the Right to Information Act of 2005 and the Information Technology Act of 2000, have been established at the same time that are damaging to individual individuals’ private rights. In the contemporary era, these are the two contentious laws that represent a major danger to the individual’s right to privacy. The sole glimmer of light in this circumstance is the Right to Privacy Bill, 2011, now known as the Privacy Bill, 2011, which has the potential to make substantial changes in the realm of privacy in India.[[7]](#footnote-7)

# Right to Privacy and legislative framework

In advent of information technology and internet and specifically the exposure to global market, it had become essential to provide some protection to the commercial activities in India. With this specific intention, Information Technology Act, 2000 was enacted. The object of this Act is to facilitate ecommerce mainly. The main provisions related to transactions by electronic data interchange and other means of communications are provided in the Act. The government has enacted various Rules governing the protection of privacy and empowering the government under the Act.[[8]](#footnote-8) These provisions are discussed in the following paragraphs.

## Information Technology Act, 2000

The Information Technology Act, 2000 was enacted with the objective of providing legal framework for facilitating e-commerce, e-governance and protecting privacy of individuals. After enactment of the Act, information and communication technology through internet has engulfed almost all human activities at alarming speed. Almost all transactions of businesses and also the governments were done through internet. Due to its omnipotent and omnipresent nature, security, confidentiality and privacy was threatened. There were only two options, either to enact new legislation covering the protection of transactions done through information and communication technology via internet or amend or modify the existing legal provisions under Act. Indian Government has chosen the second option of amending the IT Act, 2000. The government selected to amend and enact some more provisions in the existing Act instead of enacting new legislation for data protection. This Act was amended in 2008 and its scope is widened. It covers many new activities including provisions for data protection and crimes.

## Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 were passed to provide control. It provides the procedure to conduct interception. But privacy of the persons is thought of as it is provided that such interception requires prior approval from the competent authority i.e. Secretary in Ministry of Home Affairs, in case of Central Government and Secretary in charge of Home department in case of State Government. In the cases of emergency different procedure is to be followed. The purpose for interception must be the same which is specified in S. 69(1) of Information Technology Act, 2000, i.e. for protection of sovereignty and integrity of India. It is mandatory to record reasons for Interception. Interception is permitted for the period of 60 days and on renewal not to exceed 180 days.

Intercepted communications shall be kept confidential not only by intermediaries but their employees. Rule 25 prohibits its disclosure except to the officer of authorized agency who can use such information only for specified uses pursuant to direction of competent authority. Rule 23 prescribes that unless the intercepted information is required by law, it should be destroyed after six months.[[9]](#footnote-9)

The power of interception is regulated with the provision that competent authority shall first verify whether there are alternative means to acquire the information. If it is observed that such alternative mean or method is not available then and then only the direction for interception, monitoring or decryption is issued. Government’s power to intercept or monitor or decrypt without finding other means to get information is checked and regulated by this and interests of individuals are protected. After interception, monitoring and decryption, the data is collected and used by the government. There are two actions, one is interception, monitoring and decryption of information and other is monitoring and collection of traffic data or information. For collection of traffic data, interception is essential. For these two actions different legislations are enacted.[[10]](#footnote-10)

# Privacy Bill

After the EU Directive in 1995, the law relating to data privacy was much stronger in countries outside India. But in India, lone privacy legislation in the form of Information Technology Act, 2000 and Rules enacted under it was trying to provide protection.

The Information Technology Act, 2000 was a lone act covering protection for e-commerce transactions, facilitating e-governance and providing privacy of person. The main function of legislation pertaining to electronic communication that is protection of personal information or data is not provided substantially. As threats on privacy, confidentiality and security of personal information or data are increased and resulted in loss to concerned individuals, the demand forprivacy and data protection law gained force. The demand for enactment of such legislation was increasing, the Government had drafted two bills which were proposing the Right to Privacy and data protection. But they were not finalized and enacted in law.[[11]](#footnote-11)

# Information Technology Law and Right to Privacy

India has information Technology Act which provides protection for personal data or information in limited sense. Basically, it provides the legal framework for protection of such data or personal information and provides for privacy for information related to business transactions. Privacy Rules are made in 2011 under this Act. But these regulations are not covering privacy encroachments which are the outcome of the processing of personal data by new and advanced technology. The process of enacting law takes time, within which the technology advances by leaps and bounds.[[12]](#footnote-12)

Protection of privacy of personal information is crucial for maintaining the person’s liberty and freedom. It becomes possible when the rules, regulations and legislations are enacted against the violation by any entity including government.

