



Right to Privacy: A Fundamental Right in the Digital Era

Dr. K.L. CHANDRASHEKHARA¹

¹ Asst. Professor of Law, Vidyavardhaka Law College (Affiliated to Karnataka State Law University), Sheshadri Iyer Road, MYSURU -570001 KARNATAKA.

Article Info

Article History:

Published: 23 June 2026

Publication Issue:

Volume 3, Issue 6
June-2026

Page Number:

274-285

Corresponding Author:

Dr. K.L.
CHANDRASHEKHARA

Abstract:

In the era of digital revolution, where our mornings do not begin with the rising sun, but with the notification sound of our smartphones, from sending messages on WhatsApp, checking for updates, joining online classes, making payments, every activity in our day-to-day life revolves around our smartphones. By every tap, swipe, and click on our smartphones during our daily routine, we are sharing our personal data and giving consent without thinking for a second about where and how our information may be used. When we willingly tap 'Agree' or click 'Accept' countless times, few of us fully read the agreement in which we are entering that to what extent our personal data is collected, shared with the other parties. This effortless flow of personal data has created an uncontrolled and unregulated domain of data, this makes digital privacy not just a matter of personal interest, but a fundamental right of every citizen that requires protection under the law. The Supreme Court of India in the landmark case of K.S. Puttaswamy vs. Union of India recognized the Right to Privacy as a Fundamental Right and laid down the foundation for the protection by extending it to digital privacy.

Keywords: Right to Privacy, Digital Privacy, Human Dignity, Fundamental Right, Protection of Privacy

1. Introduction

The right to privacy is a fundamental entitlement that underpins numerous other human rights and is crucial for personal autonomy and the protection of human dignity. By enabling individuals to establish boundaries and establish barriers to shield themselves from external influences, privacy grants us the liberty to determine our interactions with the outside world and shape our own identities. Setting boundaries for who can access our bodies, places, and belongings, as well as our communications and information, is made easier by privacy.

Right to Privacy means the ability of an individual to determine when, how and to what extent their personal information can be shared with communicated with others. This personal information can be someone's name, location, contact, online or real-world behaviour.

According to the Oxford Dictionary of Law, privacy is the "right to be left alone." We may comprehend this term to mean that the right to privacy is the freedom to maintain the confidentiality of our personal data. Electronic communication, sexual orientation, professional activity, and even emotions or intelligence can all be considered forms of personal information.

Just as someone may want to exclude people from their private communications, many online users want to control or restrict their personal data from collection.

Privacy is an intrinsic element of human dignity and autonomy. The right to privacy protects individuals from unwarranted intrusion into their personal lives, home, correspondence, and information. In the modern digital age, where data is constantly collected, analysed, and monetized, the significance of privacy has become increasingly critical. This article examines the evolution, legal framework, judicial interpretations, and contemporary challenges surrounding the right to privacy, with special emphasis on India's constitutional jurisprudence.¹

In India, the right to privacy was formally recognized as a fundamental right under Article 21 of the Constitution through the landmark judgment of Justice *K.S. Puttaswamy v. Union of India* (2017)². This transformation from an implied concept to an enforceable fundamental right marked a watershed moment in Indian constitutional law.³

2. Historical Evolution of the Right to Privacy

Global Perspective

The concept of privacy has evolved significantly over centuries. In the United States, the Supreme Court first recognized the “right to privacy” in *Griswold v. Connecticut* (1965)⁴, deriving it from the “penumbras” of other explicitly stated constitutional protections like the First, Third, Fourth, Fifth, and Ninth Amendments.⁵ Before this judicial recognition, Louis Brandeis (later a Supreme Court Justice) co-authored a seminal Harvard Law Review article titled “The Right to Privacy,” advocating for the “right to be let alone.”⁶

Key American cases that extended the right to privacy include:

- *Eisenstadt v. Baird* (1971)⁷: Extended privacy rights to unmarried couples regarding contraceptives.
- *Roe v. Wade* (1973)⁸: Recognized a woman's right to abortion under privacy rights.
- *Lawrence v. Texas* (2003)⁹: Extended privacy rights to sexual conduct between persons of the same sex.¹⁰

However, the right to abortion was overturned in *Dobbs v. Jackson Women's Health Organization* (2022)¹¹, demonstrating that privacy rights remain contested.¹²

¹ Journal article, “Right to Privacy under Article 21 in the Digital Era: Constitutional Challenges and Prospects,” Zenodo, June 19, 2025.

