DIGITAL SURVEILLANCE AND THE RIGHT TO PRIVACY: REASSESSING CONSTITUTIONAL BOUNDARIES UNDER ARTICLE 21 OF THE INDIAN CONSTITUTION

Mr Garvit Chand, Jagannath University, Jaipur

Mr Nikhil Jain, Jagannath University, Jaipur

ABSTRACT

The proliferation of advanced digital surveillance tools has redefined the State's capacity to monitor individuals, intensifying concerns regarding the protection of privacy in India. Following the recognition of the right to privacy as a fundamental right under Article 21 in Justice K.S. Puttaswamy v. Union of India, the constitutional framework has undergone a significant transformation. Nevertheless, the growing deployment of technologies such as facial recognition systems, biometric databases, and communication interception mechanisms presents complex challenges to the effective realization of this right.

This article critically examines the evolving tension between State surveillance and the right to privacy within the framework of Article 21. It analyses the constitutional principles of legality, necessity, and proportionality as essential safeguards against arbitrary State action. The study further evaluates the adequacy of existing legal frameworks, including the Information Technology Act and surveillance-related executive measures, in protecting privacy rights.

The research also explores the implications of mass surveillance on democratic values, particularly the chilling effect on freedom of speech and expression. By drawing comparative insights from global data protection regimes, the article highlights the need for a robust and comprehensive legal framework governing digital surveillance in India. It argues that the absence of clear statutory safeguards and independent oversight mechanisms undermines constitutional guarantees and risks transforming India into a surveillance state.

The article concludes by proposing legal and policy reforms aimed at recalibrating the balance between national security interests and individual privacy. It emphasizes the necessity of judicial oversight, legislative clarity, and accountability mechanisms to ensure that surveillance practices remain

within constitutional limits while safeguarding fundamental rights in the digital age.

Keywords: Digital Surveillance, Right to Privacy, Article 21, Constitutional Law, Proportionality, Data Protection, State Power, Human Rights; Surveillance Regulation, Informational Privacy

1. INTRODUCTION

This research article introduces the growing integration of digital technologies into governance and law enforcement has significantly transformed the nature and scope of State surveillance in India. Surveillance practices, once limited to targeted monitoring, have expanded into sophisticated systems involving large-scale data collection, real-time tracking, and algorithmic analysis. While such measures are often justified on grounds of national security, public order, and efficient governance, they raise serious constitutional concerns regarding the protection of individual privacy and civil liberties. The absence of a comprehensive statutory framework regulating digital surveillance further heightens the risk of excessive and arbitrary State intrusion into private life.

The legal basis of surveillance in India can be traced to colonial-era legislation such as the Indian Telegraph Act, 1885, which permits interception of communications under certain conditions.[1] With technological advancements, the scope of surveillance has expanded considerably through statutes like the Information Technology Act, 2000, which empowers the government to intercept, monitor, and decrypt digital information in the interest of sovereignty, integrity, and security of the State.[2]

In recent years, the deployment of technologies such as facial recognition systems, biometric identification frameworks like Aadhaar, and centralized data collection mechanisms has enabled pervasive forms of surveillance. These developments have blurred the distinction between targeted and mass surveillance, raising concerns about the proportionality and necessity of such measures. Moreover, the lack of independent oversight and transparency mechanisms has been widely criticized by scholars and civil society as being inconsistent with constitutional guarantees.[3]

[1] Indian Telegraph Act, No. 13 of 1885, § 5(2) (India).
[2] Information Technology Act, No. 21 of 2000, § 69 (India).
[3] Usha Ramanathan, *Aadhaar: From Welfare to Surveillance*, 54 Econ. & Pol. Wkly. 50, 52–55 (2019).

The constitutional status of the right to privacy was conclusively established by the Supreme Court in Justice K.S. Puttaswamy v. Union of India, wherein a nine-judge bench held that privacy is an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution.[4] The Court recognized privacy as encompassing multiple dimensions, including informational privacy, bodily autonomy, and decisional freedom.

Significantly, the judgment laid down a threefold test to determine the validity of State action infringing privacy: (i) legality, requiring the existence of a law; (ii) necessity, defined in terms of a legitimate State aim; and (iii) proportionality, ensuring a rational nexus between the means adopted and the objective pursued.[5] This framework serves as a constitutional safeguard against arbitrary surveillance.

