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

VOLUME 6 AND ISSUE 12 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

THE CONSTITUTIONAL RIGHT TO PRIVACY IN THE AGE OF ARTIFICIAL INTELLIGENCE: CHALLENGES OF STATE SURVEILLANCE IN INDIA

AUTHOR – ISHANJYOT* & DR. AUSAF AHMAD MALIK**

L.L.M. STUDENT, UILS, CHANDIGARH UNIVERSITY, MOHALI, PUNJAB, INDIA

PROFESSOR, UILS, CHANDIGARH UNIVERSITY, MOHALI, PUNJAB, INDIA

BEST CITATION – ISHANJYOT & DR. AUSAF AHMAD MALIK, THE CONSTITUTIONAL RIGHT TO PRIVACY IN THE AGE OF ARTIFICIAL INTELLIGENCE: CHALLENGES OF STATE SURVEILLANCE IN INDIA, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 6 (12) OF 2026, PG. 189-202, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The rapid advancement of Artificial Intelligence (AI) has significantly transformed the methods through which governments collect, process and analyse personal information. AI-based surveillance technologies, including facial recognition systems, biometric identification, predictive analytics and automated monitoring, have increasingly become relevant to public administration, law enforcement and national security. Although these technologies offer advantages in crime prevention and the maintenance of public order, their extensive use raises serious constitutional concerns regarding individual liberty, privacy and the limits of State authority.

In India, the right to privacy has been recognised as a fundamental right under Article 21 of the Constitution and as an essential component of the freedoms guaranteed under Part III. The landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India established that any infringement of privacy must satisfy the requirements of legality, legitimate State aim and proportionality. However, the growing use of artificial intelligence in surveillance presents challenges that existing constitutional and statutory safeguards may not adequately address.

This research examines the constitutional implications of AI-based State surveillance in India, with particular emphasis on Articles 14, 19 and 21 of the Constitution. It analyses the judicial interpretation of privacy, proportionality and procedural fairness, alongside relevant legislative provisions under the Information Technology Act, 2000, the Telecommunications Act, 2023 and the Digital Personal Data Protection Act, 2023. It further investigates the potential risks of indiscriminate data collection, algorithmic discrimination, lack of transparency and inadequate accountability in surveillance practices.

The paper argues that technological advancement and national security requirements cannot operate as unrestricted justifications for State surveillance. It concludes that a constitutionally compliant surveillance framework must incorporate necessity, proportionality, transparency, independent oversight, data minimisation and effective remedies against unlawful intrusion.

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

VOLUME 6 AND ISSUE 12 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

Keywords: Artificial Intelligence, Right to Privacy, State Surveillance, Article 21, Constitutional Law, Proportionality, Data Protection.

1. INTRODUCTION

The development of Artificial Intelligence has introduced a new dimension to the relationship between the State and individuals. Modern surveillance is no longer confined to conventional methods such as physical observation, telephone interception or manual monitoring. Technological developments have enabled governments and law enforcement authorities to utilise sophisticated systems capable of facial recognition, biometric identification, behavioural analysis and large-scale processing of personal information.

Artificial Intelligence has significantly enhanced the capacity of surveillance systems to collect and analyse information at a speed and scale that were previously difficult to achieve. These technologies may assist authorities in identifying suspects, preventing criminal activities, monitoring public spaces and addressing threats to national security. Nevertheless, their application also creates the possibility of excessive State interference in the private lives of individuals. The increasing use of surveillance technologies raises an important constitutional question: to what extent can the State exercise its surveillance powers without violating the fundamental rights guaranteed under the Constitution of India?

The right to privacy is an essential component of individual dignity, autonomy and personal liberty. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court of India unanimously recognised privacy as a constitutionally protected fundamental right. The Court clarified that privacy is protected under Article 21 and forms part of the freedoms guaranteed under Part III of the Constitution. It further established that State interference with privacy must satisfy legality, legitimate State purpose and proportionality.1 Indian Kanoon +1

The constitutional significance of privacy becomes particularly important when artificial intelligence is employed for surveillance. Unlike traditional surveillance, AI-based systems can process extensive amounts of information, identify patterns and generate predictions concerning individual behaviour. Such capabilities may result in continuous monitoring, profiling and the collection of personal information without meaningful awareness or control on the part of individuals.