² (2017) 10 SCC 1 and AIR 2017 SC 4161.

³ *Ibid.*

⁴ 381 U.S. 479 (1965).

⁵ Legal Information Institute, “right to privacy | Wex | US Law,” Cornell Law, accessed June 13, 2026.

⁶ *Ibid.*

⁷ 405 U.S. 438 (1972).

⁸ 410 U.S. 113 (1973).

⁹ 539 U.S. 558 (2003).

¹⁰ Legal Information Institute, “right to privacy | Wex | US Law,” Cornell Law, accessed June 13, 2026.

¹¹ 597 U.S. 215 (2022).

¹² *Ibid.*

3. Evolution of Right to Privacy

When addressing the authority to search and confiscate documents from the Dalmia Group in the 1954 case of *M.P. Sharma v. Satish Chandra*¹³, an eight-judge Supreme Court bench rejected the existence of a right to privacy on the basis that the makers of Constitution. As there is no provision in Constitution of India that deals with the right to privacy, it can't be violated as well.

After ten years (about), our quest for a private existence reappeared before a six-judge Supreme Court bench in the case of *Kharak Singh v. State of Uttar Pradesh*¹⁴, only to be turned down once more. The Supreme Court ruled that there is no such thing as a basic right to privacy, but it also struck down the part that permitted night time visits on the grounds that it violated "personal liberty." As expressed in opposition by Justice Subba Rao, who claimed that although while the Indian Constitution does not explicitly recognize the right to privacy as a basic freedom, it is nevertheless a necessary component of individual freedom. This famous disagreement helped initiate the development of the right to privacy.¹⁵

After eleven long years, the Supreme Court ruled in *Gobind v. State of Madhya Pradesh*¹⁶ that there is a fundamental right to privacy under Article 21. This decision was made by a smaller three-judge bench. Even though Gobind was defeated, privacy won for the first time and received small recognition under the Indian Constitution's provisions for personal liberty. Supreme Court recognise the significance of right to privacy but said that it should give way to a larger state interest.

By this time, our fundamental rights were the foundation of privacy. It has never seen a more formidable opposition to its continued existence than it did in the 2017 case of *K.S. Puttaswamy v. Union of India*,¹⁷ the decision delivered in 2018 by a nine judge bench read the right to privacy within the ambit of Art. 21.

The fundamental right to privacy is crucial for individuals, and the personal liberty court overturned a previous ruling by *M.P. Sharma and Kharak Singh*,¹⁸ which stated that the Indian Constitution did not safeguard privacy.

In its ruling, the bench stated the following:

1. Recognizing the right to privacy does not necessitate altering the constitution; instead, it simply requires interpreting its existing provisions.
2. Privacy protects personal relationships, marriage, procreation, sexual orientation, and other aspects.
3. Privacy can also be defined as the ability to be alone.
4. Entering a public space does not automatically mean forfeiting one's right to privacy.

¹³ 1954 AIR 300, 1954 SCR 1077, Right to Privacy in the Digital Age, <https://lawvs.com/articles/the-right-to-privacy-in-the-digital-age>, accessed 14 June 2026.

¹⁴ 1963 AIR 1295, 1964 SCR (1) 332.

¹⁵ *Ibid.*

¹⁶ AIR 1975 SC 1378.

¹⁷ (2017) 10 SCC 1 and AIR 2017 SC 4161.

