 ISSN: 2349-6002

Privacy and Data Protection: The Expanding Scope of Fundamental Rights

Dr. Saurabh Garg
Dean, Faculty of Law, Tantia University, Sri Ganganagar
doi.org/10.64643/IJIRTV12I6-191390-459

I. INTRODUCTION

The emergence of the digital society has fundamentally transformed traditional understandings of privacy, reshaping how personal identity, autonomy, and liberty are perceived and protected. With the integration of technology into nearly every sphere of human life—ranging from banking, healthcare, education, governance, transportation, communication, and entertainment—individuals constantly generate vast quantities of personal, behavioural, biometric, financial, and sensitive data. This unprecedented datafication of human activity has elevated personal data from a mere informational component to a critical socio-economic and political resource capable of shaping behaviour, influencing democratic choices, determining economic opportunities, and redefining power structures in society.[1]

In earlier legal and philosophical discourse, privacy was largely conceived as the "right to be left alone,"[2] confined primarily to personal solitude and protection from physical intrusion. However, in the contemporary digital ecosystem, privacy encompasses a much broader spectrum. It now includes the right to informational self-determination, decisional autonomy, digital identity protection, and control over how one's personal data is collected, processed, stored, shared, and exploited.[3] As governments increasingly rely on digital governance tools, biometric identification systems, surveillance mechanisms, and data-driven welfare models, and as corporations build powerful economic empires on data analytics, profiling, and behavioural targeting, privacy concerns have moved beyond individual interests to become constitutional, democratic, and civilizational imperatives.[4]

The expansion of digital infrastructures has not only created opportunities for innovation, efficiency, and connectivity but has simultaneously exposed individuals to risks of intrusive surveillance, data manipulation, cybersecurity threats, identity theft, algorithmic discrimination, and corporate exploitation.[5] This evolving environment necessitates a robust legal and ethical framework that recognizes privacy as an indispensable fundamental right essential for dignity, liberty, equality, and democratic participation.[6]

This expanded research, therefore, undertakes a comprehensive examination of privacy and data protection as evolving fundamental rights.[7] It explores their philosophical and international foundations, analyses key judicial developments such as the landmark Indian Supreme Court judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, and evaluates global developments including the European Union's GDPR. Further, it critically examines emerging challenges posed by artificial intelligence,

[1] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019) 12.
[2] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" (1890) 4 Harvard Law Review 193.
[3] Daniel Solove, *Understanding Privacy* (Harvard University Press, 2008) 2.
[4] Julie E. Cohen, "What Privacy Is For" (2013) 126 Harvard Law Review 1904.
[5] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton, 2015) 45.
[6] Raghav Chopra, "Fundamental Right to Privacy in India" (2018) 60(1) Journal of Indian Law Institute 99.
[7] Patrick Breyer, "Data Protection Rights in the Digital Age" (2017) 9 International Data Privacy Law 1.

algorithmic governance, biometric systems, corporate surveillance capitalism, cyber vulnerabilities, and expanding state surveillance. Finally, the study underscores the urgent need for strong regulatory frameworks, independent oversight institutions, technological accountability, ethical digital practices, and informed citizen participation to safeguard privacy in the digital age.

II. CONCEPTUAL FRAMEWORK: UNDERSTANDING PRIVACY AND DATA PROTECTION

Privacy, in modern jurisprudence, is multidimensional. Scholars broadly categorize it into three interrelated domains:

1. Bodily Privacy

This dimension protects individuals from physical intrusion and unauthorized interference with their bodies, including medical data and biometric identifiers.

2. Decisional Privacy

Decisional privacy safeguards autonomy in personal and intimate life choices, including family, reproductive rights, identity, beliefs, and lifestyle. It ensures freedom from coercion and intrusion in personal decision-making.

3. Informational Privacy

The most significant in the digital era, informational privacy concerns control over the creation, storage, access, dissemination, and use of personal data.[8] It ensures individuals retain authority over how their information is collected and utilised.

Data protection is a more technical and regulatory concept. It creates legal obligations governing data processing—ensuring transparency, consent, accountability, security, purpose limitation, and rights of individuals over their data.[9] Thus, while privacy represents a constitutional right, data protection is the mechanism that operationalizes it.

III. PRIVACY AS A FUNDAMENTAL RIGHT: PHILOSOPHICAL AND INTERNATIONAL FOUNDATIONS

Article 21 and the Constitutional Foundation of the Right to Privacy: Article 21 of the Constitution of India states that *"No person shall be deprived of his life or personal liberty except according to procedure established by law."*[10] Over time, this provision has evolved into one of the most dynamic and judicially interpreted constitutional guarantees, extending far beyond mere protection of physical life and liberty. The Indian judiciary has consistently expanded the meaning of "life" to include dignity, autonomy, and the ability to make meaningful personal choices. Within this progressively enriched interpretation, the right to privacy has come to occupy a central position.

