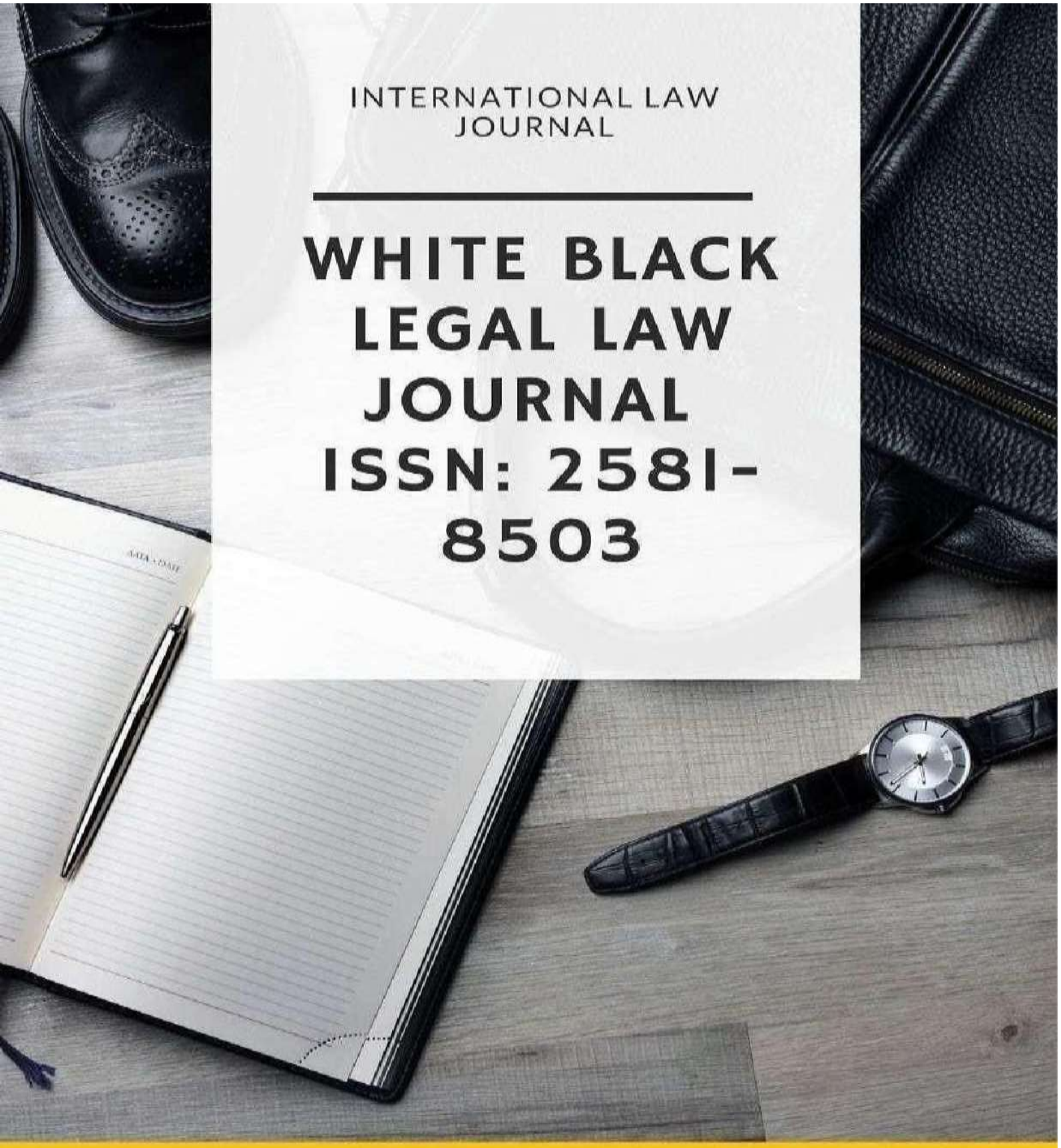

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 3 | Jan 2026 ISSN: 2581-8503

ARTIFICIAL INTELLIGENCE, STATE SURVEILLANCE, AND THE RIGHT TO PRIVACY IN INDIA: A CONSTITUTIONAL ANALYSIS AFTER *PUTTASWAMY*

AUTHORED BY - RENU

Abstract

The rapid integration of Artificial Intelligence (AI) into governance and law enforcement has fundamentally transformed the nature, scale, and intensity of State surveillance in India. From facial recognition systems and predictive policing tools to large-scale biometric databases and algorithmic profiling, AI-driven technologies have enabled the State to collect, process, and analyse personal data at an unprecedented scale. While such technologies are often justified in the name of national security, public order, and administrative efficiency, they raise serious constitutional concerns relating to privacy, autonomy, dignity, and democratic accountability. The recognition of the right to privacy as a fundamental right under Article 21 of the Constitution of India by the Supreme Court in Justice K.S. Puttaswamy v. Union of India marked a watershed moment in Indian constitutional jurisprudence. However, the post-Puttaswamy era has witnessed an expansion—not a contraction—of surveillance infrastructures powered by AI, often without adequate legislative backing, transparency, or effective oversight mechanisms.

