DIGITAL PRIVACY VS NATIONAL SECURITY: A CONSTITUTIONAL ANALYSIS

Deona Lita Dsouza, SDM Law College, Mangalore

ABSTRACT

The rapid digitalization of governance and society in India has significantly changed the relationship between individual rights and State power. The rise of surveillance technologies, claimed to be for national security, has increased worries about privacy, autonomy, and dignity. This article draws on Indian legal scholarship and constitutional law to explore the growing tension between digital privacy and national security. It examines how the view of privacy as a fundamental right has shifted, especially after the case of Justice K.S. Puttaswamy v. Union of India. It also assesses whether India's legal framework for surveillance and data protection is adequate. The article argues that while national security is a valid constitutional goal, the lack of strong safeguards and oversight may weaken democratic values and the rule of law. It concludes by promoting a proportionality-based constitutional approach that balances privacy and security.

Keywords: Digital Privacy, National Security, Surveillance, Constitutional Law, India, Data Protection, Fundamental Rights, Cyber Law.

I. Introduction

India's shift to a digitally driven society has reshaped constitutional governance, highlighting the conflict between individual privacy and State security. The widespread use of digital platforms, biometric identification, and data-driven governance has led to continuous personal data collection and processing, making privacy a key issue in current constitutional discussions. Indian scholars note that digital privacy has become crucial as technology becomes more integrated into daily life, with both State and private actors routinely collecting and analyzing personal information.[1] This situation has greatly increased State surveillance, raising fears about the loss of civil liberties.

Meanwhile, the State defends its expanded surveillance powers as necessary for national security, pointing to the need to address terrorism, cybercrime, and threats to public order. Indian academic work highlights that surveillance has grown significantly with advances in digital technology and a greater reliance on online communication, often justified as necessary for security and governance.[2] However, this growth raises a constitutional concern, as the quest for security often intrudes on individual privacy.

The acknowledgment of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India[3] marked a pivotal moment in Indian constitutional law. It requires careful consideration of individual rights against State interests. This article aims to critically analyze this balance through doctrinal analysis and engagement with Indian academic literature.

II. Conceptual Foundations of Digital Privacy and National Security

In India, digital privacy is seen as the right of individuals to control their personal data's collection, use, and distribution. This goes beyond traditional privacy concepts to include informational self-determination and autonomy in digital environments. Indian scholars argue that the digital era has created new challenges for privacy protection, as technologies like artificial intelligence, biometrics, and the Internet of Things deeply penetrate personal and social lives.[4] This change has made it harder to keep personal information secure.

[1] Diksha Taneja & Ganesh Dubey, Digital Privacy: A Legal and Social Perspective in India, 11 JMSG E-J. 1 (2025).
[2] Suja Nayar, Digital Era and Human Rights in India, IERJ (2025).
[3] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
[4] Priyanka Dalal & Richa, Right to Privacy in India, RRIJM (2025).

National security has become a broad concept that includes not only territorial security but also cybersecurity, digital infrastructure protection, and information control. Research shows that the State frequently cites national security to justify surveillance actions, such as intercepting communications and monitoring online activities.[5] While such measures might be needed in some cases, they also risk excessive State intrusion.

The conflict between digital privacy and national security is structural. As Indian scholars point out, the balance often favors the State due to a lack of clear legal boundaries and accountability measures.[6] This imbalance raises important questions about the limits of State power in a democracy.

III. Evolution of Privacy Jurisprudence in India

The development of privacy rights in India shows a gradual change from a strict interpretation to a more substantive understanding of constitutional rights. In early cases like M.P. Sharma v. Satish Chandra,[7] the Supreme Court denied that a fundamental right to privacy existed, using a narrow focus on legal text. Similarly, Kharak Singh v. State of Uttar Pradesh[8] offered limited protection against physical intrusion but did not define a complete right to privacy.

