RIGHT TO PRIVACY IN THE DIGITAL AGE

Priya Verma, Amity Law School, Amity University, Lucknow

Dr. Kunvar Dushyant Singh, Assistant Professor (Grade III), Amity Law School, Amity University

ABSTRACT

Technological innovation in the twenty-first century has dramatically reshaped how personal information is created, processed, and exchanged. Digital platforms, biometric identification systems, artificial intelligence, and data analytics have enabled unprecedented access to individual data by both the State and private entities. While these developments have contributed to efficiency and economic growth, they have simultaneously intensified concerns relating to privacy, surveillance, and individual autonomy. In India, the constitutional status of the right to privacy was conclusively settled by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India* (2017), which recognized privacy as a fundamental right inherent in human dignity and liberty. This research paper critically examines the evolution of the right to privacy in India and evaluates its relevance in the contemporary digital environment. It analyses issues such as mass surveillance, corporate data exploitation, biometric identification, and social media intrusion, while assessing the adequacy of India's legal framework for data protection. The paper argues that safeguarding privacy is essential for preserving constitutional democracy in the digital age. This paper undertakes a comprehensive doctrinal and analytical study of privacy in the digital era. It traces the evolution of privacy from its early conceptual foundations to its recognition as a constitutional right in India through *Justice K.S. Puttaswamy (Retd.) v. Union of India*. It evaluates international regulatory frameworks such as the GDPR, examines challenges posed by artificial intelligence and surveillance technologies, and critically assesses India's emerging data protection regime. The paper argues that privacy must be understood as a structural democratic guarantee essential for safeguarding dignity, autonomy, equality, and constitutional governance in a data-driven society.

Keywords: Privacy, Digital Technology, Fundamental Rights, Surveillance, Data Protection, Constitution of India.

Introduction

The rapid advancement of digital technology has profoundly altered modern society. Activities that were once conducted in physical spaces—such as communication, banking, education, and governance—are now largely mediated through digital platforms. Smartphones, social media networks, digital payment systems, and online databases have become indispensable to daily life. As a result, vast quantities of personal data are continuously generated, stored, and analyzed.

While digital technologies have improved access to services and information, they have also exposed individuals to serious privacy risks. Personal data is routinely collected without meaningful consent, stored indefinitely, and often shared with third parties. Surveillance technologies enable continuous monitoring of individuals' activities, both online and offline. These developments raise fundamental questions about the limits of state power, corporate accountability, and individual autonomy.

In constitutional democracies, privacy serves as a safeguard against arbitrary interference by the State and private actors. In India, the absence of an explicit constitutional provision on privacy initially led to uncertainty regarding its legal status. However, judicial interpretation gradually expanded the scope of personal liberty under Article 21. The landmark judgment in *Justice K.S. Puttaswamy v. Union of India* finally affirmed privacy as a fundamental right, particularly relevant in the context of digital governance. This research paper undertakes a comprehensive examination of the right to privacy in the digital age through a constitutional and comparative lens. It seeks to analyze how technological developments have reshaped the meaning and scope of privacy, evaluate the effectiveness of regulatory responses, and assess the implications for democratic governance. The paper advances the argument that privacy must be conceptualized not merely as an individual entitlement but as a structural constitutional guarantee that underpins dignity, autonomy, equality, and participatory democracy.

In a society increasingly governed by data flows and algorithmic systems, the preservation of privacy represents one of the defining legal and ethical challenges of our time. The future of constitutional democracy may well depend upon the capacity of legal institutions to reconcile technological innovation with the enduring values of liberty and human dignity.

Nature and Dimensions of the Right to Privacy

The right to privacy is a multifaceted and evolving fundamental right that safeguards individual autonomy, dignity, and liberty. In India, its constitutional status was firmly recognized in **Justice K.S. Puttaswamy (Retd.) v. Union of India**, where the Supreme Court held that privacy is intrinsic to Article 21 and other freedoms under Part III of the Constitution. The Court clarified that privacy is not an isolated right but intersects with freedoms of speech, movement, association, and personal liberty.

The nature of privacy is both negative and positive. Negatively, it restrains the State from arbitrary interference in personal life. Positively, it imposes an obligation on the State to protect individuals against non-state actors, including corporations and digital platforms. Privacy is not absolute; any restriction must satisfy legality, necessity, and proportionality.

The dimensions of privacy are broad. First, **bodily privacy** protects physical integrity, including protection against forced medical procedures and biometric collection. Second, **informational privacy** concerns control over personal data, especially in the digital age of data analytics and surveillance. Third, **decisional privacy** safeguards intimate personal choices relating to marriage, reproduction, and sexual orientation. Fourth, **spatial privacy** protects private spaces such as the home and communications.