This research paper undertakes a comprehensive constitutional analysis of AI-enabled State surveillance in India through the lens of the right to privacy. It critically examines whether existing surveillance practices satisfy the constitutional tests of legality, necessity, proportionality, and procedural safeguards laid down by the Supreme Court. The study analyses key surveillance frameworks such as the Aadhaar ecosystem, facial recognition technologies deployed by law enforcement agencies, predictive analytics in policing, and mass data collection practices enabled through digital governance platforms. It argues that AI-based surveillance differs qualitatively from traditional surveillance methods due to its capacity for continuous monitoring, automated decision-making, and predictive inference, thereby intensifying the risk of constitutional violations.

The paper further explores the interplay between Articles 14, 19, and 21 of the Constitution in regulating surveillance practices. Algorithmic opacity, data bias, and automated profiling raise concerns of arbitrariness and discrimination under Article 14, while pervasive surveillance has a chilling effect on freedom of speech, association, and movement under Article 19. The research also evaluates the adequacy of existing statutory frameworks, including the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, in addressing the unique challenges posed by AI-driven surveillance. It highlights the

absence of independent oversight, weak consent mechanisms, and limited remedies for individuals affected by unlawful surveillance.

Comparative insights from international human rights law and foreign jurisdictions are incorporated to contextualise India's constitutional obligations in the global digital order. The paper argues that unchecked AI surveillance risks transforming India into a data-driven surveillance State, undermining the foundational values of constitutionalism, rule of law, and democratic governance. It concludes by proposing a rights-centric regulatory framework that balances legitimate State interests with individual freedoms, emphasising the need for comprehensive surveillance legislation, judicial oversight, algorithmic transparency, and robust accountability mechanisms.

KEYWORDS

Artificial Intelligence; State Surveillance; Right to Privacy; Constitutional Law; Puttaswamy Judgment; Facial Recognition Technology; Predictive Policing; Data Protection; Proportionality; Democratic Accountability

Introduction

The relationship between the State, technology, and individual liberty has always been a defining concern of constitutional governance. In the digital age, this relationship has undergone a profound transformation with the advent of Artificial Intelligence (AI), which has enabled governments to collect, process, and analyse vast quantities of personal data with unprecedented speed and precision. In India, AI-driven technologies are increasingly being deployed across governance and law enforcement mechanisms, ranging from biometric identification systems and facial recognition tools to predictive analytics used in policing and public administration. While these technologies promise efficiency, security, and administrative convenience, they simultaneously raise fundamental constitutional questions concerning privacy, dignity, autonomy, and the limits of State power.

Historically, surveillance by the State was constrained by practical limitations of manpower, time, and resources. Traditional forms of surveillance required physical presence, targeted monitoring, and human discretion, thereby providing a natural check against indiscriminate intrusion. AI-powered surveillance, however, fundamentally alters this balance. Through

automated data aggregation, real-time tracking, and algorithmic profiling, the State is now capable of engaging in continuous, mass, and often invisible surveillance of individuals and populations. This shift from targeted to pervasive surveillance poses unique challenges to constitutional protections, as it erodes the distinction between public and private spheres and normalises constant monitoring as a feature of everyday life.

The Indian constitutional framework, though drafted in a pre-digital era, is rooted in values that are inherently adaptable to technological change. Articles 14, 19, and 21 collectively form the bedrock of individual liberty and democratic accountability. The recognition of the right to privacy as an intrinsic part of the right to life and personal liberty under Article 21 by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India* marked a transformative moment in Indian constitutional jurisprudence. The judgment not only affirmed privacy as a fundamental right but also articulated a principled framework to assess State intrusions into individual privacy. By laying down the tests of legality, legitimate State aim, necessity, proportionality, and procedural safeguards, the Court sought to ensure that technological advancements do not become instruments of unchecked executive power.

Despite this constitutional clarity, the post-*Puttaswamy* period has witnessed a rapid expansion of surveillance infrastructures in India, often justified on grounds of national security, crime prevention, and efficient governance. Initiatives such as the Aadhaar-based identification system, facial recognition databases maintained by law enforcement agencies, and AI-enabled predictive policing tools illustrate the State's increasing reliance on data-driven governance. These systems operate at the intersection of technology and coercive State power, making their constitutional scrutiny both urgent and complex. The opacity inherent in algorithmic decision-making further exacerbates these concerns, as individuals are frequently unaware of how their data is collected, processed, or used to make decisions that affect their rights.

The constitutional implications of AI-driven surveillance extend beyond the right to privacy under Article 21. Pervasive surveillance has a chilling effect on the freedoms guaranteed under Article 19, including freedom of speech, expression, association, and movement. When individuals are aware that their digital footprints, communications, and physical movements are constantly monitored, they are more likely to engage in self-censorship, thereby undermining the democratic discourse essential to a constitutional republic. Moreover, algorithmic biases embedded within AI systems raise serious concerns under Article 14, as

automated profiling can result in discriminatory outcomes, arbitrary targeting, and unequal treatment before the law. The lack of transparency and explainability in AI systems makes it difficult to challenge such discrimination, thereby weakening constitutional remedies.