Subsequent judicial pronouncements have reinforced these principles in the digital context. In Anuradha Bhasin v. Union of India, the Supreme Court emphasized that restrictions on fundamental rights, including access to the internet, must meet the standards of reasonableness and proportionality.[6] Despite these developments, the expanding scope of digital surveillance continues to challenge the effective realization of privacy rights, necessitating a re-examination of constitutional boundaries in contemporary governance.

2. CONCEPTUAL FRAMEWORK OF DIGITAL SURVEILLANCE

Digital surveillance refers to the systematic monitoring, collection, and analysis of individuals' data and communications through technological means by State authorities. In the contemporary digital era, surveillance extends beyond traditional interception to include sophisticated mechanisms such as metadata analysis, artificial intelligence-based profiling, and real-time tracking. These practices are often justified on grounds of national security, crime prevention, and governance efficiency. However, the increasing reliance on digital surveillance raises critical concerns regarding privacy, autonomy, and the potential for abuse of power, particularly in the absence of adequate legal safeguards.

Digital surveillance manifests in multiple forms, including communication interception, mass data collection, biometric identification, and visual monitoring. Statutory provisions under the

[4] Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).
[5] Ibid. at Pgno.325
[6] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637, ¶¶ 87–92 (India).

Information Technology Act, 2000 authorize the government to intercept, monitor, and decrypt digital information under specified circumstances.[7] Similarly, telephonic interception is governed by the Indian Telegraph Act, 1885.[8]

Modern techniques include facial recognition systems, internet monitoring, GPS tracking, and the use of centralized databases such as Aadhaar. These technologies enable both targeted and mass surveillance, often blurring the distinction between the two. In People's Union for Civil Liberties v. Union of India, the Supreme Court acknowledged the privacy implications of surveillance and laid down procedural safeguards against arbitrary telephone tapping.[9] Despite such safeguards, concerns remain regarding the proportionality and necessity of contemporary surveillance techniques.[10]

The growth of State surveillance in India has been driven by rapid technological advancements and increasing security concerns. Government initiatives such as centralized monitoring systems, and crime tracking networks have significantly enhanced the State's surveillance capacity. While these mechanisms aim to improve national security and law enforcement efficiency, they also facilitate large-scale data aggregation and profiling of individuals.

Judicial scrutiny of such practices remains limited. However, in Kharak Singh v. State of Uttar Pradesh, the Supreme Court recognized that certain forms of surveillance could violate personal liberty under Article 21.[11] Scholars have argued that the expansion of surveillance infrastructure without corresponding legal safeguards risks creating a surveillance state and undermining democratic freedoms.[12]

Therefore, the rapid growth of digital surveillance mechanisms necessitates a careful balancing of State interests with constitutional protections, ensuring that surveillance practices remain within the limits of legality, necessity, and proportionality.

3. CONSTITUTIONAL DIMENSIONS OF THE RIGHT TO PRIVACY

The research article states as to how right to privacy has evolved as a fundamental component

[7] Ibid 2
[8] Ibid 1
[9] People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India).
[10] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677, 690–95 (2015).
[11] Kharak Singh v. State of Uttar Pradesh, A.I.R. 1963 S.C. 1295 (India).
[12] Gautam Bhatia, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution* 210–215 (2016).

of constitutional jurisprudence in India, particularly under Article 21, which guarantees the right to life and personal liberty. Initially, the Constitution did not explicitly recognize privacy as a fundamental right, and early judicial decisions reflected a limited understanding of its scope. Over time, however, the Supreme Court expanded the interpretation of Article 21 to include various facets of human dignity and personal autonomy, ultimately culminating in the formal recognition of privacy as a constitutionally protected right.

A significant turning point in Indian constitutional law came with the landmark judgment in Justice K.S. Puttaswamy v. Union of India, where a nine-judge bench of the Supreme Court unanimously affirmed that the right to privacy is intrinsic to Article 21 and other fundamental freedoms.[13] The Court overruled earlier decisions such as M.P. Sharma v. Satish Chandra and Kharak Singh v. State of Uttar Pradesh to the extent that they denied the existence of a constitutional right to privacy.[14]

The judgment emphasized that privacy is essential to individual dignity, autonomy, and liberty, forming the foundation of a democratic society. Importantly, the Court introduced a threefold test to assess the validity of State actions infringing privacy: legality (existence of law), necessity (legitimate State aim), and proportionality (rational nexus between means and objective).[15] This framework serves as a constitutional safeguard against arbitrary State interference, particularly in the context of digital surveillance.

