INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 7 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 7 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-7-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 7 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

RIGHT TO PRIVACY IN RELATION WITH SOCIAL MEDIA IN TODAY'S DIGITAL ERA

AUTHOR - PRAGYA PANDEY, VRUSHTI SHAH & HITANSHI PAREKH,

STUDENTS AT KES' SHRI JAYANTILAL H. PATEL LAW COLLEGE, MUMBAI, MAHARASHTRA, INDIA.

BEST CITATION – PRAGYA PANDEY, VRUSHTI SHAH & HITANSHI PAREKH**,** RIGHT TO PRIVACY IN RELATION WITH SOCIAL MEDIA IN TODAY'S DIGITAL ERA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (7) OF 2026, PG. 873-881, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

The right to privacy, though not explicitly mentioned in the Indian Constitution, was unanimously recognized as a fundamental right under Article 21 by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). This paper examines the evolution, constitutional

framework, and contemporary relevance of this right in the context of social media and the digital era.

Privacy is a multidimensional concept encompassing bodily integrity, informational autonomy, communication confidentiality, and spatial freedom. It serves not merely as an individual preference but as a structural precondition for human dignity, democratic participation, and the

effective exercise of all other fundamental rights. Judicially, the right evolved from early denials in M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1963), through progressive recognition in Gobind v. State of M.P. (1975) and R. Raja Gopal v. State of Tamil Nadu (1994), culminating in the landmark Puttaswamy judgment.

In the digital era, social media platforms connecting hundreds of millions of Indians operate on business models that harvest and monetize intimate user data. Citizens face mounting threats including mass data breaches, surveillance through programs like the Central Monitoring

System, corporate data exploitation, deep fake abuse, and structural gaps in the Digital Personal Data Protection Act, 2023 compounded by

widespread digital illiteracy.

To address these challenges, the paper recommends expedited implementation of the DPDP Act, enactment of a Surveillance Accountability

Act, establishment of an independent Data Protection Board, statutory recognition of the Right to Be Forgotten, mandatory privacy-by-design for

platforms, and large-scale digital literacy investment.

Protecting personal data on social media is not merely a regulatory concern it is a constitutional imperative determining whether Indian citizens

engage with the digital world as free and dignified individuals or as commodified data points.

Keywords: Right to Privacy, Article 21, Puttaswamy Judgment, Social Media, Digital Personal Data Protection Act 2023, Data Protection, Fundamental Rights, Surveillance, Aadhaar, Digital Era, Informational Privacy, Constitutional Law, India.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 7 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

I. Introduction: Social Media and Privacy : A threat to Article 21

Privacy is one of the most fundamental human right that protects an individual's personal life from unnecessary interference by others. It is the right of every individual to live freely, without unwanted intrusion into their personal life, thoughts, relationships, or information. It ensures that every person has the freedom to make personal choices, maintain confidentiality, and live with the dignity. It is crucial for preventing identity theft, securing financial information, and maintaining trust in digital public platforms, particularly under the digital Personal Data Protection Act

(DPDPA)

In India, the Right to Privacy was recognized as a fundamental right under *Article 21* (Right to Life and Personal Liberty) by the landmark judgment of Justice K.S. Puttaswamy v. Union of India. The Supreme Court held that privacy is intrinsic to life and liberty, and it includes aspects such as bodily autonomy, informational privacy, and decisional freedom.1.1 Definition of Privacy as a Human Right

Privacy, is not simply about secrecy. It is about control the power of an individual to decide what is shared, with whom, and on what terms. Privacy is not a single, neat concept. . It also serves a deeper psychological function it gives individuals the space to develop their own identity, make autonomous decisions, and participate freely in Society, privacy rights support an individual's right to determine who they are as a person; the right to freely willfully make choices; and the right to fully engage in their own community. Therefore, it is an essential element of both personal well-being as well as a democratic society.

The transformation of our society as a result of digitization is evident every day. The internet was initially only used by researchers and governmental entities but has now became something that billions of individuals use in everyday life. In 2025 there are approximately 5.4 billion (67%) of the world's population who use the internet; there are over 5 billion users of various social media platforms such as Facebook, Instagram, X (Twitter), WhatsApp, YouTube, Snapchat, LinkedIn, and TikTok, which have changed how people interact socially, communicate politically, conduct commerce, and share news and culture. The impact these networks have had on redefining our understanding, definition, range, and insecurity of personal privacy is immeasurable.

