



# The Right to Privacy: A Fundamental Human Right in the Digital Age

MS. MAMTABEN DANABHAI PATEL  
Research Scholar at HNGU- Patan, (Gujarat)

## Abstract:

*The right to privacy is a foundational and universally recognized human right that has evolved over time to adapt to the changing landscape of technology and information. In an era characterized by unprecedented advancements in communication, surveillance, and data collection, the concept of privacy has gained paramount importance. This abstract explores the historical development of the right to privacy, its significance in contemporary society, and the challenges it faces in the digital age. Beginning with a historical perspective, the paper traces the origins of the right to privacy, emphasizing its emergence as a fundamental human right in international legal frameworks and national constitutions. It delves into landmark legal cases and milestones that have shaped the modern understanding of privacy as an essential element of human dignity and autonomy. The abstract then examines the contemporary relevance of the right to privacy, especially in the context of rapidly evolving technologies such as the internet, social media, and surveillance systems.*

*Furthermore, the abstract discusses the challenges and debates surrounding the right to privacy in the digital age. These include issues related to mass surveillance, data breaches, the balance between national security and individual privacy, and the ethical implications of emerging technologies like artificial intelligence and biometrics. The abstract also considers the role of governments, corporations, and individuals in safeguarding and promoting the right to privacy.*

*In conclusion, the right to privacy remains a cornerstone of human rights, even as technology reshapes the boundaries of personal space and information. Understanding the historical context, contemporary relevance, and ongoing challenges of this fundamental right is crucial for policymakers, legal scholars, and society as a whole as they grapple with the complex interplay between technological innovation and individual privacy. The protection of the right to privacy in the digital age requires a delicate balance between innovation and preservation of human dignity, autonomy, and personal freedoms.*

---

**Keywords:** *Privacy, Technology, Social media, Security, Fundamental Rights, Issue And Challenges, Protection.*

---

## 1. Introduction

Privacy is a fundamental human right enshrined in many international treaties. It is important for the protection of human dignity and is one of the important pillars of a democratic country. It supports the rights of self and others. Privacy is a right that all human beings enjoy by virtue of their existence. It also extends to physical integrity, individual autonomy, free speech, and freedom to move, or think. This means that privacy is not only about the body, but extends to integrity, personal autonomy, data, speech, consent, objections, movements, thoughts, and reputation. Therefore, it is a neutral relationship between an individual, group, and an individual who is not subject to interference or unwanted invasion or invasion of personal freedom. All modern societies recognize that privacy is essential and recognize it not only for humanitarian reasons but also from a legal point of view. The terms of privacy and the right to privacy cannot be easily conceptualized. Privacy uses the theory of natural rights and often corresponds to new information and communication technologies. Privacy is our right to maintain the

territory around us, including everything that belongs to us, including our bodies, homes, possessions, thoughts, feelings, secrets, identities, etc. Your privacy allows you to choose what parts of this area can be accessed by others and to control the scope, method, and duration of the parts you choose to disclose.

A recent development in the Indian jurisprudence is the widening of the scope of Article 21 particularly post the case of *Maneka Gandhi vs. UOI* (1978). The Supreme Court has time and again laid down that Article 21 is the basic foundation of fundamental rights. Article 21 has proven to be multi-faceted. The scope of Article 21 has been widened by reinterpreting what constitutes life and liberty in specific circumstances. These terms, that is life and liberty, are not one size fits for all terms. In order to understand the Right to Privacy, it becomes necessary to look into what constitutes privacy. According to Black's Law Dictionary, "right to be let alone; the right of a person to be free from any unwarranted publicity; the right to live without any unwarranted interference by the public in matters with which the public is not necessarily concerned". In order to widen the scope of Article 21, the Supreme Court has decided to interpret it along with the Universal Declaration of Human Rights.

The right to privacy is not formally advocated as a fundamental right in the Constitution. The right to privacy came into light in *Kharak Singh v the State of U.P* (1962) where the main issue was pertaining to surveillance of suspects.