Informational privacy, as recognized in the Puttaswamy judgment, refers to an individual's right to control the collection, use, and dissemination of personal data.[16] In the digital age, where vast amounts of personal information are processed and stored by both State and private entities, informational privacy has gained heightened significance. The Court acknowledged that unchecked data collection and profiling could lead to serious violations of individual autonomy and freedom.

Subsequent decisions have reinforced this dimension of privacy. In Justice K.S. Puttaswamy (Aadhaar) v. Union of India, the Supreme Court upheld the constitutional validity of the Aadhaar scheme but stressed the need for data protection safeguards and limitations on data

[13] Ibid 4
[14] M.P. Sharma v. Satish Chandra, A.I.R. 1954 S.C. 300 (India); Kharak Singh v. State of Uttar Pradesh, A.I.R. 1963 S.C. 1295 (India).
[15] Ibid , page no. 325
[16] Ibid 4, page no 297-300

usage.[17]Scholars have argued that informational privacy is central to protecting individuals against surveillance and data misuse in the digital era.[7]

Thus, the constitutional recognition and expansion of informational privacy underscore the need for robust legal frameworks to ensure that technological advancements do not undermine fundamental rights.

4. LEGAL AND REGULATORY FRAMEWORK GOVERNING SURVEILLANCE IN INDIA

India's legal framework governing surveillance is primarily rooted in statutory provisions that predate the digital era, supplemented by later enactments addressing electronic communication. The regulatory structure is fragmented, relying largely on executive authorization with limited judicial oversight. While these laws provide a legal basis for interception and monitoring, concerns persist regarding their adequacy in safeguarding the fundamental right to privacy under Article 21, especially in the context of evolving digital technologies.

The Information Technology Act, 2000 serves as the principal legislation governing digital surveillance in India. Section 69 of the Act empowers the Central and State Governments to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource in the interest of sovereignty, integrity, defence, security of the State, or public order. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 further prescribe procedural safeguards, including authorization by competent authorities.[18]

However, the research states that critics argue that these provisions grant broad discretionary powers to the executive without adequate independent oversight. The lack of transparency and judicial scrutiny raises concerns regarding potential misuse and disproportionate interference with privacy.[19] Judicial observations in Shreya Singhal v. Union of India highlight the need for clear and narrowly tailored restrictions in matters affecting fundamental rights.[20]

[17] Justice K.S. Puttaswamy (Aadhaar) v. Union of India, (2019) 1 S.C.C. 1 (India).
[18] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E) (India).
[19] Usha Ramanathan, *State Surveillance and the Right to Privacy in India*, 54 Econ. & Pol. Wkly. 30, 32–34 (2019).
[20] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

The Indian Telegraph Act, 1885 provides the statutory basis for interception of telephonic communications. Under Section 5(2), the government is authorized to intercept messages in cases of public emergency or in the interest of public safety.[5]

In People's Union for Civil Liberties v. Union of India, the Supreme Court recognized telephone tapping as an invasion of privacy and laid down procedural safeguards to prevent arbitrary use of surveillance powers.[6] These include requirements of necessity, limited duration, and review by a high-level committee.

Despite these safeguards, the continued reliance on a colonial-era statute raises concerns regarding its compatibility with modern constitutional standards. The absence of comprehensive legislation specifically addressing digital surveillance underscores the urgent need for reform to ensure alignment with the principles of legality, necessity, and proportionality.

5. LIMITS ON SURVEILLANCE UNDER CONSTITUTIONAL LAW

State surveillance in India is subject to constitutional limitations derived primarily from Article 21, which guarantees the right to life and personal liberty. Any intrusion into privacy must conform to established constitutional principles to prevent arbitrary exercise of State power. The Supreme Court has consistently emphasized that surveillance measures must be balanced against individual rights, ensuring that they do not disproportionately infringe upon personal liberty and dignity.