A. Evolution of Privacy in India:

Privacy rights have been developed slowly, through legal interpretations by Indian courts over the years. Early on, the courts did not consider privacy to be part of the fundamental rights of Indian citizens. Examples include M.P. Sharma v. Satish Chandra and Kharak Singh v. State of U.P. where the Indian Supreme Court did not recognize right to privacy or protect citizens' rights from wrongful government actions. However as time passed, the courts began to view the right to privacy as part of citizens' right to personal liberty. Ultimately, in Justice K.S. Puttaswamy

v. Union of India, where the Supreme Court ruled, by 9-judge majority, that there was a right to privacy that was part of the fundamental right protected in Article 21 of the Constitution. The Significance of Privacy as a Right in Digital Years.[11354]

II. The Significance of Privacy as a Right in Digital Era:

The global digital shift means that the protection of online individuals has never been more important. Individuals' privacy has protected them from data theft, mass invasion of privacy, and the abuse of your private information. While privacy protects your freedoms of expression, your ability to live independently and participate in democratic processes, privacy is also a fundamental right (2017 Supreme Court ruling) in India. The new Digital Personal Data Protection Act (2023) creates legal protections for your digital data;

[1354] Constitution of India, 1950, Articles 14, 19 and 21 — Part III (Fundamental Rights).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

however, without adequate implementation, the success of the new law will be undermined.

B. Digital Privacy Is Challenging:

The unprecedented increase in the internet, the number of smartphones and devices around us, artificial intelligence (AI), and social media have given us many benefits but many more challenges. You are creating a digital footprint every time you conduct a search online, send a message, conduct a transaction or make any other activity online. Your digital information is continuously collected, stored, and analyzed to derive insights through the billions of transactions being recorded. There is an ever-increasing risk that a third party may obtain, misuse or access your information for unlawful purposes. Therefore, privacy is not just an option; it has become a daily requirement.

1. Identity Theft and Personal Data Protection:

Keeping your privacy secure from identity thieves, fraudsters and cybercriminals helps protect your sensitive personal information such as bank account information, Aadhaar number(s), and medical histories. Globally, the number of data breaches is increasing When personal data is not protected properly, it can result in both financial losses and reputational damage.

The legal framework provides for the security of personal data thereby preventing the use of such data without the consent of the person to whom it pertains.

2. Privacy Risks Associated With AI:

AI collects, analyzes and makes decisions based upon the personal data it collects.

Used in rental agreements, employment/hiring practices, medical decisions. Individuals have limited influence/control over the manner in which their personal data is used, thereby creating a conflict between innovative technologies & protecting the privacy of individuals.

3. Privacy and Free Speech:

In order to communicate freely, Privacy (including protecting one's privacy) is essential to a journalist, activist and citizen's ability to function.

Surveillance results in discouraging individuals from communicating with one another. Metadata tracking can provide enough information to enable others to make conclusions as to the habits and relationships they have When privacy rights are non-existent/diminished, Democracy and Accountability can be destroyed.

4. India's digital privacy law awaits implementation under DPDP Act 2023:

The Digital Personal Data Protection (DPDP) Bill has passed into law and will afford individuals living in India (Data Principals the same rights and protections as their counterparts in Europe under The General Data Protection Regulation Regulations (GDPR). Data Principals will have the right to Access to personal data Amend or correct their information Request the deletion of their data. Businesses will be required to operate under the principle of Privacy by Design.

5. Right to Delete (Right to be forgotten):

Individuals have the right to request removal of outdated or harmful personal information from digital platforms. This right has been recognized by courts in India. This right assists individuals in protecting their reputation and dignity.