¹⁸ AIR 1963 SC 1295.

5. The constitution should be interpreted broadly to accommodate technological advancements and foster growth and development.
6. Although the right to privacy is a fundamental right, it is not absolute.
7. Acknowledging the right to privacy as a fundamental right safeguards an individual's inner life from interference by both governmental and non-governmental entities.

Indian Perspective

In India, the right to privacy was not explicitly mentioned in the original Constitution. Early judicial decisions debated whether privacy was a fundamental right:

- *M.P. Sharma v. Satish Chandra* (1954): The Supreme Court held that the right to privacy was not a guaranteed fundamental right.¹⁹
- *Kharak Singh v. State of Uttar Pradesh* (1963): The Court reiterated that privacy was not a fundamental right but acknowledged its importance in a democratic society.²⁰

For decades, privacy remained an implied right under Article 21 (protection of life and personal liberty), but it was not explicitly recognized as a standalone fundamental right until 2017.

Constitutional Foundation in India

Article 21 and Privacy

Article 21 of the Indian Constitution states: “No person shall be deprived of his life or personal liberty except according to procedure established by law.”²¹ The Supreme Court has progressively interpreted “life” and “personal liberty” to include various unenumerated rights, including privacy.

The evolution occurred through several landmark judgments:

1. *Gopalan v. State of Madras* (1950)²²: Initial interpretation of Article 21.
2. *Maneka Gandhi v. Union of India* (1978)²³: Expanded Article 21 to include “right to live with human dignity.”
3. *Rajagopal v. State of Tamil Nadu* (1994)²⁴: Recognized privacy as part of Article 21.
4. *Justice K.S. Puttaswamy v. Union of India* (2017): Explicitly declared privacy a fundamental right.²⁵

The Puttaswamy Judgment (2017)²⁶

¹⁹ AIR 1954 SC 300, iPleaders, “Right to privacy - Different aspects of right to privacy under Article 21,” February 4, 2024.

²⁰ AIR 1963 SC 1295.

²¹ “Right to Privacy under Article 21 in the Digital Era: Constitutional Challenges and Prospects,” Zenodo, June 19, 2025.

²² AIR 1950 SC 27.

²³ AIR 1978 SC 597.

²⁴ AIR 1995 SC 264.

²⁵ AIR 2017 SC 4161.

²⁶ *Ibid.*

In a nine-judge bench unanimous decision, the Supreme Court held that the right to privacy is an intrinsic part of Article 21. The key observations included:

- Privacy is an integral element of the spirit of liberty and dignity of the individual.²⁷
- Privacy includes protection of one's body, home, correspondence, information, and decisions.
- Privacy is not an absolute right and can be restricted under certain conditions.²⁸

Any infringement on privacy must satisfy the test of:

1. **Legality:** There must be a law authorizing the intrusion.
2. **Necessity:** The intrusion must be necessary for a legitimate state aim.
3. **Proportionality:** The intrusion must be proportionate to the objective sought.

This judgment transformed privacy from an implied right to a constitutionally enforceable fundamental right, fundamentally altering India's constitutional landscape.

Philosophical Foundations of Privacy

Three philosophical pillars underpin the modern conception of privacy:

1. Dignity

Privacy protects human dignity by allowing individuals to maintain their self-respect and avoid being reduced to objects of scrutiny. When personal information is exposed without consent, it can diminish an individual's sense of dignity.²⁹

2. Autonomy

Privacy enables individuals to exercise autonomy over their personal lives, choices, and decisions. It allows people to control what information about them is shared, with whom, and under what circumstances.³⁰

3. Individuality

Privacy protects individuality by creating spaces where people can develop their unique identities, beliefs, and personalities without external pressure or judgment. It allows for the formation of authentic self-expression.³¹

These pillars collectively justify why privacy is essential for a free and democratic society.