## 2. What is privacy

Privacy is a fundamental concept that relates to an individual's right to control their personal information and to keep it protected from unauthorized access or disclosure. It encompasses various aspects of a person's life, including their personal data, communications, physical space, and personal choices. Privacy is essential for safeguarding individual autonomy, dignity, and freedom. Key aspects of privacy include:

A. Information Privacy: This aspect focuses on an individual's right to control their personal data. It involves the collection, use, and disclosure of personal information, such as name, address, financial records, medical history, and more. Privacy laws and regulations often govern how organizations handle individuals' data.

B. Communication Privacy: Communication privacy pertains to the confidentiality of conversations, messages, and correspondence. It covers forms of communication like phone calls, emails, text messages, and private messaging apps. People expect that their communications will remain private and not be intercepted or accessed without their consent.

C. Physical Privacy: Physical privacy concerns the right to control access to one's personal space, such as their home or private property. It also includes the ability to maintain bodily privacy, meaning individuals have the right to decide who can touch or access their body.

D. Privacy of Personal Choices: This aspect of privacy relates to the freedom to make personal choices without unwarranted interference or judgment. It includes decisions about one's lifestyle, beliefs, religion, sexuality, and other personal matters.

E. Surveillance and Security: Privacy also involves protection against unwarranted surveillance, both by government entities and private individuals or organizations. This can include issues like government surveillance programs, video surveillance in public places, and the use of technologies like facial recognition.

F. Data Protection and Security: With the rise of the digital age, data privacy has become a significant concern. Individuals have a right to expect that their personal data is securely stored and protected from data breaches and cyberattacks.

G. Consent and Control: Central to privacy is the idea of informed consent. Individuals should have the right to decide how their personal information is collected, used, and shared. They should also have the ability to exercise control over their data.

The concept of privacy varies across cultures, legal systems, and contexts. In many countries, privacy is considered a fundamental human right, enshrined in laws and regulations. These laws often set the boundaries for how organizations and governments can handle personal information and engage in surveillance. Balancing privacy with other important societal interests, such as security and public safety, is an ongoing challenge in the digital age.

### 3. Right to privacy versus fundamental right

The "right to privacy" and the concept of "fundamental rights" are closely related but not identical terms. Let's see the differences: -

#### **Right to Privacy:**

The right to privacy is a specific aspect of fundamental rights that pertains to an individual's right to control their personal information, autonomy, and private life. It encompasses various facets of personal privacy, such as information privacy, communication privacy, physical privacy, and more, as explained in the previous response. The right to privacy is often considered a fundamental human right in many legal systems and international agreements, such as the Universal Declaration of Human Rights.

#### **Fundamental Rights:**

Fundamental rights are a broader category of rights that are considered essential and inherent to human beings. They form the foundation of a just and democratic society, ensuring that individuals are protected from abuses of power and discrimination. Fundamental rights include a wide range of civil, political, economic, social, and cultural rights. These can vary from one country to another but often include rights like freedom of speech, freedom of religion, the right to a fair trial, and more. The term "fundamental rights" often encompasses the right to privacy as one of its components. In summary, the right to privacy is a specific subset of fundamental rights that deals with protecting an individual's personal information and private life. Fundamental rights, on the other hand, encompass a broader array of rights that are considered fundamental to human dignity and freedom. The right to privacy is typically recognized as one of these fundamental rights in many legal systems worldwide, and it is essential for safeguarding personal autonomy and individual liberties.

### 4. Right to privacy as per Indian laws

In India, the right to privacy is a fundamental right protected by the Constitution of India. It was affirmed as a fundamental right by the Supreme Court of India in a landmark judgment in 2017. The right to privacy is primarily protected under Article 21 of the Indian Constitution, which guarantees the right to life and personal liberty. Here's an overview of the right to privacy as per Indian laws:

i. Constitutional Basis: The right to privacy is considered an integral part of the right to life and personal liberty under Article 21 of the Indian Constitution. This means that any action by the state or private entities that infringes upon an individual's personal privacy must meet certain constitutional standards of reasonableness and necessity.

ii. Landmark Judgment: In August 2017, the Supreme Court of India, in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India, declared that the right to privacy is a fundamental right protected by the Constitution. The judgment recognized privacy as a natural right inherent in every individual.