The constitutional implications of such practices extend beyond Article 21. Surveillance may also affect Article 14, where algorithmic systems produce arbitrary or discriminatory outcomes, and Article 19, where excessive monitoring creates a chilling effect on freedom of speech and expression and other protected freedoms. Consequently, the regulation of AI-based surveillance requires a constitutional approach that balances legitimate governmental objectives with the fundamental rights of individuals. The State's responsibility to maintain national security and public order must be exercised within the limitations imposed by constitutional principles. This research therefore examines the constitutional validity and regulatory challenges associated with AI-based State surveillance in India, while analysing the role of judicial safeguards and data protection legislation in preserving individual liberty.

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

VOLUME 6 AND ISSUE 12 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

2. STATEMENT OF THE RESEARCH PROBLEM

The growing adoption of artificial intelligence in governmental surveillance has created a significant challenge for constitutional privacy protection in India. Although the Constitution recognises privacy as a fundamental right, the development of AI-based surveillance systems has increased the ability of the State to collect, analyse, store and utilise personal information on an extensive scale.

Existing legal provisions regulate certain forms of interception, monitoring and digital data processing. However, the application of these provisions to emerging AI-driven surveillance technologies raises questions regarding the adequacy of existing safeguards. The principal research problem concerns the absence of a sufficiently comprehensive, technology-specific framework that clearly addresses the constitutional implications of AI-based State surveillance, including algorithmic accountability, transparency, discrimination, data retention and independent supervision. The research therefore investigates whether the existing constitutional and statutory framework adequately protects individuals against arbitrary and disproportionate surveillance, while allowing the State to pursue legitimate national security and public safety objectives.

3. CONSTITUTIONAL FRAMEWORK GOVERNING THE RIGHT TO PRIVACY AND AI-BASED SURVEILLANCE

3.1 Article 21: Right to Life and Personal Liberty

Article 21 provides that no person shall be deprived of life or personal liberty except according to procedure established by law. The Supreme Court has interpreted Article 21 broadly to include dignity, autonomy and privacy as essential elements of individual liberty. In K.S. Puttaswamy, the Supreme Court recognised that privacy protects an individual's ability to make personal choices and maintain control over aspects of personal life. The Court also recognised the negative obligation of the State not to interfere arbitrarily with privacy and its positive obligation to protect individuals against unlawful interference.

The judgment established a threefold requirement for determining the constitutional validity of an infringement of privacy:

- Legality: There must be a valid law authorising the interference.
- Legitimate State aim: The interference must pursue a constitutionally permissible objective.
- Proportionality: The measure must maintain a rational relationship between the objective pursued and the means adopted.

These requirements are particularly relevant to AI-based surveillance because automated monitoring can involve extensive collection and processing of personal information.

For instance, the deployment of facial recognition systems in public places may raise privacy concerns when individuals are identified and tracked without adequate legal authority, necessity or safeguards. Therefore, Article 21 requires that technological surveillance must remain within constitutionally permissible limits.

3.2 Article 19: Protection of Fundamental Freedoms

Article 19 guarantees important freedoms to citizens, including freedom of speech and expression under Article 19(1)(a), and freedom of movement under Article 19(1)(d). AI-based surveillance may indirectly restrict these freedoms by creating an environment in which individuals believe that their activities, communications and movements are continuously monitored. Such monitoring may discourage individuals from expressing opinions, participating in peaceful demonstrations or engaging in activities protected by the Constitution. This phenomenon is commonly understood as the chilling effect.

The constitutional significance of surveillance therefore extends beyond the direct collection of personal information. It also concerns the potential impact of monitoring on the exercise of fundamental freedoms. Restrictions on Article 19 freedoms must satisfy the applicable constitutional requirements under Article 19(2) and other relevant clauses, including the requirement of reasonable restrictions. Consequently, surveillance measures cannot be justified merely because technology makes monitoring easier or more efficient. Their necessity and constitutional justification must be independently established.