The doctrine of proportionality has emerged as a central standard for assessing the validity of State action that restricts fundamental rights. In Justice K.S. Puttaswamy v. Union of India, the Supreme Court held that any infringement of privacy must be proportionate to the legitimate aim sought to be achieved.[21] This requires that the measure adopted must be suitable, necessary, and the least restrictive alternative available.

The application of proportionality was further elaborated in Modern Dental College v. State of Madhya Pradesh, where the Court emphasized that restrictions on fundamental rights must maintain a balance between the importance of the objective and the extent of the limitation

[21] Ibid 4, page no 325

imposed.[22] In the context of digital surveillance, this doctrine ensures that excessive or indiscriminate data collection does not violate constitutional guarantees.

Closely linked to proportionality are the tests of necessity and legality, which act as preconditions for any valid State interference with privacy. The legality requirement mandates that any surveillance measure must have a clear statutory basis. In Justice K.S. Puttaswamy v. Union of India, the Court stressed that executive action unsupported by law would be unconstitutional.

The necessity test requires that the surveillance measure pursue a legitimate State aim, such as national security or public order, and that there are no less intrusive alternatives available. In Anuradha Bhasin v. Union of India, the Supreme Court reiterated that restrictions on fundamental rights must be necessary and proportionate to the objective sought to be achieved.[23]

Together, these principles form a robust constitutional framework aimed at preventing arbitrary surveillance. However, their effective implementation remains a challenge, particularly in the absence of comprehensive legislation and independent oversight mechanisms.

6. EMERGING CHALLENGES OF DIGITAL SURVEILLANCE

The article states that the rapid advancement of digital technologies has intensified the scope and scale of State surveillance, giving rise to significant constitutional challenges. While surveillance is often justified on grounds of national security and public order, its expanding reach in the digital era poses serious risks to individual privacy and democratic freedoms. The absence of comprehensive data protection legislation and independent oversight mechanisms further aggravates these concerns, making it difficult to ensure accountability and transparency in surveillance practices.

Mass surveillance involves the large-scale collection and analysis of personal data, often without individualized suspicion. In India, initiatives such as centralized databases, facial recognition systems, and communication monitoring frameworks enable continuous tracking of individuals' activities. Such practices raise concerns regarding informational privacy, as

[22] Modern Dental College v. State of Madhya Pradesh, (2016) 7 S.C.C. 353 (India).
[23] Ibid 6, page no 87–92

recognized in Justice K.S. Puttaswamy v. Union of India, where the Supreme Court emphasized the need to protect individuals from unwarranted State intrusion.

The indiscriminate nature of mass surveillance blurs the line between targeted and blanket monitoring, increasing the risk of misuse and abuse of power. Scholars argue that unchecked data aggregation can lead to profiling, discrimination, and erosion of personal autonomy.[24]Moreover, the lack of transparency in surveillance programs undermines public trust and weakens constitutional safeguards.

One of the most significant consequences of pervasive surveillance is its chilling effect on fundamental rights, particularly freedom of speech and expression under Article 19(1)(a). The awareness or perception of constant monitoring may deter individuals from exercising their rights freely, thereby undermining democratic participation.

In Shreya Singhal v. Union of India, the Supreme Court recognized that vague and overbroad restrictions on expression can create a chilling effect, discouraging lawful speech. Similarly, in Anuradha Bhasin v. Union of India, the Court underscored the importance of proportionality and reasonableness in restricting digital freedoms.

Thus, the expanding surveillance framework not only threatens privacy but also impacts the broader constitutional fabric by restricting individual autonomy and free expression. Addressing these challenges requires robust legal safeguards, transparency, and accountability to ensure that surveillance practices remain consistent with constitutional principles.

7. REFORMING THE LEGAL FRAMEWORK FOR DIGITAL SURVEILLANCE

The rapid expansion of digital surveillance in India necessitates urgent legal and institutional reforms to ensure alignment with constitutional guarantees. The existing framework, largely based on fragmented statutes and executive rules, lacks coherence, transparency, and effective safeguards. In the absence of a comprehensive regulatory regime, surveillance practices risk undermining the fundamental right to privacy and enabling arbitrary State action. Therefore, reform is essential to establish a balanced framework that accommodates legitimate State interests while protecting individual rights.