Another significant concern is the absence of a comprehensive legislative framework governing surveillance in India. Much of the existing surveillance infrastructure operates under executive orders, colonial-era laws, or fragmented statutory provisions that were not designed to address the complexities of AI-enabled monitoring. While the enactment of the Digital Personal Data Protection Act, 2023 represents an important step towards regulating data processing activities, it does not adequately address the specific challenges posed by State surveillance, particularly in contexts involving national security and law enforcement exemptions. This regulatory gap creates a fertile ground for constitutional violations, as broad discretionary powers are exercised without sufficient checks and balances.

The role of constitutional courts in mediating the tension between technological progress and fundamental rights is therefore of paramount importance. Indian courts have historically played an activist role in expanding the scope of fundamental rights to meet contemporary challenges. However, judicial review in cases involving surveillance often encounters institutional constraints, including claims of secrecy, national security, and technical complexity. These factors necessitate a rethinking of constitutional doctrines and remedial mechanisms to ensure effective protection of privacy and liberty in the age of AI.

Against this backdrop, this research paper seeks to critically examine AI-enabled State surveillance in India through a constitutional lens. It aims to analyse whether current surveillance practices align with the principles laid down in *Puttaswamy* and subsequent jurisprudence, and whether existing legal frameworks provide meaningful safeguards against abuse. By situating AI surveillance within the broader discourse of constitutionalism, rule of law, and human dignity, the study endeavours to contribute to an evolving body of scholarship that seeks to reconcile technological innovation with the enduring values of the Indian Constitution.

Research Methodology

This research adopts a predominantly doctrinal and analytical methodology to examine the constitutional implications of Artificial Intelligence–enabled State surveillance in India. The

doctrinal approach is particularly suitable for this study as it allows for a systematic analysis of constitutional provisions, judicial precedents, statutory frameworks, and administrative practices governing surveillance and data processing. Given that the right to privacy and the limits of State surveillance are primarily shaped by constitutional interpretation and judicial reasoning, doctrinal research provides an appropriate foundation for evaluating the legality and proportionality of AI-driven surveillance measures.

The study relies extensively on primary legal sources, including the Constitution of India, landmark judgments of the Supreme Court and High Courts, and relevant statutory enactments such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023. Judicial pronouncements, particularly *Justice K.S. Puttaswamy v. Union of India* and subsequent cases interpreting the scope of privacy and State power, form the core analytical framework of this research. These decisions are examined not merely for their outcomes but for the constitutional principles and tests articulated therein, such as legality, necessity, proportionality, and procedural safeguards. By applying these principles to contemporary AI-enabled surveillance practices, the study evaluates whether existing mechanisms meet constitutional standards.

In addition to doctrinal analysis, the research incorporates a qualitative analytical approach to assess the functional operation of AI-based surveillance technologies in India. While the study does not employ empirical data collection in the form of surveys or interviews, it critically examines policy documents, government reports, parliamentary debates, and publicly available information regarding the deployment of technologies such as facial recognition systems, biometric identification platforms, and predictive policing tools. This approach enables an understanding of how surveillance technologies are implemented in practice and how they impact individual rights beyond their formal legal justifications.

A comparative methodology is also employed to contextualise India's constitutional approach within the broader framework of international human rights law and foreign constitutional practices. International instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights are examined to assess India's obligations regarding privacy, liberty, and due process in the digital age. Judicial decisions from foreign jurisdictions, particularly those addressing mass surveillance and data protection, are referenced to highlight alternative regulatory models and judicial safeguards. This comparative

analysis is not intended to transplant foreign doctrines wholesale but to draw normative insights that may inform Indian constitutional interpretation.

The research further adopts an interdisciplinary perspective by engaging with scholarship from fields such as technology law, data protection, and ethics of artificial intelligence. Academic articles, reports by expert committees, and publications by civil society organisations are analysed to understand the technical characteristics of AI systems, including algorithmic opacity, data bias, and automated decision-making. This interdisciplinary engagement is essential to bridge the gap between legal theory and technological reality, ensuring that constitutional analysis is grounded in an accurate understanding of how AI surveillance operates.

An important aspect of the methodology is the critical evaluation of existing legal and institutional safeguards against surveillance abuse. The study examines mechanisms such as executive oversight, judicial authorisation, and grievance redressal procedures to assess their effectiveness in protecting individual rights. It also analyses the limitations of these mechanisms, particularly in contexts involving national security exemptions and claims of confidentiality. By identifying structural and procedural weaknesses, the research seeks to highlight areas where constitutional protections may be rendered illusory.

The scope of the research is confined to State surveillance and does not extend to surveillance conducted by private entities, except where such entities act under State authority or in collaboration with government agencies. This limitation ensures analytical focus while acknowledging the broader ecosystem of data-driven surveillance. Additionally, the study primarily focuses on the Indian legal framework, with comparative references serving a supplementary role.