The concept of right to privacy has undergone a sea change with the advent of technology. In the preceding chapters, the researcher has discussed the development of the concept of Privacy at length. Also, in the above discussion, the researcher has discussed and analyzed the Information Technology Act, 2000 with the Rules and guidelines. Also, the various legislative attempts at data protection have been discussed. After studying and analyzing the above legislations, it has been observed that there is an interface between Right to Privacy and Information Technology Act. Also, it has emerged from the above discussion that the enactment of Information Technology Act, 2000 was not sufficient to cover the right to privacy issues arising over of data protection.

The law has to maintain balance between rights of people and interests of the State. A study of the laws in European Union show that it has tried to control violation of informational privacy by providing guidelines and regulations forpersonal data protection. Member countries of European Union have adopted these regulations. Many other countries like UK and USA have also enacted the legislations for privacy of personal data or information.

India has also attempted to enact a legislation for Data Protection. The protection of Data, the right to manage and control the data, choice and control over data, disclosure of information, power to intercept / encrypt the data, security of information, are a few privacy issues which remain unaddressed by the Information Technology Act and press an urgent need for a separate legislation for protection of informational Privacy in this digital age.

# Conclusion and Suggestions

Right to Privacy is a valuable human right for every individual of past, present and future society. It is a variable concept and varies with the passage of time, place and society. Therefore, it is not easy to define ‘Privacy’ in strict sense of the term. Privacy generally means, the right to be let alone (Justice Cooley, 1888). In 1890, Louis Brandeis and Samuel Warren published a seminal article in the Harvard Law Review, titled “The Right to Privacy,” where it was observed that, the object of Privacy is to protect ‘inviolate personality.’ Next important landmark in the field of Privacy, is the book written by Prof. Alan F. Westin, titled “Privacy and Freedom,” 1970. It defines Privacy as the desire of individuals for solitude, intimacy, anonymity and reserve. According to him, Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent, information about them is communicated to others.

Adam Carlyle Breckenridge in his book, “The Right to Privacy” (November, 1971), has described Right to Privacy as “A most Comprehensive Right.” In view of Carlyle, Privacy is the rightful claim of the individual to determine the extent to which he wishes to share himself with others and his control over the time, place and circumstances to communicate with others. It means, his right to withdraw or to participate as he thinks fit. It is also the individual’s right to control dissemination of information about himself and it is his own personal possession.

Therefore, Right to Privacy cannot be described as a single human right, rather it is a bundle of rights and it includes human being’s choice over his or her own personal affairs to decide the extent of public disclosure of the same. In briefPrivacy means, freedom from unauthorized and unwarranted intrusion into one’s private and personal life. In the modern age, various new dimensions of Right to Privacy have been emerged, like Privacy of Family, Home and Correspondence, Privacy of Marriage, Privacy of Information, Workplace Privacy, Privacy of Celebrity Life, Health Care Privacy and so on.[[13]](#footnote-13)

In order to analyses the Privacy Bills and Data Protection Bills and to study their provisions towards protecting the right to privacy, an in - depth study of the Bills was also done. The researcher also studied in detail the Information Technology Act, 2000, and Rules made under the Act

The researcher analyzed the Information Technology Act, 2000, Rules made under it for privacy of personal data or information, 2011, and rules for interception of data by the government, 2009, which are primary legislations. These legislations nowhere expressly and elaborately provided for person’s informational privacy and data protection in era of continuously and fast developing technology. This protection is essential for personal, informational and decisional privacy of a person. The researcher has inferred that legislation suffers from the following loopholes:

1. Information Technology Act, 2000 is protecting the provisions regarding privacy of sensitive personal data or information in a limited sense under S. 43A. But the definition of sensitive personal data is not provided under it.
2. The term ‘sensitive personal data’ is defined in Rule 3 under Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which is delegated legislation for rule making power provided under S. 43A. This means these rules can made or can be amended by the executive officer empowered by Central Government. These rules are not made by Parliament by conducting discussion on the matters. Threat to privacy is more likely when rules are made by delegated/subordinate legislation.
3. Sensitive personal data is to be protected by ‘body corporate’. The explanation to S. 43 A provides the definition for ‘body corporate’ include the firm, company or association engaged in commercial or professional activities. This not applicable to the government as it is not engaged in commercial activities.
4. It covers liability of body corporate only possessing or handling the sensitive personal data or information in negligent way. But there are many other ways and methods by which such data is compromised or misused or abused.
5. Information Technology Act, 2000 and the Rules made under it are not providing for cross border transfer and processing of data.
6. The government is providing services to citizens through electronic media using information technology. Personal information is also gathered with the government but government’s responsibility is nowhere provided.
7. In many situations, government actions are resulting into violation of privacy of person. Information Technology Act, 2000 and Rules made under it do not provide any protection against these actions. Under these legislations, government’s liability is not provided for.
8. Responsibility of intermediaries are provided in Information Technology Act, 2000 on open ended terms. Any activity can be covered under it for exclusion of the responsibility. Moreover, the liability of cloud service providers is not provided specifically.