iii. Scope of Right to Privacy: The right to privacy in India is not an absolute right but is subject to reasonable restrictions imposed by law to protect legitimate state interests, such as national security and public order. It encompasses various aspects of privacy, including informational privacy, bodily privacy, communication privacy, and more.

iv. Data Protection and Privacy Laws: India has also enacted data protection and privacy laws to regulate the collection, use, and processing of personal data. The Personal Data Protection Bill, 2019 (now known as the Personal Data Protection Act, 2021) is a significant piece of legislation that aims to protect individuals' data privacy rights.

v. Judicial Safeguards: Indian courts, including the Supreme Court, have played a crucial role in interpreting and safeguarding the right to privacy. They have issued rulings to protect individuals'

privacy rights in various contexts, such as surveillance, government actions, and technology-related matters.

vi. Balancing of Interests: The right to privacy in India is not absolute, and the courts often engage in a balancing act between the right to privacy and other legitimate state interests, such as national security and public order.

It's important to note that the right to privacy in India, like in many other countries, is evolving and subject to judicial interpretation and legislative developments. The legal framework is continually adapting to address emerging issues related to privacy in the digital age, including issues like data protection, surveillance, and the use of emerging technologies.

## 5. Issue and challenges for right to privacy

The right to privacy is a fundamental human right recognized in various international treaties and constitutions. However, in today's digital age, several issues and challenges have emerged that can undermine individuals' privacy rights. Here are some of the key issues and challenges associated with the right to privacy:

1. Data Collection and Surveillance: Mass Surveillance: Governments and private companies have access to vast amounts of personal data through surveillance programs, both online and offline, which can infringe on individual privacy.
2. Data Brokers: The buying and selling of personal data by data brokers can lead to the aggregation of extensive profiles on individuals without their knowledge or consent.
3. Data Breaches: The frequent occurrence of data breaches can expose individuals' personal information, leading to identity theft, fraud, and other privacy violations.
4. Inadequate Security Measures: Many organizations do not implement robust security measures, making it easier for malicious actors to access sensitive data.
5. Tracking and Profiling: Online platforms use tracking technologies to collect user data and create detailed profiles for targeted advertising, often without user consent.
6. Cookie Consent Fatigue: Users are often bombarded with cookie consent pop-ups, leading to a lack of meaningful choices and awareness of privacy settings.
7. Biometric Data and Facial Recognition: The widespread use of facial recognition technology by governments and corporations raises concerns about mass surveillance, false positives, and the potential for abuse.
8. Privacy in the Workplace: Employers may monitor employees' activities, both online and offline, which can create a hostile work environment and infringe on individual privacy.
9. Lack of Control: Individuals often lack control over their personal data, as it is collected, processed, and shared without their informed consent or knowledge.
10. Legal and Regulatory Challenges: Laws and regulations related to privacy may lag behind technological advancements, making it challenging to protect privacy adequately. Conflicting laws and regulations in different jurisdictions can create legal uncertainty for individuals and organizations.
11. Social Media and Public Sharing: Individuals often share personal information on social media platforms, sometimes unknowingly, leading to a loss of privacy.
12. Emerging Technologies: New technologies, such as Internet of Things (IoT) devices and artificial intelligence, can collect and analyze personal data in ways that individuals may not fully understand or control.
13. Cultural and Ethical Considerations: Cultural norms and ethical considerations vary widely, affecting how different societies perceive and protect privacy rights.
14. Government Access and Surveillance Laws: Some governments pass laws that grant them broad surveillance powers, often in the name of national security, which can infringe on individual privacy.
15. Digital Literacy: Many individuals lack the digital literacy necessary to understand and protect their online privacy effectively.

Addressing these challenges and safeguarding the right to privacy requires a combination of legal reforms, technological innovations, education, and public awareness campaigns to ensure that individuals' privacy rights are respected in the digital age.