3.3 Article 14: Right to Equality and Protection Against Arbitrariness

Article 14 guarantees equality before the law and equal protection of the laws. The use of AI-based surveillance creates concerns regarding algorithmic discrimination and unequal treatment. Artificial intelligence systems operate through data collection, pattern recognition and algorithmic decision-making. If the information used to develop or operate these systems is inaccurate, incomplete or unrepresentative, the resulting decisions may adversely affect particular individuals or groups.

For example, facial recognition systems may produce inaccurate identification results, potentially resulting in wrongful suspicion or disproportionate monitoring. Where State authorities rely on such systems without transparent standards or effective mechanisms for correction, their decisions may raise constitutional concerns under Article 14. Therefore, the principle of equality requires that AI-based surveillance must be subject to non-arbitrary standards, adequate testing and meaningful accountability.

3.4 Constitutional Balance Between Privacy and National Security

The right to privacy is not absolute. The State may legitimately undertake certain surveillance activities to protect national security, prevent criminal offences and maintain public order. However, the existence of a legitimate governmental objective does not automatically validate every surveillance measure. Constitutional limitations require that the interference must be authorised by law, necessary for achieving the intended objective and proportionate to the threat being addressed. The constitutional challenge lies in ensuring that national security does not become an unrestricted justification for excessive State interference.

4. STATUTORY FRAMEWORK GOVERNING DIGITAL SURVEILLANCE IN INDIA

4.1 Information Technology Act, 2000[573]

The Information Technology Act, 2000 provides an important statutory framework governing electronic records, computer resources and certain forms of digital monitoring. Section 69 empowers the Central Government, State Government or specially authorised officers to issue directions for interception, monitoring or decryption of information through computer resources, subject to specified grounds and prescribed safeguards. The grounds include sovereignty and integrity of India, defence, security of the State, public order and investigation of offences, among others. Section 69 requires reasons to be recorded in writing, while the applicable procedural safeguards are prescribed under the Information Technology (Procedures and Safeguards for Interception, Monitoring or Decryption of Information) Rules, 2009.2 IndiaCode. However, the provision primarily addresses interception, monitoring and decryption of information through computer resources. It should not be treated as a comprehensive regulatory framework for every form of AI-based physical or biometric surveillance. This distinction is important because facial recognition, predictive analytics and automated profiling may involve different forms of personal data processing and surveillance.

4.2 Telecommunications Act, 2023[574]

The Telecommunications Act, 2023 introduces a legislative framework governing telecommunication services and networks. Section 20 provides powers relating to public emergency and public safety. Under Section 20(2), the government may direct interception, detention or disclosure of messages in intelligible form, or suspension of telecommunication services, subject to the prescribed procedure and safeguards. The Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024 provide procedural requirements relating to competent authorities, interception orders, review committees, duration and record maintenance.3 India Code. These provisions are relevant to the constitutional regulation of communications surveillance. However, they do not independently establish a complete legal framework governing all AI-based surveillance technologies.

4.3 Digital Personal Data Protection Act, 2023[575]

The Digital Personal Data Protection Act, 2023 seeks to regulate the processing of digital personal data while recognising the interests of individuals in protecting their personal information. The legislation establishes the concepts of Data Fiduciaries and Data Principals and provides a framework for data protection, accountability and individual rights. Section 17 is particularly relevant because it provides specified exemptions, including certain processing activities connected with the prevention, detection, investigation or prosecution of offences. The application of these exemptions to State processing requires careful examination in light of constitutional privacy protections.

An important temporal qualification is necessary: the Act received Presidential assent in August 2023, but its provisions have been brought into force in stages. The commencement notification dated 13 November 2025 schedules the principal data-processing provisions, including Sections 3–17, to

[573] Act No. 21 of 2000, s. 69; Information and technology (procedures and safeguards for interception, monitoring, or Decryption of Information) Rules, 2009.
[574] Act No. 44 of 2023 s. 20; Telecommunication (procedures and safeguards for lawul interception of Message) Rules, 2024.
[575] Act No. 22 of Electroninc s and Information Technology, Notification G.S.R. 843(E), 13 November, 2025.

commence eighteen months after publication, that is, on 13 May 2027. Therefore, as of the date of this research draft, those substantive provisions are not yet in force.4 India Code.The legislation is relevant to the future regulation of AI-based data processing, but it should not be presented as though its entire substantive framework is already operational.