The limitations of this research stem from the lack of transparency surrounding surveillance programmes and restricted access to official data. Many AI-based surveillance initiatives operate without public disclosure, making it difficult to assess their full extent and impact. Furthermore, the rapidly evolving nature of AI technology means that legal frameworks and practices are subject to frequent change. Despite these limitations, the research aims to provide a robust constitutional analysis based on available information and established legal principles.

Statement of Problem

The exponential growth of Artificial Intelligence–enabled surveillance technologies has significantly altered the nature of State power in India, raising serious constitutional concerns that remain inadequately addressed within the existing legal framework. While technological advancements have enhanced the State's capacity to maintain public order, prevent crime, and deliver efficient governance, they have simultaneously expanded the scope for intrusive monitoring of individuals' lives. The core problem lies in the absence of a coherent constitutional and statutory mechanism capable of regulating AI-driven surveillance in a manner that balances legitimate State interests with the fundamental rights of individuals.

Despite the Supreme Court's recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India*, surveillance practices in India continue to operate largely under executive discretion, often without explicit legislative authorisation. Many AI-based surveillance systems are introduced through administrative notifications, pilot projects, or internal guidelines that lack parliamentary scrutiny. This raises a fundamental issue concerning the principle of legality, which requires that any restriction on fundamental rights must be sanctioned by law. The continued reliance on executive instruments undermines constitutional safeguards and creates an environment where surveillance practices can expand without meaningful democratic oversight.

Another significant problem arises from the qualitative difference between traditional surveillance and AI-enabled surveillance. AI systems enable continuous, large-scale data collection and automated analysis, allowing the State to infer behavioural patterns, predict future actions, and profile individuals or groups. Such predictive and pre-emptive surveillance challenges traditional notions of privacy, which were primarily concerned with discrete intrusions. Existing constitutional doctrines have not been fully adapted to address the cumulative and systemic harms caused by persistent data aggregation and algorithmic profiling. As a result, individuals may suffer privacy violations not through a single identifiable act, but through the ongoing erosion of informational autonomy.

The lack of transparency and accountability in AI-driven surveillance further exacerbates the constitutional problem. Algorithmic systems often function as "black boxes," making it difficult for individuals to understand how decisions affecting them are made. This opacity limits the ability of courts to exercise effective judicial review and of citizens to challenge

unlawful surveillance. Without access to information regarding data sources, decision-making criteria, and error rates, affected individuals are left without effective remedies, thereby weakening the constitutional promise of due process and access to justice.

AI-enabled surveillance also raises concerns of arbitrariness and discrimination, implicating Article 14 of the Constitution. Algorithmic bias, whether arising from skewed training data or flawed design, can disproportionately target marginalised communities, leading to discriminatory policing and unequal treatment. In the absence of clear standards and oversight mechanisms, such discriminatory outcomes may go undetected or unremedied. This undermines the constitutional guarantee of equality before the law and exposes systemic vulnerabilities in the deployment of automated decision-making systems by the State.

Furthermore, pervasive surveillance has a chilling effect on the freedoms guaranteed under Article 19, particularly freedom of speech, expression, association, and movement. When individuals are aware that their communications, digital activities, or physical movements are subject to constant monitoring, they may refrain from lawful dissent, political participation, or association. This subtle but pervasive impact on democratic freedoms is difficult to quantify, yet it poses a serious threat to the functioning of a constitutional democracy. Existing legal frameworks fail to adequately recognise or address these indirect but profound consequences of surveillance.

The enactment of the Digital Personal Data Protection Act, 2023, while a significant development in India's data protection regime, does not sufficiently resolve these concerns. Broad exemptions granted to the State in matters of national security and public order dilute the effectiveness of privacy protections and allow surveillance activities to escape rigorous scrutiny. The absence of an independent oversight authority specifically empowered to regulate State surveillance further compounds the problem, leaving individuals with limited avenues for redress.

In essence, the central problem addressed by this research is the growing disconnect between constitutional principles and technological realities. The expansion of AI-enabled State surveillance in India has outpaced the development of legal safeguards necessary to protect fundamental rights. Without a robust constitutional and legislative framework grounded in transparency, accountability, and proportionality, AI-driven surveillance risks normalising a

culture of constant monitoring that is incompatible with the values of dignity, autonomy, and democratic governance enshrined in the Constitution of India.

Research Questions

This research paper is guided by five central research questions that seek to examine the constitutional implications of Artificial Intelligence–enabled State surveillance in India. These questions are framed to address doctrinal, practical, and normative concerns arising from the increasing use of AI technologies by the State, while remaining aligned with the constitutional framework laid down by the Supreme Court of India.

The first research question examines whether the deployment of AI-enabled surveillance technologies by the State satisfies the constitutional requirement of legality as articulated in *Justice K.S. Puttaswamy v. Union of India*. This question seeks to analyse whether existing surveillance practices are supported by clear, accessible, and democratically enacted laws, or whether they continue to operate primarily through executive orders and administrative guidelines. By focusing on the source and quality of legal authorisation, this question addresses the foundational requirement that any restriction on fundamental rights must be sanctioned by law.