## 6. The supreme court's Aadhaar judgement and the right to privacy

The Aadhaar Act grants residents the right to receive an Aadhaar number by submitting biometric and demographic information as part of the enrolment procedure. The Supreme Court was tasked with determining whether the Aadhaar Act's provisions were infringing on the right to privacy, which was declared a fundamental right by the Supreme Court in 2017. In this regard, it's worth noting that a number of services supplied by both private businesses and the government required an individual to link their Aadhaar number for authentication, effectively making obtaining an Aadhaar number necessary for the vast majority of people. As a result, the question was not so much whether this constituted an infringement of the right to privacy, but rather whether it was a legitimate exemption. Certain sections of the Aadhaar Act were overturned or read down by the Supreme Court because they failed to meet the aforesaid proportionality standard. Apart from these provisions, however, the Supreme Court found that the Aadhaar Act serves a legitimate state goal and is proportionate, making it a justifiable exception to the right to privacy.

## 7. Cases related to right to privacy in India

The right to privacy in India has gained significant legal recognition and protection through various landmark cases. Here are some key cases related to the right to privacy in India:

1. *Kharak Singh v. State of Uttar Pradesh* (1962): This case is one of the earliest cases addressing the right to privacy in India. The Supreme Court held that the right to privacy is not explicitly mentioned in the Indian Constitution but is implied as part of the fundamental rights. However, the court also stated that the right to privacy is not an absolute right and can be restricted by the state for certain valid reasons.
2. *R. Rajagopal v. State of Tamil Nadu* (1994): This case recognized the right to privacy as an inherent part of the right to life and personal liberty under Article 21 of the Constitution. It also established the "Right to be Let Alone" and the concept of privacy in matters related to one's personal life, reputation, and dignity.
3. *P.U.C.L. v. Union of India* (1997): In this case, the Supreme Court upheld the right to privacy in the context of telephone tapping. The court laid down guidelines and safeguards that must be followed by the government when intercepting telephone conversations to protect individuals' privacy rights.
4. *Naz Foundation v. Government of NCT of Delhi* (2009): While primarily known for decriminalizing homosexuality, this case also emphasized the importance of privacy in matters of sexual orientation and intimate relationships. It recognized the right to privacy as a fundamental right and a cornerstone of human dignity.
5. *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017): This landmark case, also known as the "Aadhaar case," established the right to privacy as a fundamental right explicitly under Article 21 of the Indian Constitution. The Supreme Court held that privacy is an integral part of individual liberty and dignity and cannot be infringed upon unless the state demonstrates a compelling reason to do so. This case had far-reaching implications for data protection and surveillance issues in India.
6. *Justice K.S. Puttaswamy (Retd.) v. Union of India II* (2018): This case further clarified and expanded upon the principles laid down in the earlier Puttaswamy case. The Supreme Court held that the state must ensure that any restrictions on the right to privacy are narrowly tailored, proportionate, and comply with the principles of legality, necessity, and legitimacy.

These cases represent significant milestones in the development and protection of the right to privacy in India. They have had a profound impact on various aspects of Indian law, including data protection, surveillance, and individual freedoms.

## 8. Recommendation for right to privacy

Protecting the right to privacy is essential in the modern digital age where personal information is often vulnerable to various threats. Here are some recommendations for safeguarding the right to privacy:

- a. **Strengthen Legal Protections:** Enact and enforce comprehensive privacy laws that clearly define individuals' rights and the responsibilities of organizations that collect and process personal data.