Over time, judicial views shifted, as in Gobind v. State of Madhya Pradesh[9], where the Court recognized that privacy could be based on Article 21, allowing for reasonable restrictions. Indian scholars suggest that this period marked the start of recognizing privacy as a key part of personal freedom.[10]

This evolution reached its peak in Justice K.S. Puttaswamy v. Union of India,[11] where the Supreme Court unanimously ruled that privacy is a fundamental right that is part of life and personal liberty. The Court stressed that privacy involves informational self-determination and is vital for protecting human dignity. It also set out a framework for restricting privacy, stating that any limitations must meet the tests of legality, necessity, and proportionality.[12]

[5] Shivani et al., Privacy vs Surveillance in Digital Age, IJSR (2025).
[6] Sarvajith Kumar J N & Manohar N, Right to Privacy v National Security, IJFMR (2025).
[7] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (India).
[8] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India).
[9] Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148 (India).
[10] Anupam Kurlwal, Evolution of Privacy in India, ShodhKosh (2024).
[11] Puttaswamy, (2017) 10 SCC 1.
[12] Id

IV. Surveillance Laws and Constitutional Concerns

India's laws on surveillance mainly come from the Indian Telegraph Act of 1885 and the Information Technology Act of 2000. These laws give the government wide-ranging powers to intercept, monitor, and decrypt communications for national security reasons.[13] However, Indian scholars criticize these rules for being too broad and lacking proper safeguards.

Research shows that the lack of judicial oversight and transparency leads to a high risk of misuse, as the government mainly controls surveillance decisions.[14] Furthermore, the secrecy of surveillance operations limits public scrutiny, weakening democratic accountability.

Indian journal articles point out that surveillance can have a chilling effect on free speech and expression. People may choose not to exercise their rights out of fear of being monitored.[15] This issue is especially important with digital communication, where surveillance can be widespread and hard to notice.

V. Data Protection and Legislative Developments

The Digital Personal Data Protection Act has been a major step toward regulating data privacy in India. However, scholars note that the Act includes broad exemptions for government agencies, especially around national security.[16] These exemptions raise worries about unchecked surveillance and weakened privacy protections.

Academic studies suggest that while the legislation tries to balance privacy and security, it often favors government power because of weak safeguards and oversight.[17] This shows the need for a stronger regulatory framework that ensures accountability and transparency in handling personal data.

VI. Proportionality and Constitutional Balancing

The principle of proportionality has become a key method for addressing conflicts between privacy and national security. According to Indian constitutional law, any limits on

[13] Information Technology Act, 2000, § 69 (India); Indian Telegraph Act, 1885, § 5(2) (India).
[14] Sarvajith Kumar J N & Manohar N, supra note 6.
[15] Suja Nayar, supra note 2
[16] Shivani et al., supra note 5.
[17] Id

fundamental rights must have a legitimate purpose, must be necessary, and must not be excessive. [18]

Scholars assert that applying proportionality to digital surveillance requires careful consideration of whether less invasive options exist.[19] Mass surveillance, in particular, raises major challenges because it involves collecting data indiscriminately and may not meet the necessity requirement.

VII. Emerging Challenges in the Digital Era

The fast-paced development of technology poses new challenges for privacy protection in India. The rise of artificial intelligence, biometric systems, and extensive data analysis has enhanced the government's ability to monitor people. Indian research indicates that these technologies create complex privacy risks, as they allow for the collection and analysis of large amounts of personal data.[20]

Additionally, blending private sector data with government surveillance has blurred the lines between public and private domains. This situation raises concerns about accountability and protecting individual rights.

VIII. Democratic Implications

Expanding surveillance powers has serious effects on democracy and the rule of law. Scholars stress that too much surveillance can hinder democratic participation by chilling free speech and dissent.[21] It may also concentrate power with the government, which can weaken checks and balances.

The lack of transparency in surveillance practices worsens these issues, making it difficult for citizens to hold the government responsible. In a constitutional democracy, the legitimacy of government actions relies on principles of accountability, transparency, and the rule of law.

[18] Modern Dental College v. State of Madhya Pradesh, (2016) 7 SCC 353 (India).
[19] Sarvajith Kumar J N & Manohar N, supra note 6.
[20] Priyanka Dalal & Richa, supra note 4.
[21] Suja Nayar, supra note 2.

IX. Conclusion

The clash between digital privacy and national security stands as one of the biggest constitutional challenges in modern India. While national security is a valid goal, it needs to be pursued within constitutional limits. Recognizing privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India highlights the need to protect individual autonomy and dignity in the digital age.

A balanced approach involves applying proportionality, creating strong safeguards, and enhancing institutional oversight. Ultimately, the future of constitutional governance in India depends on reconciling security demands with the safeguarding of fundamental rights.