The second research question explores whether AI-driven surveillance measures meet the tests of necessity and proportionality under Article 21 of the Constitution. This involves an assessment of whether such surveillance is essential to achieve legitimate State aims such as national security or public order, and whether less intrusive alternatives are available. The question further examines whether the scale, duration, and intensity of AI-based surveillance are proportionate to the objectives sought to be achieved, particularly in light of the enhanced intrusiveness of automated and continuous monitoring systems.

The third research question focuses on the impact of AI-enabled surveillance on the freedoms guaranteed under Article 19 of the Constitution, including freedom of speech, expression, association, and movement. It seeks to determine whether pervasive surveillance creates a chilling effect on democratic participation and lawful dissent. This question also examines the extent to which surveillance practices indirectly restrict fundamental freedoms, even in the absence of explicit prohibitory measures, thereby raising concerns about the subtle erosion of civil liberties in a constitutional democracy.

The fourth research question examines whether AI-based surveillance practices are consistent with the guarantee of equality before the law under Article 14 of the Constitution. This question analyses the risks of arbitrariness and discrimination arising from algorithmic decision-making, particularly in contexts such as predictive policing and facial recognition. It seeks to assess whether existing safeguards are adequate to prevent biased outcomes and ensure non-discriminatory application of surveillance technologies.

The fifth and final research question evaluates the adequacy of existing legal and institutional safeguards in protecting individuals against unlawful or excessive State surveillance. This includes an examination of oversight mechanisms, judicial remedies, transparency requirements, and accountability frameworks. The question also considers whether recent legislative developments, particularly the Digital Personal Data Protection Act, 2023, provide meaningful protection against AI-enabled surveillance or whether significant regulatory gaps persist.

Hypothesis

This research paper is premised on the hypothesis that the current framework governing Artificial Intelligence–enabled State surveillance in India is constitutionally inadequate and fails to sufficiently protect the fundamental rights of individuals. While the State possesses a legitimate interest in maintaining public order, national security, and efficient governance, the unchecked deployment of AI-driven surveillance technologies has resulted in a disproportionate expansion of executive power at the cost of individual liberty, privacy, and democratic accountability.

The first hypothesis of this study posits that most AI-enabled surveillance practices in India do not fully satisfy the constitutional requirement of legality as laid down in *Justice K.S. Puttaswamy v. Union of India*. It is hypothesised that the absence of comprehensive, surveillance-specific legislation has led to a reliance on executive orders, administrative guidelines, and general statutory provisions that were not designed to regulate advanced AI technologies. This lack of precise legal authorisation undermines the rule of law and weakens the constitutional safeguard that restrictions on fundamental rights must be clearly defined and democratically enacted.

The second hypothesis suggests that AI-driven surveillance measures often fail the test of proportionality under Article 21 of the Constitution. Given the intrusive nature of automated data collection, real-time monitoring, and predictive analytics, it is hypothesised that such surveillance exceeds what is necessary to achieve legitimate State objectives. The study assumes that in many instances, less intrusive alternatives are available but are not adequately considered, leading to excessive and continuous monitoring that disproportionately infringes upon individual privacy and autonomy.

The third hypothesis asserts that pervasive AI-enabled surveillance has a chilling effect on the freedoms guaranteed under Article 19, particularly freedom of speech, expression, and association. It is hypothesised that the awareness or perception of constant monitoring discourages individuals from engaging in lawful dissent, political participation, and free expression. This indirect restriction on fundamental freedoms, though not always visible or measurable, is assumed to pose a significant threat to the democratic functioning of the State.
The fourth hypothesis of this research is that AI-based surveillance systems risk violating the guarantee of equality under Article 14 due to inherent algorithmic biases and lack of transparency. It is hypothesised that automated decision-making tools, when deployed without adequate safeguards, may disproportionately target specific communities or groups, resulting in discriminatory outcomes. The absence of explainability in algorithmic processes further exacerbates this issue by limiting the ability of affected individuals to challenge arbitrary or unequal treatment.

The fifth and final hypothesis contends that existing legal and institutional safeguards are insufficient to provide effective remedies against unlawful or excessive State surveillance. It is hypothesised that oversight mechanisms lack independence, transparency, and technical capacity to meaningfully regulate AI-enabled surveillance practices. Furthermore, broad exemptions granted to the State under data protection laws are assumed to dilute privacy protections, leaving individuals with limited avenues for redress.

Collectively, these hypotheses reflect the overarching assumption that the rapid adoption of AI surveillance in India has outpaced the development of constitutional safeguards necessary to protect fundamental rights. The research seeks to test these hypotheses through doctrinal analysis, judicial interpretation, and comparative insights, with the ultimate aim of proposing a more balanced and rights-oriented regulatory framework.