4.4 Need for a Comprehensive AI Surveillance FrameworkJustice K.S. Puttaswamy (Retd.) v. Union of India,[576]

The existing legal framework addresses different aspects of digital monitoring, telecommunications interception and personal data processing. However, these provisions do not, by themselves, comprehensively address the constitutional risks associated with AI-based surveillance, including algorithmic bias, automated profiling, explainability, biometric identification and the accountability of governmental agencies. A stronger regulatory approach is therefore required to ensure that technological surveillance remains consistent with fundamental rights.

5. JUDICIAL ANALYSIS: SUPREME COURT APPROACH TO PRIVACY AND SURVEILLANCE

The Supreme Court of India has played a significant role in developing the constitutional understanding of privacy, personal liberty and limitations on governmental power. Its decisions provide the foundation for evaluating the legality of emerging AI-based surveillance practices.

5.1 K.S. Puttaswamy v. Union of India

This is the most significant judgment for the present research.

A nine-judge Constitution Bench of the Supreme Court unanimously recognised the right to privacy as a fundamental right protected under Article 21 and the freedoms guaranteed under Part III of the Constitution. The Court recognised that privacy is closely connected with human dignity, individual autonomy and personal liberty. The judgment also established that any State action infringing privacy must satisfy the requirements of legality, legitimate State purpose and proportionality.

Relevance to AI surveillance: The principles laid down in this judgment provide the constitutional standard against which AI-based surveillance must be examined. The use of facial recognition, biometric monitoring and automated profiling cannot be considered constitutionally valid merely because such technologies are capable of assisting law enforcement. The State must demonstrate the legal authority, necessity and proportionality of the surveillance measure. The judgment therefore provides the central constitutional foundation of this research.5 Indian

5.2 People's Union for Civil Liberties v. Union of India[577]

The case concerned the legality of telephone tapping under Section 5(2) of the Indian Telegraph Act, 1885. The Supreme Court recognised that telephone tapping constitutes a serious invasion of individual privacy. It emphasised the need for procedural safeguards to prevent arbitrary and indiscriminate interception of communications. The Court laid down safeguards relating to authorisation, duration, review and supervision of telephone interception.

[576] (2017) 10 SCC 1.
[577] (1997) 1 SCC 301.

Relevance to AI surveillance: The judgment demonstrates that technological surveillance powers must be accompanied by meaningful procedural safeguards. The principles are relevant to contemporary surveillance systems because AI-based monitoring may extend beyond individual communications to large-scale collection and analysis of personal information. The decision reinforces the constitutional requirement that surveillance must not become an unrestricted instrument of governmental power.6 Indian Kanoon

5.3 Maneka Gandhi v. Union of India[578]

This landmark judgment significantly expanded the interpretation of Article 21. The Supreme Court held that the procedure established by law must be just, fair and reasonable and must not be arbitrary, fanciful or oppressive. The Court also established an important relationship between Articles 14, 19 and 21.

Relevance to AI surveillance: The principles developed in this judgment require State surveillance to comply with standards of fairness and reasonableness. Even where surveillance is authorised by legislation, the manner in which governmental authorities exercise that power must remain constitutionally fair. An arbitrary deployment of facial recognition or automated monitoring without adequate legal safeguards may therefore raise concerns under the constitutional framework established by this judgment.7 Indian Kanoon +1

5.4 Modern Dental College and Research Centre v. State of Madhya Pradesh[579]

The Supreme Court discussed the principle of proportionality while examining the constitutional validity of regulatory restrictions. The judgment explained the importance of assessing whether a restriction is suitable, necessary and appropriately balanced against the rights affected.

Relevance to AI surveillance: The proportionality principle is particularly significant where the State seeks to justify extensive surveillance in the interests of public safety or national security.

For example, if a limited surveillance measure can achieve a legitimate objective, the State should be required to justify why a more intrusive AI-based monitoring system is necessary. The principle prevents governmental authorities from adopting excessively intrusive measures where less restrictive alternatives are reasonably available.8 Indian Kanoon

5.5 Anuradha Bhasin v. Union of India[580]

This judgment concerned restrictions on internet services in Jammu and Kashmir. The Supreme Court held that freedom of speech and expression and freedom to practise any profession through the internet receive constitutional protection under Article 19. It also emphasised the importance of proportionality and the requirement that suspension orders must satisfy applicable legal standards and remain subject to review.