Thus, the right to privacy is dynamic and adaptive, responding to technological developments and social change. It functions as a shield against excessive intrusion and as a foundation for democratic participation and human dignity.

Judicial Development of Privacy Rights in India

a. Initial Resistance to Privacy as a Fundamental Right

In the early years of constitutional interpretation, Indian courts were hesitant to recognize privacy as a fundamental right. In **M.P. Sharma v. Satish Chandra (1954)**, the Supreme Court rejected the argument that search and seizure violated a right to privacy, noting the absence of an explicit constitutional guarantee. Similarly, in **Kharak Singh v. State of Uttar Pradesh (1963)**, the majority held that surveillance measures did not infringe any fundamental right to privacy.

However, the dissenting opinion of Justice Subba Rao in *Kharak Singh* marked a significant departure from this view. He emphasized that personal liberty under Article 21 must include freedom from unwarranted intrusion into private life. Although not immediately accepted, this reasoning influenced later judicial developments.

b. Expansion Through Progressive Interpretation

From the 1970s onwards, the Supreme Court adopted a more expansive understanding of fundamental rights. In **Gobind v. State of Madhya Pradesh (1975)**, the Court acknowledged that privacy could be inferred from Articles 19 and 21, though subject to reasonable restrictions. In **R. Rajagopal v. State of Tamil Nadu (1994)**, the Court recognized an individual's right to prevent unauthorized publication of personal information.

Further, in **People's Union for Civil Liberties v. Union of India (1997)**, the Court held that telephone tapping constitutes an invasion of privacy unless conducted in accordance with a fair and lawful procedure. These decisions collectively paved the way for the formal recognition of privacy as a fundamental right.

Constitutional Recognition in the Puttaswamy Judgment

The constitutional status of the right to privacy was conclusively settled in **Justice K.S. Puttaswamy v. Union of India (2017)**. A nine-judge bench unanimously held that privacy is an integral part of the right to life and personal liberty under Article 21, as well as a component of freedoms guaranteed under Part III of the Constitution.

The Court emphasized that privacy is essential for the realization of dignity, autonomy, and individuality. It rejected the argument that privacy is a privilege enjoyed only by a few, affirming that it is a universal right applicable to all citizens. Importantly, the judgment acknowledged the challenges posed by digital technologies, including data aggregation and surveillance.

The Court formulated a three-fold test to assess restrictions on privacy: the existence of a valid law, a legitimate state objective, and proportionality between the means employed and the objective sought. This framework has become the foundation of privacy jurisprudence in India.

Digital-Age Threats to Privacy

a. State Surveillance Mechanisms

Advances in technology have enhanced the State's capacity to monitor individuals through digital surveillance tools such as internet interception, facial recognition, and data analytics. While such measures may be justified for security and law enforcement purposes, unchecked surveillance risks undermining democratic freedoms. Excessive monitoring can deter individuals from exercising their rights to speech, association, and dissent.

b. Corporate Control Over Personal Data

Private corporations play a dominant role in the digital ecosystem. Technology companies collect and process vast amounts of personal data for targeted advertising, behavioral analysis, and profit generation. Consent is often obtained through complex and inaccessible privacy policies, undermining informed choice. Data breaches and unauthorized sharing further erode trust and individual control.

c. Social Media and Informational Exposure

Social media platforms have transformed communication by enabling instant sharing of personal information, opinions, and multimedia content. However, this widespread connectivity increases informational exposure, often blurring the line between public and private life. Users voluntarily disclose data, but platforms also collect metadata, track behavior, and analyze preferences for targeted advertising and profiling. This creates risks of identity theft, cyberstalking, misinformation, and reputational harm. The permanence and viral nature of online content further intensify these concerns. While social media enhances democratic participation and expression, it simultaneously challenges informational privacy, requiring stronger data protection laws and responsible digital literacy practices.

Aadhaar and Biometric Information

Aadhaar is India's biometric-based identification system administered by the Unique Identification Authority of India (UIDAI). It assigns a unique 12-digit identification number to residents, linked to demographic details and biometric information such as fingerprints, iris scans, and facial photographs. The primary objective of Aadhaar is to ensure efficient delivery

of government subsidies, welfare benefits, and services by eliminating duplication and identity fraud.

Biometric information plays a crucial role in authentication, enabling individuals to access banking services, mobile connections, and public distribution systems. However, the large-scale collection and storage of sensitive biometric data have raised significant privacy and security concerns. Issues such as data breaches, surveillance risks, and misuse of personal information have sparked constitutional debates.