This right has not received enough public awareness.[1355]

III. **Online Tracking : Websites and Mobile apps**

a) Cookie-Based Tracking

Third-party cookies track users across websites, building detailed behavioral profiles

[1355] India's surveillance landscape after the DPDPA: IAPP IAPP.org, https://iapp.org/news/a/india-s-surveillance-landscape-after-the-dpdpa (last visited Apr 10, 2026) [6] Defending privacy in the digital age: Reflections for data privacy day 2026 Harvard Kennedy School, https://www.hks.harvard.edu/centers/carr-ryan/our-work/carr-ryancommentary/defending-privacy-digital-age-reflections-data (last visited Apr 10, 2026)

for ad targeting. Google's AdTech network covers ~92% of indexed websites. Its "Privacy Sandbox" replacement has faced regulatory scrutiny for potentially entrenching Google's dominance rather than protecting user privacy.

b) Mobile App Tracking

Apps routinely collect far more data than needed — location, contacts, microphone, and camera. Apple's ATT framework forced apps to ask permission to track, costing Meta $10 billion in 2022 revenue. Period-tracking apps raised serious concerns post-Dobbs that intimate health data could be subpoenaed or sold.

Cybercrime & Hacking

Data breaches have exposed billions of records — Yahoo (3B accounts), Equifax (147M Americans), Aadhaar (1B citizens). Ransomware encrypts organizational data and threatens to leak it publicly, targeting hospitals and governments. Stolen data is openly sold on the dark web for identity theft and fraud.

1. Google

Google aggregates search history, location, emails, health, and financial data across billions of users. Law enforcement uses "geofence warrants" to extract location data, sometimes wrongly implicating innocent people. In 2023, Google paid $391.5M for secretly tracking users even after they disabled location settings.

2. Meta

Meta tracks users across millions of third-party sites via pixel tracking and targets ads using sensitive attributes like health, religion, and politics. A 2021 WhatsApp policy update sparked backlash by sharing user data with Facebook. In 2023, Meta received a record €1.2 billion GDPR fine for illegally transferring EU user data to the US.

A. Case study:

The landmark case *of* *Justice K.S. Puttaswamy v. Union of India* arose from a challenge to the Aadhaar scheme, where the petitioner argued that the collection and use of biometric data violated individual privacy. A nine-judge bench of the Supreme Court unanimously held that the Right to Privacy is a fundamental right protected under Article 21 (Right to Life and Personal Liberty) and is intrinsic to human dignity and freedom. The Court overruled earlier decisions that denied this right and clarified that privacy includes bodily autonomy, personal choices, and informational control. It further established that any infringement of privacy must meet the threefold test of legality, necessity, and

proportionality. This judgment is considered a turning point in Indian constitutional law, as it strengthened the protection of individual rights in the digital age and laid the foundation for data protection and personal liberty jurisprudence.

In Kharak Singh v. State of Uttar Pradesh, the Supreme Court dealt with the issue of police surveillance and its impact on individual liberty. Although the Court did not explicitly recognize privacy as a fundamental right, it held that unauthorized intrusion into a person's home violates personal liberty under Article 21, thereby laying the groundwork for future recognition of privacy right

In R. Rajagopal v. State of Tamil Nadu, also known as the Auto Shankar case, the Supreme Court explicitly recognized the "right to be let alone." It held that individuals have the right to safeguard the privacy of their personal life, and that the publication of private details without consent would amount to a violation of this right, unless justified by public interest.[613561357]

IV. Core Arguments: Social Media as a Threat to Privacy under Article 21

A.Illusion of Consent

Social media platforms claim that users voluntarily consent to data collection through privacy policies. However, such consent is often

[1356] The right to privacy in the age of Social Media: An analysis of Indian jurisprudence IJLLR Journal, https://www.ijllr.com/post/the-right-to-privacy-in-the-age-of-socialmedia-an-analysis-of-indian-jurisprudence (last visited Apr 10, 2026)

[1357] Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors., Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1, AIR 2017 SC 4161 — Supreme Court of India, Nine-Judge Constitution Bench, decided on 24 August 2017.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

not truly informed, as policies are lengthy, complex, and rarely read by users. This creates an illusion of consent, undermining the principles of autonomy and informed choice, which are essential to the Right to Privacy under Article 21.

B.Data as a Commercial Commodity

Social media platforms treat user data as an economic asset. Personal information such as browsing behavior, preferences, and interactions is collected, analyzed, and sold to third parties for targeted advertising. This commodification of personal data reduces individuals to mere sources of profit, thereby affecting their dignity and informational privacy.

1. Surveillance and Tracking Culture

Continuous monitoring of user activity, including location tracking and online behavior, has led to the emergence of a surveillance culture. Users are constantly observed, often without their explicit knowledge, which restricts their freedom of expression and creates a chilling effect on personal liberty.