**REFERENCE**

**Books**

* The Constitutional Law Of India:- By- Dr. J.N Pandey.
* Indian Constitutional Law:- By- Prof. Mp Jain.
* The Right To Information Act,2005: A Handbook:- By- SudhirNaib.
* Right To Information Act In India: Concepts And Problems:-Ritu Banerjee.

**Statutes**

* The Constitution of India.
* Right to Information Act, 2005.

**Articles**

* Privacy And Human Rights: An International Survey Of Privacy Laws And Practices
* Right To Privacy: An Analysis Of Developmental Process In India, America And Europe:- By- Shriniwas Gupta And Preeti Mishra.
* Privacy And The Constitution:- By- N.S Nappinai
* Fight Between Right To Privacy And Right To Know:- By- Adv. Vishal K Vora
* The Right To Privacy In The Information Era : A South Asian Perspective:- By: AlthafMarsoof.

**Case Laws**

* Kharak Singh v. State of Uttar Pradesh AIR 1963 SC1295: (1964) 1 SCR 332
* Malak Singh v. State of Punjab and Haryana, AIR 1981 SC 760, 763 : (1981) 1 SCC 420
* District Registrar and Collector v. Canara Bank, (2001) 1 SCC 496, 515: 2000 Supp (5) SCR 496.
* United States v. Miller, 425 US 435 (1976)
* Poe vs. Ullman, 367 US 497 at 522
1. Director & Dean Academics

Indore Institute of Law [↑](#footnote-ref-1)
2. Supreme Court of India Civil Original Jurisdiction Writ Petition (Civil) No. 494 Of 2012.2017, Retrieved From: http://main.sci.gov.in/supremecourt/2012/35071/35071\_2012\_Judgement\_24-Aug-2017.pdf ,Retrieved on 10-10-2021. [↑](#footnote-ref-2)
3. Lukasz Olejnik, “India's Data Protection Bill Threatens Global Cybersecurity,” Wired, February 8, 2020, https://www.wired.com/story/opinion-indias-data-protection-bill-threatens-global-cybersecurity/. [↑](#footnote-ref-3)
4. Section 26 of the Indian Post Act of 1898. [↑](#footnote-ref-4)
5. M.P. Jain, “Indian Constitutional Law,” LexisNexis, (2018). [↑](#footnote-ref-5)
6. AIR 1963 S.C. 1295 [↑](#footnote-ref-6)
7. DikshaMunjal, “Personal Data Protection Bill: Compliance Costs to Rise for India Inc,” BusinessLine, March 3, 2020, https://www.thehindubusinessline.com/info-tech/personal-data-protection-bill-compliance-costs-to-rise -for-india-inc/article30971116.ece [↑](#footnote-ref-7)
8. GauravGoyal&Ravinder Kumar, “The Right to Privacy in India: Concept and Evolution,” Patridge Publishing India, (2016). [↑](#footnote-ref-8)
9. SuyashRai, “A Pragmatic Approach to Data Protection,” The Leap Blog, accessed on May 10, 2020, https://blog.theleapjournal.org/2018/02/a-pragmatic-approach-to-data-protection.html. [↑](#footnote-ref-9)
10. KarishmaMehrotra, “Explained: The Issues, Debate Around Data Protection Bill,” The Indian Express, December 7, 2019, https://indianexpress.com/article/explained/personal-data-protection-bill-cyber-security-hacking-61530 15/. [↑](#footnote-ref-10)
11. “India’s Personal Data Protection Bill, 2019,” accessed on October 23, 2021, https://www.pwc.in/assets/pdfs/consulting/cyber-security/data-privacy/indias-personal-data-protectionbill-2019.pdf [↑](#footnote-ref-11)
12. DikshaMunjal, “Personal Data Protection Bill: Compliance Costs to Rise for India Inc,” BusinessLine, March 3, 2020, https://www.thehindubusinessline.com/info-tech/personal-data-protection-bill-compliance-costs-to-rise -for-india-inc/article30971116.ece [↑](#footnote-ref-12)
13. “Right To Privacy: Surveillance in the Post-Puttaswamy Era,” Bloomberg Quint Opinion, November 12, 2019,

https://www.bloombergquint.com/law-and-policy/right-to-privacy-surveillance-in-the-post-puttaswamy

-era. [↑](#footnote-ref-13)