Initially, the Supreme Court did not recognize privacy as a fundamental right. Early decisions such as M.P. Sharma v. Satish Chandra (1954)[11] and Kharak Singh v. State of U.P. (1963)[12] rejected privacy as a constitutionally protected right. However, subsequent jurisprudence gradually shifted towards recognizing privacy as intrinsic to personal liberty under Article 21. The transformation was ultimately crystallized in the landmark Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[13] judgment, wherein a nine-judge Constitution Bench unequivocally declared privacy to be a fundamental right, inherent in Article 21 and part of the freedoms guaranteed under Part III of the Constitution.

In the Puttaswamy judgment, the Court held that privacy forms the core of human dignity and autonomy, encompassing various dimensions such as bodily privacy, informational privacy, decisional privacy, and spatial privacy. The Court emphasized that without privacy, the enjoyment of many other fundamental rights—such as freedom of speech, freedom of movement, and the right to personal

[8] Alan Westin, *Privacy and Freedom* (Atheneum, 1967) 31.

[9] Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press, 2014) 8.

[10] Constitution of India, Art. 21.

[11] *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.

[12] *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.

[13] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

liberty—would be rendered incomplete.[14] Importantly, the Court also acknowledged that privacy is not an absolute right; reasonable restrictions may be imposed but only on the basis of a legitimate state interest, with compliance to principles of necessity, proportionality, and legality.

Following this recognition, Article 21 has become the constitutional bedrock for contemporary debates surrounding data protection, surveillance, and digital rights. In an era characterized by increasing technological penetration, mass data collection, biometric identification systems, and artificial intelligence-driven analytics, informational privacy has emerged as a critical concern. The Court has repeatedly highlighted that individuals must retain control over their personal data and that the State must establish legal safeguards to prevent arbitrary intrusion.

The interpretation of Article 21 now obligates the State not only to refrain from unlawful interference but also to actively create a secure legal architecture for protecting privacy in both physical and digital spaces. This is reflected in subsequent judicial and legislative developments, including deliberations on the Digital Personal Data Protection Act, 2023, debates on unlawful surveillance, issues of data breaches, and concerns regarding the misuse of personal information by public and private entities.

Thus, Article 21 has evolved from a narrow guarantee of physical liberty to a comprehensive protector of human dignity, autonomy, and privacy. It stands today as the constitutional cornerstone underpinning the expanding scope of privacy and data protection as fundamental rights in India, ensuring that individual freedoms remain safeguarded against both state overreach and technological exploitation.

Internationally, privacy has been recognized as a human right for decades.

- Article 12[15] of the Universal Declaration of Human Rights protects individuals from arbitrary interference with privacy, family, home, or correspondence.
- Article 17[16] of the International Covenant on Civil and Political Rights reinforces similar protections.

These instruments have influenced constitutional jurisprudence globally, transforming privacy from a moral aspiration into a legally enforceable right.

IV. JUDICIAL RECOGNITION: THE PUTTASWAMY JUDGMENT AND GLOBAL DEVELOPMENTS

A landmark turning point in privacy jurisprudence is the Indian Supreme Court's decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The unanimous nine-judge bench declared privacy as a fundamental right under Article 21 of the Constitution. Importantly, the Court interpreted privacy as intrinsic to dignity, liberty, identity, and personal autonomy. It emphasized informational privacy, recognizing that the digital age demands constitutional protection beyond traditional notions of secrecy.[17]

The Court introduced essential safeguards—legality, necessity, proportionality, and accountability—as prerequisites for any state intrusion into privacy. This decision placed India among progressive constitutional democracies prioritizing digital rights.[18]

Globally, the European Union's General Data Protection Regulation (GDPR) represents a comprehensive and rights-centric data protection regime. It introduces obligations such as explicit consent, the right to access personal data, data portability, the right to be forgotten, and strict penalties for violations. Many countries, including Brazil, South Africa, and Japan, have modeled their frameworks on GDPR, marking a global shift toward recognizing personal data protection as a human right.[19]

[14] Ibid.

[15] Universal Declaration of Human Rights, 1948, Art 12.

[16] International Covenant on Civil and Political Rights, 1966, Art 17.

[17] Gautam Bhatia, *Offend, Shock, or Disturb: Free Speech Under the Indian Constitution* (Oxford University Press, 2016) 122.

[18] Regulation (EU) 2016/679 (General Data Protection Regulation).

[19] Dan Jerker B. Svantesson, *European Union Data Protection Law* (Kluwer Law International, 2014) 61.