2. Increased Risk of Cyber Crimes

The widespread use of social media has increased vulnerability to cyber crimes such as identity theft, hacking, data breaches, and deepfake technology. These activities directly infringe upon an individual's privacy and can cause significant personal, financial, and reputational harm.

3. Blurring of Public and Private Spheres

Social media platforms have significantly blurred the distinction between public and private life. Personal information shared online can easily become accessible to a wide audience, often beyond the user's control. This erosion of boundaries weakens the protection of private life under Article 21.

4. Psychological Impact and Loss of Autonomy

Constant exposure and fear of judgment on social media can lead to anxiety, self-censorship, and reduced personal freedom. The pressure to maintain an online presence often compromises individual autonomy, which is a core element of the Right to Privacy.

Thus, while social media enhances connectivity and expression, it simultaneously poses serious challenges to privacy, dignity, and personal liberty guaranteed under Article 21.

V. Challenges to the Right to Privacy in Today's Digital World: The Indian Perspective

A. .The Supreme Court of India recognized privacy as a fundamental right in the landmark case Justice K.S. Puttaswamy v. Union of India (2017). However, simply having this right acknowledged in law does not ensure its proper protection. In today's highly connected digital world, the right to privacy of Indian citizens is encountering challenges that are both vast in scope and complex in nature, and these challenges cannot be fully addressed by a single court ruling or law. The right to privacy, as outlined in Article 21, is now facing unprecedented threats in the digital age of 2025. Issues such as data breaches, surveillance, and misuse of social media are endangering personal freedoms. The rapid growth of digital technologies— like social media, artificial intelligence, and government surveillanceis significantly impacting the right to privacy. This raises concerns about data tracking, government overreach, and the exposure of personal information. The following sections explore the most significant challenges that Indian citizens face in preserving their right to priv acy in this evolving digital landscape.

B. Mass Data Breaches and the Vulnerability of Personal Information

One of the most urgent and immediate threats to privacy in India is the repeated occurrence of largescale data breaches affecting personal information stored in both public and private digital systems. Indian citizens have experienced some of the biggest data breaches globally, exposing the personal details of hundreds of millions of people to criminal misuse. In October 2024, Star Health Insurance, one of the country's leading health

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

insurers, faced a major data breach that compromised the personal details of 31

million customers. A 2023 report from the cybersecurity firm CloudSEK revealed a security incident that exposed the personal information of 750 million Indians, with the data amounting to 1.8 terabytes considered one of the largest data breaches in recent history, affecting around 85% of the population. (Business Standard)

These breaches are not just technical issues they are serious violations of the constitutional right to privacy.

When a citizen's medical records, financial details, biometric data, or home address are made public and sold on underground digital markets, the harm goes beyond material loss. It affects the individual's sense of dignity, autonomy, and personal safety in a way that can ly personal and hard to reverse.

C. The Aadhaar System and Biometric Data Risks

A discussion on digital privacy challenges in India cannot be complete without examining the Aadhaar system— the world's largest biometric identity platform, which has enrolled over 1.4 billion Indian residents and processes about 2.5 billion authentication requests each month.

Although initially designed to streamline welfare programs, the Aadhaar system has grown into a widely used infrastructure that is now essential for banking, telecom services, and AI-driven verification.

While it has been praised as one of the most advanced ID systems globally, it has also drawn criticism due to several data breaches and privacy concerns. In January 2025, the Indian government began allowing private companies to access Aadhaar's infrastructure under a new regulatory sandbox. This development has raised new worries about the potential for misuse of citizens' biometric data by corporations.

State Surveillance and the Absence of Judicial Oversight

Another significant category of privacy challenges comes from the government's own surveillance systems—networks of tools and programs that have expanded rapidly in the digital era, often without proper laws, judicial checks, or public accountability.

India's surveillance infrastructure now includes a wide range of connected systems.

The Central Monitoring System (CMS) gives the government the ability to monitor communications across mobile phones, landlines, and

the internet. This system operates without requiring approval from service providers, allowing for extensive access to personal data. This raises serious conc erns about unchecked government power. A major example of this abuse was the Pegasus spyware scandal of 2021. The revelations shocked the country, exposing the use of advanced spyware to monitor journalists, activists, and political figures. The use of such technology, which can silently take control of a smartphone, access all communications,

and track a person's location without the owner's knowledge, represents one of the most severe threats to privacy. It is targeted, invisible, and leaves no trace.