Categories of Privacy

Privacy is not a monolithic concept; it encompasses several dimensions:

²⁷ *Ibid.*

²⁸ *Ibid.*

²⁹ NeGD, "The Right to Privacy: History, Philosophy, and Law," April 22, 2026.

³⁰ *Ibid.*

³¹ *Ibid.*

1. Bodily Privacy

Protection from physical intrusion, including medical examinations, genetic testing, and bodily surveillance. This includes issues like forced sterilization, drug testing, and biometric data collection.

2. Spatial Privacy

Protection of one's home, property, and private spaces from intrusion. This includes unlawful searches, surveillance in private spaces, and intrusion into residential areas.

3. Communicational Privacy

Protection of correspondence, communications, and conversations from unwarranted surveillance. This includes telephone conversations, emails, letters, and digital communications.

4. Informational Privacy

Protection of personal data and information from unauthorized collection, use, and disclosure. This is increasingly critical in the digital era with data collection by governments and corporations.³²

5. Decisional Privacy

Protection of personal decisions regarding lifestyle, relationships, reproduction, and other intimate matters from state interference. This includes decisions about contraception, abortion, and sexual conduct.

Key Judicial Cases on Privacy in India

1. Justice K.S. Puttaswamy v. Union of India (2017)³³

This is the most significant privacy case in India. The nine-judge bench unanimously declared privacy a fundamental right. The judgment established that:

- Privacy is intrinsic to Article 21
- Privacy includes informational privacy
- Privacy restrictions must satisfy legality, necessity, and proportionality tests

2. Supporting Aadhaar Challenge (2018)

Following Puttaswamy, the Aadhaar scheme (biometric-based identity system) was challenged as violating privacy rights. The Supreme Court, in *K.S. Puttaswamy v. Union of India (2017)*³⁴, held that:

- Aadhaar is constitutional but with limitations
- Mandatory Aadhaar for welfare benefits is acceptable
- Mandatory Aadhaar for bank accounts and PAN cards is not acceptable

³² RSIS International, "Data Protection Vis- A- Vis Right to Privacy," July 20, 2025.

³³ AIR 2017 SC 4161.

³⁴ AIR 2017 SC 4161.

- Data protection measures must be strengthened

3. Pegasus Spyware Controversy (2021)

The revelation that Pegasus spyware was used to hack phones of politicians, journalists, and activists raised serious privacy concerns. The Supreme Court ordered an independent expert committee to investigate, acknowledging the gravity of digital surveillance threats.

4. Navtej Singh Johar v. Union of India (2018)³⁵

While primarily about LGBTQ+ rights, this judgment reinforced decisional privacy by striking down Section 377 of the Indian Penal Code, which criminalized homosexual conduct. The Court held that personal choices regarding intimate relationships fall within the realm of privacy.

5. Common Cause v. Union of India (2018)³⁶

This case recognized the right to die with dignity as part of privacy rights, establishing that individuals have the autonomy to make end-of-life decisions.

Right to Privacy in the Digital Era

Contemporary Challenges

The digital revolution has fundamentally transformed privacy landscapes:

1. State Surveillance

Governments worldwide, including India, employ surveillance technologies for national security and crime prevention. However, unchecked surveillance threatens privacy. India lacks a comprehensive surveillance law, and programs like the National Intelligence Grid (NATGRID) operate with limited oversight.³⁷

2. Artificial Intelligence and Machine Learning

AI systems collect and analyse massive amounts of personal data, often without explicit consent. Algorithms can predict behaviour, preferences, and even political views, creating privacy risks.³⁸

3. Social Media Profiling

Social media platforms collect extensive user data for advertising purposes. Users often unknowingly consent to data collection through terms of service. This profiling can lead to manipulation, discrimination, and loss of autonomy.³⁹

4. Large-Scale Data Analytics

³⁵ AIR 2018 SC 4321.

³⁶ AIR 2018 SC 1665.