V. PRIVACY IN THE DIGITAL AGE: EMERGING DIMENSIONS AND CHALLENGES

1. Surveillance Capitalism
Corporate entities increasingly rely on data analytics to predict and influence consumer behavior. Social media platforms, search engines, and digital service providers collect, profile, and monetize user data. This commodification of personal identity poses risks of manipulation, behavioral control, and erosion of autonomy.[20]

2. State Surveillance and National Security
Governments justify intrusive monitoring systems for national security, crime prevention, and public order. While legitimate in certain contexts, unchecked surveillance threatens civil liberties, enabling mass monitoring, profiling, and political targeting.

3. Cybercrimes and Data Breaches
Cyberattacks, identity theft, phishing scams, ransomware attacks, and unauthorized data dissemination expose individuals to severe financial, psychological, and social harm. Weak security systems and poor regulatory compliance exacerbate risks.

4. Artificial Intelligence, Algorithms, and Big Data
AI systems rely on massive datasets. However, algorithmic decision-making often lacks transparency and may embed bias, discrimination, or unfairness. Decisions affecting employment, education, credit access, and public services increasingly depend on algorithmic assessments, raising ethical and constitutional concerns.

5. Biometric and Genetic Data
The use of facial recognition technologies, biometric authentication, DNA databases, and health-tracking applications introduces sensitive privacy challenges. Such data, if misused, can permanently alter personal identity protection.

VI. BALANCING PRIVACY WITH COMPETING STATE AND SOCIETAL INTERESTS

Privacy is not absolute. States may impose restrictions to address security, law enforcement, and public welfare objectives. However, constitutional democracies require that such limitations:

- Be grounded in lawful authority
- Pursue a legitimate objective
- Be necessary and proportionate
- Remain subject to judicial and institutional oversight

This balance maintains both societal safety and personal liberty, preventing authoritarian overreach.

VII. TOWARDS ROBUST PRIVACY GOVERNANCE: LEGAL AND INSTITUTIONAL IMPERATIVES

For effective privacy protection, nations must develop comprehensive strategies that include:

1. Strong Data Protection Legislation addressing emerging technologies.
2. Independent Data Protection Authorities with enforceable powers.
3. Transparent Corporate Accountability and ethical digital practices.
4. Digital Literacy and Citizen Awareness to ensure informed consent.
5. Technological Safeguards such as encryption, anonymization, and secure architecture.
6. Judicial Vigilance to guard against violation of constitutional guarantees.

Privacy protection is not merely a state responsibility; it requires cooperation between governments, corporations, civil society, and individuals.

VIII CONCLUSION: PRIVACY AND DATA PROTECTION AS CORNERSTONES OF HUMAN DIGNITY, LIBERTY, AND DEMOCRATIC INTEGRITY

The journey of privacy from a limited, individualized notion of personal seclusion to a robust and

[20] Paul Schwartz and Daniel Solove, "The PII Problem" (2011) 86 New York University Law Review 1814.

multidimensional fundamental right reflects the profound transformation of human society in the digital age. Today, privacy is no longer a mere shield against intrusion; it is an empowering right that preserves individual dignity, safeguards autonomy, and reinforces democratic values. As digital technologies continue to penetrate every domain of life, privacy and data protection have become essential tools for maintaining a balanced, just, and humane digital order.

Personal data now constitutes a form of power—capable of influencing opinions, shaping behavior, determining opportunities, and even altering political landscapes. If left unregulated, such power threatens to undermine constitutional freedoms, erode trust in institutions, and reduce individuals to data commodities. Therefore, recognizing privacy as a fundamental right is not merely a legal necessity but a moral and democratic imperative. Judicial pronouncements, particularly the Puttaswamy judgment in India, and global frameworks like the GDPR, signify an important affirmation that individuals must retain control over their personal information and digital identity.

However, recognizing privacy as a right is only the first step. The real challenge lies in translating this recognition into effective protection. The rapid evolution of artificial intelligence, biometric surveillance, predictive analytics, data monopolies, and cyber threats continuously tests existing legal frameworks. This demands adaptive, forward-looking, and enforceable data protection regimes supported by independent regulatory bodies, ethical corporate practices, technological safeguards, and widespread digital awareness. States must ensure that any restriction on privacy remains lawful, proportionate, and subject to strict oversight, preventing the misuse of national security narratives to justify unchecked surveillance.

Ultimately, privacy and data protection embody the essence of human freedom. They protect individuals from being constantly monitored, manipulated, or controlled. They preserve the sanctity of personal choice, foster trust in digital systems, and reinforce the foundational principles of democracy and the rule of law. As societies continue to evolve technologically, safeguarding privacy will determine not only the quality of governance but also the character of civilization itself. Ensuring strong privacy protection is, therefore, not merely about regulating data; it is about upholding humanity, dignity, and justice in an increasingly digital world.