Statutory Framework for Data Protection

a. Information Technology Act, 2000

The Information Technology Act, 2000 contains limited provisions addressing data protection. Sections 43A and 72A impose liability for negligence and breach of confidentiality. However, the Act does not comprehensively regulate data processing, surveillance, or individual rights in the digital context.

b. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 seeks to establish a structured framework for personal data governance. It introduces rights for individuals and obligations for data processors. Despite these advancements, concerns remain regarding broad state exemptions and the effectiveness of enforcement mechanisms. Judicial interpretation will play a crucial role in shaping its impact.

Privacy Versus Public Interest

Privacy and public interest are two competing yet equally significant principles in constitutional democracies. The right to privacy, recognized as a fundamental right under Article 21 of the Indian Constitution in **Justice K.S. Puttaswamy v. Union of India**, protects an individual's autonomy, dignity, and control over personal information. Privacy ensures that individuals can make personal decisions—relating to family, health, communication, and data—free from unwarranted State or public intrusion.

On the other hand, public interest refers to matters that affect the welfare of the community at

large. It justifies limited interference with privacy in situations involving national security, public order, prevention of crime, transparency in governance, or protection of public health. For example, disclosure of information about corruption by public officials or surveillance to prevent terrorism may be defended on grounds of public interest.

However, public interest cannot be used as a blanket justification to invade privacy. Courts apply the tests of legality, necessity, and proportionality to ensure that restrictions are reasonable and not excessive. The balance lies in ensuring that privacy is restricted only when there is a legitimate aim and the least intrusive measure is adopted. Thus, privacy and public interest must coexist through careful constitutional balancing.

International Standards on Privacy

International standards on privacy are rooted in human rights law and data protection frameworks. Article 12 of the **Universal Declaration of Human Rights** and Article 17 of the **International Covenant on Civil and Political Rights** protect individuals against arbitrary interference with privacy, family, home, and correspondence. These instruments recognize privacy as a fundamental human right essential to dignity and liberty.

In the digital era, regional frameworks provide more detailed safeguards. The **General Data Protection Regulation** of the European Union establishes principles such as lawful processing, purpose limitation, data minimization, transparency, and accountability. It also grants rights like access, rectification, erasure ("right to be forgotten"), and data portability. Similarly, the **Convention 108** by the Council of Europe is the first binding international treaty dedicated to data protection.

Additionally, the **Organisation for Economic Co-operation and Development** Privacy Guidelines outline global principles including security safeguards and individual participation. Together, these standards influence national laws worldwide, promoting a balanced approach between technological innovation, state interests, and the protection of individual privacy rights.

Conclusion

The right to privacy in the digital age has emerged as one of the most critical constitutional and human rights concerns of the twenty-first century. Rapid technological advancements, the

widespread use of social media, big data analytics, artificial intelligence, and biometric identification systems have transformed how personal information is collected, stored, and processed. In this environment, privacy is no longer limited to physical spaces; it extends to digital identities, online communications, financial data, and behavioral patterns.

In India, the recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India marked a constitutional milestone. The Supreme Court affirmed that privacy is intrinsic to life and personal liberty under Article 21 and is closely linked to dignity, autonomy, and freedom of choice. However, the digital ecosystem presents constant tensions between individual rights and competing interests such as national security, economic development, and technological innovation.

The challenge lies not merely in recognizing privacy but in ensuring effective protection through robust data protection laws, transparent governance, accountability of corporations, and informed consent mechanisms. Surveillance practices, data breaches, and algorithmic profiling highlight the urgent need for regulatory safeguards and judicial oversight.

Ultimately, the right to privacy in the digital age must evolve alongside technology. A balanced approach—guided by legality, necessity, and proportionality—is essential to preserve democratic values while embracing digital progress. Protecting privacy is not an obstacle to development; rather, it is the foundation of trust, freedom, and human dignity in an increasingly interconnected world.

Reference

Confessore, N., et al. (2018). *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*. *The New York Times*.

European Parliament & Council. (2016). *General Data Protection Regulation (EU) 2016/679*.

Greenwald, G., & MacAskill, E. (2013). *NSA Prism program taps in to user data of Apple, Google and others*. *The Guardian*.

Kumar, R. (2020). *Data Privacy and Aadhaar: Constitutional Perspectives*. *Journal of Indian Law*.

Supreme Court of India. (2017). *Justice K.S. Puttaswamy (Retd.) vs. Union of India* (Privacy Judgment).

UN General Assembly. (1948). *Universal Declaration of Human Rights*.

UN General Assembly. (1966). *International Covenant on Civil and Political Rights*.

UN Human Rights Council. (2013). *Resolution on the promotion, protection and enjoyment of human rights on the Internet*.