³⁷ Journal article, "Right to Privacy under Article 21 in the Digital Era: Constitutional Challenges and Prospects," Zenodo, June 19, 2025.

³⁸ *Ibid.*

³⁹ *Ibid.*

Corporations and governments use big data analytics to aggregate information from multiple sources, creating detailed profiles of individuals. This “data fusion” can reveal intimate details about people’s lives.⁴⁰

5. Biometric Data Collection

India’s Aadhaar system collects biometric data (fingerprints, iris scans) of over 1.3 billion people. While useful for identity verification, it creates massive databases vulnerable to breaches and misuse.⁴¹

The Digital Personal Data Protection Act, 2023

India enacted the Digital Personal Data Protection Act (DPDPA) in 2023 to address informational privacy concerns. Key features include:

- **Data Principal Rights:** Individuals can access, correct, and erase their personal data.
- **Data Fiduciary Obligations:** Organizations must collect data lawfully, with consent, and for specified purposes.
- **Data Protection Authority:** An independent body to oversee compliance.
- **Cross-Border Data Transfer:** Regulations on transferring data outside India.
- **Penalties:** Significant fines for violations.

However, critics argue that the Act:

- Grants excessive exemptions to the government.
- Lacks strong enforcement mechanisms.
- Does not adequately address state surveillance.

Privacy vs. National Security: The Balancing Challenge

One of the most contentious issues is balancing privacy rights with national security concerns. Governments argue that surveillance and data collection are necessary for:

- Preventing terrorism
- Cracking organized crime
- Monitoring foreign threats
- Maintaining public order

However, privacy advocates contend that:

- Mass surveillance infringes on fundamental rights
- Security measures often lack judicial oversight
- Surveillance can be used for political repression.
- Less intrusive alternatives exist

⁴⁰ *Ibid.*

⁴¹ *Ibid.*

The Supreme Court's proportionality test in *Puttaswamy* provides a framework: any privacy infringement must be necessary and proportionate to the security objective. Mere assertion of national security is insufficient without demonstrating actual necessity.⁴²

Privacy as a Human Right: International Perspective

International Instruments

The right to privacy is recognized in several international human rights instruments:

1. Universal Declaration of Human Rights (1948): Article 12 states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."⁴³
2. International Covenant on Civil and Political Rights (1966): Article 17 similarly protects privacy rights.⁴⁴
3. European Convention on Human Rights (1950): Article 8 guarantees the right to respect for private and family life.⁴⁵
4. General Data Protection Regulation (GDPR): The EU's comprehensive data protection framework sets global standards for informational privacy.⁴⁶

Criticisms and Limitations

1. Lack of Enforcement Mechanisms

Despite recognizing privacy as a fundamental right, India lacks robust enforcement mechanisms. The Data Protection Authority under DPDPA has not been fully operationalized, leaving gaps in implementation.

2. Government Exemptions

The DPDPA grants broad exemptions to the government, allowing data collection without consent for "state functions." Critics argue this undermines the Act's purpose.

3. Surveillance Without Oversight

India lacks a comprehensive surveillance law requiring judicial authorization. Programs like NATGRID and CDR (Call Data Records) collection operate with minimal oversight.

4. Corporate Data Exploitation

Private corporations collect vast amounts of user data with inadequate consent mechanisms. Users often lack meaningful control over their information.

5. Inadequate Public Awareness

⁴² Journal article, "Right to Privacy under Article 21 in the Digital Era: Constitutional Challenges and Prospects," Zenodo, June 19, 2025.

⁴³ NYU Law Global, "A Brief Introduction to the Right to Privacy – An International Perspective," accessed June 13, 2026.