- Establish strict penalties for data breaches and violations of privacy rights to incentivize organizations to prioritize data security.
- b. Data Minimization and Purpose Limitation: Encourage organizations to collect only the data that is strictly necessary for their intended purpose and avoid excessive data collection. Ensure that organizations obtain informed and explicit consent from individuals before collecting and processing their personal information.
  - c. Transparency and Accountability: Require organizations to be transparent about their data practices, including data collection, processing, and sharing. Establish mechanisms for individuals to access and control their own data, including the ability to correct inaccuracies and request the deletion of personal information.
  - d. Data Encryption and Security: Promote the use of strong encryption to protect data both in transit and at rest. Encourage organizations to implement robust security measures to safeguard personal data from cyberattacks and data breaches.
  - e. Biometric Data Regulations: Implement regulations governing the collection and use of biometric data, such as facial recognition, to protect individuals from unwarranted surveillance and privacy violations.
  - f. International Collaboration: Foster international cooperation on privacy standards and data protection to ensure consistency and facilitate cross-border data flows while protecting privacy rights.
  - g. Consumer Education: Promote digital literacy and educate individuals about their privacy rights, how to protect their data, and the potential risks of oversharing on social media and other online platforms.
  - h. Privacy by Design: Encourage organizations to adopt a "privacy by design" approach when developing products and services, ensuring that privacy considerations are integrated from the beginning.
  - i. Independent Oversight: Establish independent privacy oversight bodies with the authority to investigate and address privacy violations by both public and private organizations.
  - j. Whistleblower Protection: Implement laws and protections for whistleblowers who expose privacy violations, encouraging individuals within organizations to report misconduct without fear of retaliation.
  - k. Ethical AI and Technology Development: Promote the ethical development and use of emerging technologies, including artificial intelligence and machine learning, with a focus on minimizing bias and respecting privacy.
  - l. Periodic Privacy Audits: Require organizations to conduct regular privacy audits to assess compliance with data protection regulations and ensure ongoing adherence to privacy best practices.
  - m. Public Awareness Campaigns: Conduct public awareness campaigns to inform individuals about the importance of privacy and their rights, emphasizing the need to be cautious about sharing personal information online.
  - n. Protection of Vulnerable Groups: Implement additional safeguards and protections for vulnerable populations, such as children, the elderly, and marginalized communities.
  - o. Regular Review and Updating of Laws: Periodically review and update privacy laws and regulations

To keep pace with technological advancements and evolving privacy challenges. Safeguarding the right to privacy requires a multifaceted approach involving governments, organizations, individuals, and the technology industry. These recommendations aim to strike a balance between protecting privacy and enabling the benefits of the digital age.

## 9. Conclusion

Privacy rights are essential elements of life and personal freedom rights under Article 21. Privacy rights are not absolute rights. They are subject to rational limitations for the protection of crimes, disadvantaged, or morality, or the protection of other human rights. If there is a contradiction between the two derived rights. If one looks at the later judgments of the Apex Court one can observe the

desirability of the court to treat the basic rights as water-tight compartments. This was felt foremost within the case of A.K Gopalan v. the State of Madras (1950) and also the relaxation of this stringent stand may well be felt within the decision of Maneka Gandhi v. Union of India (1978). The right to life was considered to not be the embodiment of mere animal existence, but the guarantee of a full and meaningful life.

Being a part of society often overrides the very fact that we are individuals first. Each individual needs their private space for whichever activity (assuming here that it shall be legal). The state accordingly gives each person the right to enjoy those private moments. Clinton Rossiter has said that privacy could be special reasonable independence that may be understood as a trial to secure autonomy in a minimum of some personal and spiritual concerns. This autonomy is the most special thing that the person can enjoy. They are truly free humans there. This is often not a right against the state, but against the planet.

### References

1. <https://indiankanoon.org/doc/1199182/>
2. [www.manupatra.com](http://www.manupatra.com)
3. [www.ssc.online.com](http://www.ssc.online.com)
4. [www.lexisnexis.com](http://www.lexisnexis.com)
5. <https://indiankanoon.org/doc/127517806/>
6. <https://indiankanoon.org/doc/1218090/>
7. <https://indiankanoon.org/doc/1199182/>
8. <http://www.legalservicesindia.com/article/1630/Right-To-Privacy-Under-Article-21-and-the-Related-Conflicts.html>
9. <https://www.thehindu.com/news/national/the-lowdown-on-the-right-to-privacy/article19386366.ece>
10. <https://www.hindustantimes.com/india-news>
11. <https://www.mondaq.com/india/privacy-protection/744522/the-supreme-court39s-aadhaar-judgement-and-the-right-to-privacy>
12. [www.sodhganga.com](http://www.sodhganga.com)
13. constitution of India by J.N Pandey
14. Justice K.S.Puttaswamy(Retd) vs Union Of India on 26 September, 2018
15. <http://docs.manupatra.in/newline/articles/Upload/1B38C47D-03C1-4F59-8B9C-8AA3FE39B3E5.pdf>.