D. Social Media Platforms and Corporate Data Exploitation

In addition to government surveillance, Indian citizens face serious privacy risks from private companies— especially large technology firms that run the social media platforms, e-commerce websites, and digital payment systems that millions of Indians use daily.

Social media platforms and e-commerce companies gather extensive personal data, often for targeted advertising.

This lack of transparency in how data is handled poses a threat to informational privacy.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

E. Weaknesses in the DPDP Framework and Delayed Citizen Rights

A key institutional challenge to privacy protection in India is the inadequacy and delayed implementation of the legal framework meant to safeguard it. While the DPDP rules grant the government immediate powers, they delay citizens' rights by eighteen months. The core aspects of privacy—

such as informed consent, the right to withdraw permission, the ability to correct or delete data, and enforceable timelines for resolving complaints—will not take effect until mid-2027. (IDR) This means that during this transition period, the government accumulates data governance powers while citizens' rights remain unenforceable.

Additionally, the DPDP Act and Rules weaken the Right to Information Act by allowing an override for disclosure in the public interest.

Citizens seeking transparency can now be denied information simply because it is labeled as

"Personal data," even when public interest demands otherwise. (IDR) This represents a dangerous reduction in transparency, which is essential for democratic accountability[13581359136016136]

VI. Key Legal Rights on Privacy

A. International Law

1.UDHR Article 12 (1948): Prohibits arbitrary interference by the State with a person's privacy, family, home or correspondence; the declaration that privacy is a universal human right.

2.ICCPR, Article 17 (1966): Reaffirmation of UDHR Article 12 and obligates State Parties to ensure the protection of individuals from unlawful interference's in a person's right to privacy by either governments or Private actors.

3.UN Resolution -68/167 Title- "The Right to Privacy in the Digital Age" (Adopted in 2013): States that persons have the same rights online as they have offline and calls for protection against mass digital surveillance.

B. . Is Complete Privacy Possible Today?

Realistically — no. Here's why:

1.Your smartphone alone tracks location, app usage, contacts, and voice commands continuously.

2.Every Google search, YouTube video, and Gmail is logged and profiled.

3.Even "private" browsing only hides history locally — your ISP, Google, and websites still see you.

4.Data brokers legally aggregate and sell your information without your knowledge.

5.Even opting out is largely illusory — Meta's pixel trackers follow you whether or not you have a Facebook account.

6.However, meaningful privacy is still achievable through deliberate choices:

i. Using encrypted tools like Signal, ProtonMail, and Tor.

ii. Switching to privacy-respecting browsers like Firefox or Brave.

iii. Regularly auditing app permissions.

iv. Using a VPN and DNS-over-HTTPS.

Complete privacy in the modern internet is a myth — but informed, active choices can significantly reduce your exposure. Most people, however, lack the technical literacy or time to implement these measures consistently, which

[1358] India's Data Protection Act: A Shield for privacy or a tool for state surveillance? Tech Policy Press, https://www.techpolicy.press/indias-data-protection-act-a-shield-forprivacy-or-a-tool-for-state-surveillance/ (last visited Apr 10, 2026)

[1359] The evolution of Digital Privacy Laws in India: Challenges and reforms Record Of Law, https://recordoflaw.in/the-evolution-of-digital-privacy-laws-in-india-challengesand-reforms (last visited Apr 10, 2026)

[1360] Internet Society's comments on India's Digital Personal Data Protection (DPDP) rules 2025 Internet Society, https://www.internetsociety.org/resources/doc/2025/internet-societys-comments-on-indias-digital-personal-data-protection-dpdp-rules-2025/ (last visited Apr 10, 2026) [16] Public infrastructure and private surveillance in India's Aadhaar System Tech Policy Press, https://www.techpolicy.press/public-infrastructure-and-private-surveillance-inindias-aadhaar-system/ (last visited Apr 10, 2026)

[1361] Digital Personal Data Protection Rules, 2025 — Ministry of Electronics and Information Technology, notified on 13 November 2025.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

is precisely why structural regulation matters more than individual action. [181362]

VII. Critical Opinion — Key Pointers

A. On Big Tech:

- Data extraction is not a side effect but a company strategy.
- GDPR fines are mere operational costs for trillion dollar companies.
- Regulation should target business models as well as individual practices.