⁴⁴ *Ibid.*

⁴⁵ *Ibid.*

⁴⁶ *Ibid.*

Most citizens are unaware of their privacy rights and how to protect their data. This knowledge gap limits the effectiveness of privacy protections.⁴⁷

Recommendations for Strengthening Privacy Protection

1. Comprehensive Surveillance Law

India should enact a law requiring judicial authorization for surveillance, with clear guidelines on:

- Purpose limitation
- Duration of surveillance
- Data storage and deletion
- Remedies for violations

2. Strengthen Data Protection Authority

The Data Protection Authority must be:

- Fully operationalized with adequate resources
- Independent from government influence
- Empowered to impose significant penalties
- Required to publish transparency reports

3. Eliminate Government Exemptions

The DPDPA should be amended to remove or limit government exemptions, ensuring that state data collection also requires consent and justification.

4. Promote Privacy by Design

Organizations should adopt “privacy by design” principles:

- Collect minimum necessary data
- Encrypt data by default
- Provide user control over data
- Implement data minimization

5. Enhance Public Education

Government and civil society should:

- Launch privacy awareness campaigns
- Provide privacy literacy education in schools
- Create resources for understanding data practices

⁴⁷ RSIS International, “Data Protection Vis- A- Vis Right to Privacy,” July 20, 2025.

- Support privacy advocacy organizations

6. Judicial Oversight

Establish specialized courts or benches to handle privacy cases, ensuring:

- Expert adjudication
- Timely resolution
- Consistent precedents
- Effective remedies

Privacy and Emerging Technologies

1. Blockchain Technology

Blockchain's decentralized nature offers privacy benefits but also challenges:

- Benefits: Immutable records, user control, reduced intermediaries
- Challenges: Public blockchain transparency, irreversibility of data

2. Internet of Things (IoT)

IoT devices collect extensive personal data:

- Smart homes monitor daily activities
- Wearables track health data
- Connected cars record location and behaviour

3. Facial Recognition

Facial recognition systems pose significant privacy risks:

- Mass surveillance capabilities
- Accuracy concerns, especially for marginalized groups
- Lack of regulatory framework in India

4. Quantum Computing

Future quantum computers could break current encryption, threatening data security and privacy. Proactive measures are needed to develop quantum-resistant cryptography.

4. The Future of Privacy Rights

Trends and Outlook

Several trends will shape the future of privacy:

1. Increasing Regulation: More countries will enact comprehensive data protection laws
2. Technology Advancement: New technologies will create both privacy risks and solutions

3. Global Cooperation: International frameworks for cross-border data protection will emerge
4. Individual Empowerment: Tools for privacy management will become more accessible

India's Path Forward

India must:

- Fully implement DPDPA with strong oversight
- Enact surveillance legislation
- Strengthen judicial remedies
- Promote privacy culture
- Balance innovation with protection

The recognition of privacy as a fundamental right in 2017 was transformative, but implementation remains incomplete. The journey from constitutional recognition to practical protection requires sustained effort from government, judiciary, civil society, and citizens.

5. Conclusion

The right to privacy is fundamental to human dignity, autonomy, and individuality. In India, it has evolved from an implied constitutional concept to a recognized fundamental right under Article 21 through the landmark Puttaswamy judgment. This transformation reflects the dynamic interplay between law, technology, and human rights.

However, significant challenges remain. The digital era presents unprecedented privacy threats through state surveillance, corporate data exploitation, and emerging technologies. India's new Digital Personal Data Protection Act, 2023, offers a framework but requires strengthening through robust enforcement, elimination of government exemptions, and comprehensive surveillance legislation.

Privacy is not an absolute right and must be balanced with legitimate state interests like national security. However, any infringement must satisfy the tests of legality, necessity, and proportionality established by the Supreme Court.

The future of privacy depends on:

- Strong legal frameworks
- Effective enforcement mechanisms
- Judicial vigilance
- Corporate accountability
- Public awareness
- Technological innovation for privacy protection

As India continues its digital transformation, maintaining constitutional morality and human dignity requires harmonizing innovation with privacy protection. The right to privacy remains a cornerstone of democracy, and its safeguarding is essential for preserving the freedoms that define a liberal society.