Review of Literature

The discourse on privacy, surveillance, and constitutionalism has expanded significantly in recent years, particularly with the increasing deployment of digital technologies by the State. Early constitutional scholarship in India primarily treated privacy as a peripheral concern, often subsumed within personal liberty under Article 21. However, this approach evolved substantially following the Supreme Court's decision in *Justice K.S. Puttaswamy v. Union of India*, which affirmed privacy as a fundamental right intrinsic to dignity, autonomy, and liberty. Legal scholars have widely acknowledged this judgment as a transformative moment in Indian constitutional law, noting its articulation of a structured proportionality test to evaluate State intrusions into privacy.

Several academic works have analysed the implications of *Puttaswamy* for surveillance practices in India. Scholars such as Gautam Bhatia and Apar Gupta have argued that the judgment imposes strict limitations on executive discretion, particularly in matters involving national security and data collection. Their analyses emphasise the necessity of clear legislative authorisation and robust procedural safeguards to prevent abuse. However, much of this scholarship focuses on traditional surveillance mechanisms and does not sufficiently engage with the unique challenges posed by AI-enabled systems, which operate through automated and predictive processes.

The literature on State surveillance has also engaged with the Aadhaar project as a case study of large-scale data collection in India. Numerous scholars have examined the constitutional validity of Aadhaar, particularly in relation to privacy, exclusion, and surveillance concerns. While the Supreme Court upheld the constitutional validity of Aadhaar in *K.S. Puttaswamy (Aadhaar)* with certain restrictions, academic commentary has continued to question the adequacy of safeguards against function creep and data misuse. This body of literature highlights the tension between welfare-oriented governance and privacy protection but often stops short of analysing how AI technologies further intensify surveillance capabilities.

International scholarship on AI and surveillance provides valuable insights into the systemic risks posed by automated monitoring systems. Scholars such as Shoshana Zuboff have conceptualised modern surveillance as a form of "surveillance capitalism," where data extraction becomes a central mechanism of power. While Zuboff's work focuses primarily on private corporations, its insights are increasingly applied to State surveillance practices,

particularly in contexts where governments rely on private technology vendors. Other scholars have examined algorithmic governance and its implications for transparency, accountability, and democratic oversight, highlighting the dangers of decision-making systems that are opaque and resistant to scrutiny.

Human rights literature has also engaged extensively with mass surveillance and its impact on civil liberties. Reports by international organisations and civil society groups have emphasised that pervasive surveillance undermines freedom of expression and association, even in democratic societies. These studies stress the importance of judicial oversight, independent regulatory bodies, and effective remedies for individuals affected by unlawful surveillance. While such literature provides a normative framework grounded in international human rights law, its application to the Indian constitutional context remains underdeveloped.

In the Indian context, recent scholarship has begun to address the intersection of AI, data protection, and constitutional rights. Analyses of the Digital Personal Data Protection Act, 2023, have highlighted both its potential and its limitations. While some commentators view the Act as a step towards aligning India with global data protection standards, others criticise the broad exemptions granted to the State, particularly in matters of national security. This divergence in scholarly opinion reflects an ongoing debate about the appropriate balance between privacy and State interests in a rapidly digitising society.

Despite the growing body of literature on privacy and surveillance, a significant research gap remains in the comprehensive constitutional analysis of AI-enabled State surveillance in India. Much of the existing scholarship treats AI as a peripheral issue or focuses on data protection in isolation, without fully engaging with the broader constitutional implications of automated decision-making and predictive analytics. There is limited analysis of how AI surveillance interacts simultaneously with Articles 14, 19, and 21 of the Constitution, or how traditional constitutional doctrines must evolve to address systemic and cumulative harms.

This research seeks to bridge this gap by integrating constitutional jurisprudence, technological analysis, and human rights perspectives to provide a holistic examination of AI-driven State surveillance. By situating AI surveillance within the framework of constitutionalism and democratic accountability, the study aims to contribute to an emerging field of scholarship that addresses the challenges of governing technology in a rights-respecting manner.

1. **Nature and Evolution of State Surveillance in the Age of Artificial Intelligence**

   State surveillance in India has historically evolved in response to changing political, social, and technological conditions. Traditional surveillance mechanisms were largely reactive and targeted, relying on human intelligence, physical monitoring, and interception of communications under specific legal authorisation. These mechanisms, though intrusive, were constrained by practical limitations such as manpower, cost, and time. The introduction of Artificial Intelligence has fundamentally altered this paradigm by enabling the State to engage in large-scale, automated, and continuous monitoring of individuals and populations.

   AI-enabled surveillance systems operate through the collection and processing of vast datasets, including biometric information, communication metadata, location data, and behavioural patterns. Technologies such as facial recognition systems, predictive policing tools, and biometric identification platforms allow the State not only to monitor present activities but also to infer future behaviour. This predictive capacity marks a qualitative shift in the nature of surveillance, transforming it from an investigative tool into a mechanism of pre-emptive governance. Such a transformation raises profound constitutional concerns, as it expands State power in ways that were not envisaged when existing surveillance laws were enacted.