Relevance to AI surveillance: The judgment is significant because it recognises the constitutional implications of governmental restrictions in the digital environment. AI-based surveillance may

[578] (1978) 1 SCC 248.
[579] (2016) 7 SCC 353.
[580] (2020) 3 SCC 637.

similarly affect the exercise of fundamental freedoms by discouraging individuals from participating in online discussions, expressing opinions or engaging in lawful activities. The judgment therefore supports the argument that technological measures adopted by the State must remain subject to constitutional scrutiny.9 Indian Kanoon +1

5.6 Selvi v. State of Karnataka[581]

The Supreme Court examined the constitutional validity of involuntary narcoanalysis, polygraph examinations and brain electrical activation profile tests. The Court held that the involuntary administration of such techniques violated constitutional protections, including Article 20(3) and the right to personal liberty under Article 21. The judgment is relevant to the protection of mental privacy and individual autonomy.

Relevance to AI surveillance: Although the case did not concern artificial intelligence, it provides important constitutional reasoning concerning the limits of State intrusion into an individual's mental processes and personal autonomy. Its principles can inform the analysis of AI-based behavioural profiling and technologies that seek to infer sensitive information about individuals without their meaningful participation.

5.7 Overall Judicial Position

The above judgments establish several important constitutional principles:

- Privacy is an integral part of fundamental rights.
- Surveillance must have a valid legal basis.
- State action must pursue a legitimate objective.
- Restrictions must satisfy proportionality.
- Procedural safeguards are essential to prevent arbitrariness.
- Digital restrictions and surveillance remain subject to constitutional scrutiny.

However, the application of these principles to emerging AI-based surveillance technologies requires further judicial and legislative development.

6. CRITICAL ANALYSIS: CONSTITUTIONAL CHALLENGES OF AI-BASED STATE SURVEILLANCE

The constitutional regulation of AI-based surveillance presents challenges that extend beyond the conventional understanding of privacy. The principal concern is that artificial intelligence enables surveillance to become continuous, automated and capable of analysing information on a scale that may significantly increase the potential for interference with fundamental rights.

6.1 Mass Surveillance and the Loss of Individual Privacy

Traditional surveillance generally involved the observation of identified individuals or particular activities. AI-based systems, however, may enable authorities to monitor large populations through facial recognition, biometric identification and automated data analysis. Such systems create the

[581] (2010) 7 SCC 263.

possibility of collecting information about individuals who are not suspected of any criminal activity. The indiscriminate collection of personal information raises concerns under Article 21 because privacy protection should not depend exclusively on whether an individual has something to conceal. The constitutional problem arises when surveillance becomes excessive, indiscriminate or disproportionate to the objective being pursued.

6.2 Algorithmic Bias and Discrimination

Artificial intelligence systems depend upon the quality and representativeness of the data used for their development and operation. Where such information contains errors or historical biases, the resulting systems may produce inaccurate or discriminatory outcomes. In the context of State surveillance, such inaccuracies may lead to wrongful identification, unnecessary monitoring or disproportionate targeting of particular individuals. This raises concerns under Article 14, which prohibits arbitrary State action and guarantees equal protection of the laws. Therefore, constitutional accountability must extend not only to the officials who deploy AI systems but also to the standards governing their design, testing and use.

6.3 Lack of Transparency and Accountability

One of the major difficulties associated with AI-based surveillance is the limited transparency of automated decision-making.

Individuals may not know:

- Whether they have been subjected to automated surveillance.
- What personal information has been collected.
- How their information is being analysed.
- Whether an automated system has influenced a governmental decision.
- How an incorrect identification or assessment can be challenged.

The absence of meaningful transparency makes it difficult for individuals to exercise their constitutional rights. Although operational secrecy may sometimes be necessary for national security, secrecy cannot eliminate the requirement for independent institutional oversight.