[24] Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1937–40 (2013).

A robust data protection regime is central to regulating digital surveillance. The enactment of the Digital Personal Data Protection Act, 2023 marks a significant step toward safeguarding informational privacy.[25] The Act provides for lawful processing of personal data, consent-based mechanisms, and obligations on data fiduciaries to ensure data security. However, concerns remain regarding broad exemptions granted to the State, which may dilute privacy protections in the context of surveillance.[26]

Judicial observations in Justice K.S. Puttaswamy v. Union of India emphasized the need for a comprehensive data protection framework to safeguard informational privacy in the digital age. Comparative frameworks, such as the European Union's General Data Protection Regulation (GDPR), highlight the importance of strict data minimization, purpose limitation, and accountability principles.[27] Strengthening India's data protection regime is therefore crucial to ensure that surveillance practices remain lawful and proportionate.

Effective oversight and accountability mechanisms are essential to prevent abuse of surveillance powers. Currently, authorization and review processes are predominantly executive-driven, with limited judicial or parliamentary scrutiny. This concentration of power raises concerns regarding transparency and potential misuse.

In People's Union for Civil Liberties v. Union of India, the Supreme Court laid down procedural safeguards, including review committees, to regulate interception of communications.[28] However, these measures are often criticized as insufficient in the context of modern digital surveillance. Scholars advocate for independent oversight bodies, judicial warrants, and periodic audits to ensure accountability.[29]

Thus, meaningful reforms must focus on strengthening institutional checks, enhancing transparency, and ensuring that surveillance measures comply with constitutional principles. Only through such mechanisms can the balance between State power and individual liberty be effectively maintained.

[25] Digital Personal Data Protection Act, No. 22 of 2023 (India).
[26] Apar Gupta & Raman Jit Singh Chima, *The DPDP Act, 2023: An Analysis*, Internet Freedom Found. (2023).
[27] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
[28] People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India).
[29] Justice B.N. Srikrishna (Chairman), *Report of the Committee of Experts on Data Protection Framework for India* (2018).

8. CONCLUSION

From the analysis undertaken by this article, it becomes evident that the expansion of digital surveillance necessitates a careful re-evaluation of constitutional safeguards. Digital surveillance, while often justified as an indispensable tool for national security, public order, and efficient governance, presents profound challenges to the protection of individual privacy under Article 21 of the Indian Constitution. The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India marked a transformative moment in constitutional jurisprudence, firmly embedding dignity, autonomy, and informational self-determination within the framework of fundamental rights. This development imposes a constitutional obligation upon the State to ensure that surveillance practices do not transgress the boundaries of legality and reasonableness.

However, the existing legal framework governing surveillance in India remains fragmented and largely executive-driven, lacking comprehensive statutory backing and robust oversight mechanisms. The increasing deployment of advanced technologies such as facial recognition systems, mass data analytics, and biometric databases has significantly expanded the State's surveillance capacity, often without corresponding safeguards. This imbalance creates a serious risk of arbitrary, disproportionate, and opaque intrusions into individuals' private lives, thereby undermining constitutional guarantees.

The principles of legality, necessity, and proportionality, as articulated in Puttaswamy, must serve as the cornerstone for evaluating all surveillance measures. Any deviation from these standards not only threatens the right to privacy but also produces a chilling effect on other fundamental freedoms, including speech and expression. Therefore, the challenge lies not in rejecting surveillance altogether, but in ensuring that it operates within a constitutionally permissible framework.

The Article therefore states that there is urgent need for a coherent and comprehensive regulatory regime that clearly defines the scope and limits of State surveillance. This includes the enactment of stronger data protection laws, establishment of independent oversight authorities, and incorporation of judicial review mechanisms to ensure accountability and transparency. Additionally, procedural safeguards must be strengthened to prevent misuse and ensure that surveillance remains targeted, proportionate, and justified by legitimate State interests.

Therefore, the Article states that recalibrating the balance between State surveillance and the right to privacy is essential to preserving the democratic ethos of the Constitution. A rights-centric and transparent approach to surveillance governance will not only protect civil liberties but also reinforce public trust in State institutions in the digital age.