2. **The Right to Privacy under Article 21 and the Puttaswamy Framework**

   The recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* provides the primary constitutional framework for evaluating AI-enabled surveillance. The Supreme Court conceptualised privacy as encompassing bodily integrity, informational self-determination, and decisional autonomy. Importantly, the Court acknowledged that privacy is not an absolute right and may be restricted by the State, provided such restrictions satisfy the tests of legality, legitimate aim, necessity, proportionality, and procedural safeguards.

   Applying this framework to AI-based surveillance reveals significant constitutional deficiencies. While the State often invokes legitimate aims such as national security and public order, the legality requirement remains inadequately fulfilled. Many AI surveillance initiatives lack explicit statutory backing and operate through executive discretion. Moreover, the necessity and proportionality of such measures are rarely subjected to rigorous assessment. The continuous and automated nature of AI surveillance results in pervasive data collection that often exceeds what is strictly required to achieve stated objectives, thereby undermining the proportionality principle.

3. **Informational Privacy and Data Aggregation**

   One of the most significant threats posed by AI-enabled surveillance lies in its impact on informational privacy. Informational privacy concerns an individual's ability to control the collection, use, and dissemination of personal data. AI systems rely on data aggregation, combining information from multiple sources to create detailed profiles of individuals. This aggregation enables the State to infer sensitive attributes such as political preferences, religious beliefs, and social affiliations, even when such information is not explicitly disclosed.

   The constitutional harm arising from data aggregation is often cumulative rather than discrete. Individuals may consent to isolated instances of data collection, yet suffer privacy violations when such data is combined and analysed at scale. Existing legal frameworks do not adequately address this cumulative harm, focusing instead on individual acts of data collection. As a result, AI-enabled surveillance undermines informational self-determination and erodes the boundary between public and private life.

4. **Impact on Article 19: Chilling Effect on Democratic Freedoms**

   The pervasive nature of AI surveillance has a chilling effect on the freedoms guaranteed under Article 19 of the Constitution. Freedom of speech and expression, freedom of association, and freedom of movement are particularly vulnerable to indirect restrictions arising from constant monitoring. When individuals are aware that their online activities, communications, or physical movements are subject to surveillance, they may refrain from engaging in lawful dissent or political participation.

   This chilling effect does not manifest through explicit prohibitions but through self-censorship and behavioural modification. Constitutional jurisprudence recognises that indirect restrictions on fundamental rights can be as harmful as direct ones. AI-enabled surveillance, by creating an environment of constant observation, undermines the conditions necessary for free and open democratic discourse. The absence of transparency regarding surveillance practices further intensifies this effect, as individuals cannot assess the extent or legality of monitoring.

5. **Equality and Non-Arbitrariness under Article 14**

   AI-based surveillance also raises serious concerns under Article 14, which guarantees equality before the law and protection against arbitrary State action. Algorithmic decision-making systems are susceptible to bias arising from flawed training data, design choices, and implementation practices. In the context of surveillance, such

biases can result in disproportionate targeting of specific communities, particularly marginalised or minority groups.

Predictive policing tools, for example, rely on historical crime data that may reflect existing social and institutional biases. When such data is used to predict future criminal behaviour, it risks reinforcing discriminatory patterns and legitimising unequal treatment. The opacity of AI systems exacerbates this problem by making it difficult to identify and challenge biased outcomes. Without transparency and explainability, affected individuals are denied meaningful access to constitutional remedies.

6. **Procedural Safeguards and Judicial Oversight**

Procedural safeguards are a critical component of the constitutional framework governing surveillance. Judicial authorisation, independent oversight, and effective remedies are essential to prevent abuse of power. However, existing surveillance practices in India often lack robust procedural protections, particularly in the context of AI-enabled monitoring. Claims of national security and confidentiality are frequently invoked to limit disclosure and judicial scrutiny.

The technical complexity of AI systems also poses challenges for courts, which may lack the expertise necessary to evaluate algorithmic processes. This underscores the need for specialised oversight mechanisms and institutional capacity-building. Without effective procedural safeguards, constitutional rights risk becoming illusory, as individuals are unable to challenge unlawful surveillance in a meaningful manner.

7. **Adequacy of the Digital Personal Data Protection Act, 2023**

The Digital Personal Data Protection Act, 2023 represents an important development in India's data protection regime. However, its effectiveness in regulating State surveillance is limited by broad exemptions granted to the government. Provisions allowing the State to bypass data protection obligations in the interests of national security and public order dilute the Act's protective framework.

Moreover, the Act does not specifically address the challenges posed by AI-enabled surveillance, such as algorithmic transparency, bias mitigation, and automated decision-making. The absence of a dedicated surveillance law means that AI-based monitoring continues to operate in a fragmented regulatory environment, undermining constitutional accountability.

8. **Comparative and International Perspectives**

Comparative constitutional analysis reveals that several jurisdictions have recognised the unique risks posed by mass and AI-enabled surveillance. International human rights

bodies have emphasised the need for strict legal safeguards, transparency, and independent oversight. Judicial decisions from foreign courts have underscored that technological advancements do not diminish the State's obligation to respect fundamental rights.