6.4 Chilling Effect on Freedom of Expression

Continuous surveillance may discourage individuals from expressing opinions, participating in demonstrations or engaging in lawful political and social activities. The knowledge that communications and movements may be monitored can influence individual behaviour, even where no direct restriction has been imposed. This creates an indirect interference with the freedoms guaranteed under Article 19. A democratic constitutional system must therefore ensure that surveillance does not create an environment in which individuals are discouraged from exercising their fundamental freedoms.

6.5 Proportionality and Necessity of Surveillance

The proportionality principle provides an important constitutional safeguard against excessive surveillance.

The State must demonstrate that:

- The surveillance measure is authorised by law.
- It pursues a legitimate governmental objective.
- There is a rational connection between the measure and its objective.
- Less restrictive alternatives have been considered.
- The benefits of the measure justify the interference with individual rights.

For example, deploying facial recognition throughout a public area may be more intrusive than using targeted identification measures in response to a specific and demonstrable security threat. The State should therefore be required to justify the extent and duration of surveillance rather than relying upon broad claims of administrative efficiency or public safety.

6.6 Limitations of Existing Legal Safeguards

India has introduced legislative provisions addressing digital interception, telecommunications monitoring and personal data protection. Nevertheless, these laws regulate different aspects of technological activity and do not constitute a single comprehensive framework for AI-based State surveillance. In particular, questions concerning algorithmic accountability, biometric surveillance, automated profiling, data retention and independent supervision require further legal attention. The Digital Personal Data Protection Act, 2023 is an important legislative development. However, its commencement is phased, and its substantive provisions were scheduled to take effect in May 2027 under the November 2025 notification. Furthermore, data protection legislation alone cannot replace the constitutional scrutiny required when State action interferes with fundamental rights.

6.7 Need for Independent Oversight

A system in which governmental authorities exercise surveillance powers without meaningful external scrutiny creates risks of misuse and arbitrary interference. Independent review mechanisms are important to ensure that surveillance orders are lawful, necessary and proportionate. Existing interception frameworks provide for review committees. However, constitutional accountability in the AI context should also consider the accuracy of technological systems, the use of biometric information and the possibility of discriminatory outcomes. A stronger oversight framework should provide meaningful remedies and ensure that unlawful surveillance does not remain beyond effective scrutiny.

7. FINDINGS OF THE RESEARCH

The research identifies the following principal findings:

First, the right to privacy is firmly established as a fundamental right under the Constitution of India. The principles developed in K.S. Puttaswamy provide the foundation for examining the constitutional validity of AI-based surveillance.

Second, AI-based surveillance creates risks extending beyond conventional privacy violations. These include algorithmic discrimination, continuous monitoring, behavioural profiling and interference with individual autonomy.

Third, Articles 14, 19 and 21 are interconnected in the context of AI-based surveillance. Article 14 addresses arbitrariness and discriminatory outcomes, Article 19 protects fundamental freedoms, and Article 21 safeguards privacy and personal liberty.

Fourth, national security and public order are legitimate governmental objectives, but they cannot justify unrestricted or indiscriminate surveillance.

Fifth, existing statutory provisions regulate certain aspects of digital interception and personal data processing. However, their application to emerging AI technologies requires greater clarity and stronger accountability mechanisms.

Sixth, procedural safeguards and independent oversight are essential to ensure that surveillance powers are not exercised arbitrarily. Seventh, the constitutional protection of privacy must extend to emerging technological developments, rather than being restricted to traditional forms of personal intrusion.

8. SUGGESTIONS AND RECOMMENDATIONS

8.1 Development of a Comprehensive AI Surveillance Framework

India should consider developing a specific regulatory framework governing the use of AI-based surveillance technologies by public authorities. Such a framework should clearly define permissible surveillance purposes, the conditions of deployment and the responsibilities of governmental agencies.

8.2 Mandatory Necessity and Proportionality Assessment

Before deploying intrusive AI surveillance systems, public authorities should conduct a documented assessment of necessity and proportionality. The assessment should examine the legitimate objective, potential interference with privacy, availability of less intrusive alternatives and expected impact on fundamental rights.

8.3 Independent Institutional Oversight

An independent oversight mechanism should be established or strengthened to examine the legality and proportionality of significant AI-based surveillance activities. Such oversight should include periodic audits and review of surveillance practices.