B.. On Governments:

- Post-9/11 security climate was exploited to build mass surveillance infrastructure
- PRISM and Pegasus convey a thin line between protecting and controlling citizens ➢ Democratic governments lack credibility criticizing China while running similar programs

C.. On Users:

- Privacy burdens are unfairly placed on the individuals
- Cookies and TOS are deliberately designed in a way to confuse and exhaust the individuals.
- Real consent requires real understanding that current systems prevent actively.

4. Privacy = a human rights issue, and not just a technical one

- Free thought, dissent, journalism, and autonomy are all at risk without it
- Human behavior has become the primary material of profit that is corrosive to democracy and dignity ➢ Core truth: We are already being watched.

But the real question is who controls that data, under what rules, and with what accountability?

VIII. Conclusion:

The right to privacy, recognized as a fundamental right under Article 21 of the Indian Constitution through the landmark judgment of Justice K.S. Puttaswamy v. Union of India (2017), has gained urgent importance in the digital age, something its framers could not have imagined.

Social media platforms, which today connect millions of Indian citizens, have also become the most powerful tools for collecting personal data, profiling user behavior, and influencing people through targeted content. Every action on these platforms — such as posting, searching, messaging, and reacting — creates a trail of personal data that is collected, analyzed, and used for profit, often without the user being fully aware or giving real consent. In this context, privacy is no longer just a legal right; it has become a daily necessity that supports individual freedom, expression, and active participation in democracy.

India has made important progress in safeguarding this right in the digital space.

The passing of the Digital Personal Data Protection Act, 2023, and the introduction of the DPDP Rules, 2025, have established a comprehensive legal system that regulates how social media platforms and other data controllers collect, process, store, and delete personal information. India has now introduced new privacy regulations, limiting the amount of personal data that large tech companies can gather and giving individuals more control over their own information.

However, significant challenges remain. Issues like large-scale data breaches, unchecked government surveillance, weakened regulatory independence, slow implementation of citizen rights, and a wide population lacking digital literacy to exercise or defend their privacy continue to exist. The difference between the constitutional promise and the actual experience of people requires immediate action through legislative reforms, independent institutions, accessible justice, corporate

[1362] James Rachels, "Why Privacy is Important", Philosophy and Public Affairs, Vol. 4, No. 4 (Summer, 1975), pp. 323–333.
Universal Declaration of Humàan Rights, 1948, Article 12 — United Nations, adopted 10 December 1948, G.A. Res. 217A (III), U.N. Doc. A/810 (1948).

responsibility, and ongoing efforts to improve digital literacy for all citizens.

At its core, the issue of privacy in the era of social media is about what kind of constitutional democracy India aims to be.

A society that values privacy sees its citizens as independent individuals deserving of respect, not as data points controlled by algorithms. The Indian Constitution guarantees every person within its borders the right to live with freedom, dignity, and protection from unnecessary interference. Upholding this promise in the digital age where social media has made personal life constantly visible and personal data constantly valuable is the major constitutional challenge of our time. It requires not only strong laws and independent institutions, but also the shared belief that every person's right to control their own story is something worth fighting for.

IX. **References**:-

- M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (India).
- Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India).
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
- Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).
- Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
- Digital Personal Data Protection Rules, Ministry of Electronics and Information Technology, 2025 (India).
- Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810, art. 12 (Dec. 10, 1948
- Privacy International, What is Privacy?, https://privacyinternational.org/explainer/56/what-privacy (last visited Apr. 10, 2026).
- Internet Society, Comments on India's Digital Personal Data Protection Rules 2025, https://www.internetsociety.org/resources/doc/2025/internet-societys-comments-on-indias-digital-personal-data-protection-dpdp-rules-2025/ (last visited Apr. 10, 2026).
- Harvard Kennedy School, Defending Privacy in the Digital Age, https://www.hks.harvard.edu/centers/carr-ryan/our-work/carr-ryan-commentary/defending-privacy-digital-age-reflections-data (last visited Apr. 10, 2026).

INSTITUTE OF LEGAL EDUCATION

(Managed by L TO J LAW ASSOCIATES)

NO. 08, ARUL NAGAR, SEERA THOPPU,
MARUDHAANDA KURICHI, SRIRANGAM - 620102,
TAMILNADU, INDIA.

ISSN 2583-2344