While India's constitutional framework provides a strong normative foundation, its implementation remains uneven. Comparative insights highlight the importance of proactive legislative and judicial intervention to prevent the normalisation of surveillance practices that erode democratic values.

9. Towards a Rights-Centric Surveillance Framework

The constitutional challenges posed by AI-enabled surveillance necessitate a rethinking of regulatory approaches. A rights-centric framework must prioritise transparency, accountability, and proportionality. This includes the enactment of comprehensive surveillance legislation, mandatory judicial authorisation, algorithmic audits, and effective grievance redressal mechanisms.

By embedding constitutional principles into the design and deployment of AI systems, the State can harness technological innovation while respecting individual rights. Such an approach is essential to preserve the integrity of constitutional democracy in the digital age.

Conclusion

The rapid integration of Artificial Intelligence into State surveillance mechanisms marks a critical juncture in the evolution of constitutional governance in India. While technological innovation has undoubtedly enhanced the State's capacity to address challenges relating to security, crime prevention, and administrative efficiency, it has simultaneously expanded the scope and intensity of governmental intrusion into the private lives of individuals. This research has demonstrated that AI-enabled surveillance, by virtue of its automated, continuous, and predictive nature, poses a qualitatively distinct threat to fundamental rights, necessitating a recalibration of constitutional safeguards.

The recognition of the right to privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* established a robust constitutional framework for assessing State action in the digital age. However, the analysis undertaken in this study reveals a significant gap between constitutional principle and administrative practice. Many AI-driven surveillance initiatives in

India continue to operate without clear legislative authorisation, thereby undermining the requirement of legality. The reliance on executive discretion, coupled with fragmented statutory provisions, weakens democratic accountability and exposes individuals to unchecked surveillance.

This research further establishes that AI-enabled surveillance frequently fails to satisfy the test of proportionality under Article 21. The pervasive collection and analysis of personal data often exceed what is strictly necessary to achieve legitimate State objectives. Unlike traditional surveillance, AI systems enable mass monitoring and predictive profiling, resulting in continuous intrusion into informational privacy. Such practices risk normalising excessive surveillance and eroding the constitutional value of personal autonomy.

The study also highlights the profound impact of AI surveillance on democratic freedoms protected under Article 19. The chilling effect produced by constant monitoring discourages lawful dissent, free expression, and political participation. This indirect erosion of civil liberties, though subtle, poses a serious threat to the functioning of a constitutional democracy. When individuals modify their behaviour out of fear of surveillance, the marketplace of ideas essential to democratic governance is fundamentally compromised.

Equality concerns under Article 14 further compound these challenges. Algorithmic bias and lack of transparency in AI systems risk reinforcing existing social inequalities and legitimising discriminatory practices. The opacity of automated decision-making undermines the ability of individuals to challenge arbitrary or unequal treatment, thereby weakening constitutional remedies and the rule of law.

While the Digital Personal Data Protection Act, 2023 represents a step towards regulating data processing activities, its broad exemptions for State functions limit its effectiveness in addressing surveillance-related harms. The absence of a dedicated surveillance law tailored to the challenges posed by AI technologies leaves significant regulatory gaps. Without independent oversight and meaningful accountability mechanisms, constitutional protections remain largely theoretical.

In conclusion, this research underscores the urgent need for a rights-centric approach to regulating AI-enabled State surveillance in India. Technological advancement must not come

at the cost of constitutional values. The preservation of privacy, dignity, and democratic freedoms requires proactive legislative intervention, strengthened judicial oversight, and institutional mechanisms capable of addressing the complexities of AI systems. By aligning surveillance practices with constitutional principles, India can ensure that the digital transformation of governance reinforces, rather than undermines, the foundations of its constitutional democracy.

Bibliography

Books

1. M.P. Jain, *Indian Constitutional Law* (8th ed., LexisNexis 2022).
2. Granville Austin, *The Indian Constitution: Cornerstone of a Nation* (Oxford University Press 2014).
3. Gautam Bhatia, *The Transformative Constitution* (HarperCollins 2019).
4. Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019).

Journal Articles

1. Apar Gupta, "Privacy and Surveillance in India after *Puttaswamy*," *Indian Journal of Constitutional Law*.
2. Gautam Bhatia, "The Constitutional Case against Aadhaar," *National Law School of India Review*.
3. Vrinda Bhandari & Renuka Sane, "Data Protection and the Indian State," *Economic & Political Weekly*.
4. Lawrence Lessig, "Privacy and the Architecture of Law," *Harvard Law Review*.

Case Laws

1. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
2. *K.S. Puttaswamy (Aadhaar) v. Union of India*, (2019) 1 SCC 1.
3. *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
4. *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

Statutes

1. Constitution of India.
2. Information Technology Act, 2000.

3. Digital Personal Data Protection Act, 2023.

Reports & International Instruments

1. Justice B.N. Srikrishna Committee Report on Data Protection (2018).
2. Universal Declaration of Human Rights, 1948.
3. International Covenant on Civil and Political Rights, 1966.