8.4 Algorithmic Transparency and Accountability

Government authorities should maintain appropriate records of the AI systems used for surveillance, including their intended purpose, data sources, operational limitations and accuracy assessments. Where automated systems materially influence decisions affecting individuals, adequate mechanisms should exist for explanation, human review and correction.

8.5 Protection Against Algorithmic Discrimination

AI-based surveillance systems should undergo regular testing to identify inaccurate or discriminatory outcomes. Public authorities should ensure that technological systems are not used in ways that result in arbitrary or unequal treatment.

8.6 Data Minimisation and Retention Limits

The collection of personal information should be restricted to what is reasonably necessary for the authorised purpose. Information should not be retained indefinitely. Clear rules should govern storage, access, sharing, deletion and protection against unauthorised disclosure.

8.7 Effective Remedies Against Unlawful Surveillance

Individuals should have access to appropriate complaint and review mechanisms where they believe that surveillance has unlawfully interfered with their constitutional rights. The framework should also provide accountability for misuse, unauthorised access and negligent handling of personal information.

8.8 Strengthening Constitutional Awareness

Public authorities responsible for deploying surveillance technologies should receive appropriate training concerning privacy, proportionality, equality and constitutional limitations on governmental powers. Constitutional principles must guide technological governance from the stage of procurement and deployment to ongoing monitoring and review.

9. CONCLUSION

The development of Artificial Intelligence has fundamentally changed the nature and extent of State surveillance. Technologies such as facial recognition, biometric identification and automated data analysis have created new possibilities for maintaining public safety and addressing national security concerns. However, these developments also present significant challenges to constitutional privacy and individual liberty.

The Constitution of India provides a strong foundation for protecting individuals against arbitrary State interference. Articles 14, 19 and 21 collectively establish constitutional limitations that must guide the use of surveillance technologies. The recognition of privacy as a fundamental right in K.S. Puttaswamy has strengthened the constitutional position of individuals and established that State interference with privacy must satisfy legality, legitimate purpose and proportionality.

The judicial decisions examined in this research demonstrate that governmental powers, including surveillance and interception, must remain subject to procedural fairness, reasonableness and constitutional accountability. At the same time, existing statutory provisions addressing digital interception and personal data processing require continued evaluation in light of emerging AI-based technologies.

The central concern is not whether artificial intelligence should be used by the State, but whether its use can be regulated in a manner consistent with constitutional values. National security and public order are legitimate objectives; nevertheless, they cannot be treated as unrestricted grounds for continuous or disproportionate surveillance.

It is therefore necessary to strengthen the existing legal framework through clearer statutory standards, independent oversight, algorithmic accountability, data minimisation and effective remedies against unlawful surveillance.

Ultimately, technological advancement must operate within the constitutional limitations of State power. The protection of privacy is not an obstacle to national security or technological development; rather, it is an essential requirement of a democratic constitutional system. The legitimacy of AI-based surveillance in India must therefore be measured not merely by its technological efficiency, but by its conformity with constitutional principles, individual dignity and the rule of law.

10.201 BIBLIOGRAPHY

A. Primary Sources

- Constitution of India, 1950 – Articles 14, 19 and 21.
- The Information Technology Act, 2000.
- The Telecommunications Act, 2023.
- The Digital Personal Data Protection Act, 2023.
- Information Technology (Procedures and Safeguards for Interception, Monitoring or Decryption of Information) Rules, 2009.
- Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024.
- Digital Personal Data Protection Rules, 2025.

B. Secondary Sources

Books

- Gautam Bhatia, The Transformative Constitution: A Radical Biography in Nine Acts (HarperCollins, 2019).
- Gautam Bhatia, Offend, Shock, or Disturb: Free Speech under the Indian Constitution (Oxford University Press, 2016).
- M.P. Jain, Indian Constitutional Law (LexisNexis).

International materials

- United Nations Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), 1988.
- United Nations General Assembly, Resolution 68/167, The Right to Privacy in the Digital Age, 2013.
- United Nations Human Rights Council, Report of the Special Rapporteur on the Right to Privacy in the Digital Age, A/HRC/27/37, 2014.

Judicial Decision

- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
- Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
- Modern Dental College and Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353.
- Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

- Selvi v. State of Karnataka, (2010) 7 SCC 263.