International Journal of Teaching, Learning and Education (IJTLE)
ISSN: 2583-4371
Vol-4, Issue-3, May-Jun 2025
Journal Home Page: https://ijtle.com/
Journal DOI: 10.22161/ijtle

The Role of Law in Governing AI-Powered Surveillance Systems in India

Jyoti

B. Com, LLB, LLM, PGDCA, Kurukshetra University, Kurukshetra, Haryana, India

Received: 20 May 2025, Received in revised form: 16 Jun 2025, Accepted: 22 Jun 2025, Available online: 30 Jun 2025

Abstract

Artificial intelligence has increasingly been integrated into surveillance practices in India, reshaping how the State collects, processes, and uses personal data. This paper explores the legal and constitutional dimensions of AI-based surveillance, focusing on its compatibility with fundamental rights and democratic governance. It traces the development of surveillance laws, examines constitutional principles of privacy, equality, and proportionality, and assesses the adequacy of existing statutory frameworks. The study further analyses judicial approaches to surveillance and identifies ethical and human rights concerns, including discrimination, opacity, and constraints on civil liberties. By highlighting regulatory and institutional gaps, the paper underscores the need for a comprehensive legal framework that ensures effective oversight, transparency, and accountability in the use of AI-powered surveillance systems in India.

Keywords— Artificial Intelligence, AI-powered Surveillance, Transparency, Technological Shift.

I. INTRODUCTION

The rapid advancement of artificial intelligence (AI) has significantly transformed contemporary surveillance practices, redefining the scale, scope, and intensity of State monitoring. In India, AI-powered surveillance systems—such as facial recognition technologies, predictive policing tools, biometric databases, and automated CCTV analytics—are increasingly deployed for law enforcement, public safety, welfare delivery, and national security. Unlike traditional surveillance, which relied on human discretion and limited data processing, AI-enabled systems function through automated decision-making and large-scale data analytics. This technological shift raises profound legal and constitutional concerns, particularly regarding privacy, civil liberties, accountability, and democratic governance.

Surveillance by the State has long been justified in India on grounds of maintaining public order and safeguarding national security. However, the integration of AI introduces a qualitative change by enabling continuous, real-time, and often indiscriminate monitoring of individuals and populations. AI-driven surveillance systems can collect, process, and analyse vast amounts of personal data at unprecedented speed, increasing the risk of mass surveillance, profiling, and misuse of information. Consequently, the role of law becomes central in regulating such technologies to ensure that technological efficiency does not undermine constitutional freedoms.

From a constitutional standpoint, AI-powered surveillance directly implicates the right to privacy under Article 21 of the Constitution of India. The Supreme Court's landmark decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) affirmed privacy as an intrinsic component of life and personal liberty, subject to the tests of legality, necessity, and proportionality. Any surveillance measure must therefore be sanctioned by law, pursue a legitimate aim, and adopt the least restrictive means. AI-based surveillance systems, especially those deployed without comprehensive statutory backing, often struggle to meet these constitutional thresholds. Their

Cross Ref DOI: https://dx.doi.org/10.22161/ijtle.4.3.17

automated and opaque nature further complicates the assessment of proportionality and procedural fairness.

In addition to Article 21, AI surveillance also affects freedoms guaranteed under Articles 14 and 19 of the Constitution. Algorithmic surveillance tools may disproportionately target specific communities, leading to discriminatory outcomes and violations of equality before the law. Studies have demonstrated that facial recognition technologies exhibit higher error rates for women and marginalised groups, raising concerns of wrongful identification and arbitrary policing (Buolamwini & Gebru, 2018). Moreover, pervasive surveillance can create a chilling effect on free speech, expression, and association, thereby undermining the democratic fabric of society (Citron & Pasquale, 2014).

India's statutory framework governing surveillance remains fragmented and inadequately equipped to address the complexities of AI-driven technologies. Laws such as the Information Technology Act, 2000, the Code of Criminal Procedure, 1973, and the Telegraph Act, 1885 primarily regulate interception and data monitoring in limited contexts and were enacted in a pre-AI era. Although executive rules and guidelines supplement these statutes, they often lack transparency, independent oversight, and enforceable accountability mechanisms. The Digital Personal Data Protection Act, 2023, represents an important step towards regulating personal data processing; however, its broad exemptions for State surveillance on grounds such as national security and public order raise concerns about dilution of privacy safeguards (Government of India, 2023).

The use of AI-powered surveillance by law enforcement agencies further intensifies legal challenges. Technologies such as Automated Facial Recognition Systems are increasingly employed for criminal identification and crowd monitoring across Indian states. While these systems promise efficiency and improved crime detection, their deployment without clear legal standards raises serious concerns regarding consent, data accuracy, algorithmic bias, and access to remedies. The opacity of AI algorithms—often referred to as the "black box" problem—makes it difficult for individuals to challenge surveillance decisions or hold authorities accountable (Pasquale, 2015). This undermines principles of due process, transparency, and the rule of law.

At the same time, the State frequently justifies AI-enabled surveillance on grounds of national security, public order, and efficient governance. In an era marked by terrorism, cybercrime, and public health emergencies, surveillance technologies are portrayed as indispensable tools. However, Indian constitutional jurisprudence consistently emphasises that security concerns cannot override fundamental rights without adequate safeguards. The challenge lies in striking a balance between legitimate State interests and individual freedoms through precise legal standards, proportional safeguards, and robust oversight mechanisms.

II. REVIEW OF LITERATURE

Kakkar et al. (2023), provide one of the most systematic mappings of India's surveillance architecture through the lens of the Supreme Court's privacy jurisprudence. The report links India's interception-and-monitoring framework (built largely around the Telegraph Act/Rules and IT Act/Rules) with constitutional requirements of legality, necessity, and proportionality. It highlights how fragmented authorisations, licensing conditions, and executive procedures can expand surveillance capacity without equivalent public transparency or independent oversight. A key contribution is its doctrinal framing: *Puttaswamy* is treated as the benchmark for evaluating whether surveillance measures are sufficiently foreseeable, constrained, and reviewable, while also identifying governance gaps that become sharper when surveillance is automated or data-driven.

Feldstein's (2019) work offers a macro-level view of how AI surveillance expands across countries and introduces a taxonomy of enabling technologies and governance patterns. While not India-specific, it is frequently cited to contextualise national debates within a global trend: states adopt AI surveillance for a mix of legitimate administrative goals and more coercive monitoring. For Indian scholarship, the value lies in two ways: (i) it frames the regulatory question as one of distinguishing legitimate vs. rights-violating surveillance, and (ii) it highlights how market supply chains, procurement, and state capacity influence adoption. This literature supports comparative arguments that India's legal framework should not only authorise use, but embed democratic safeguards—independent oversight, transparency, and proportionality—before AI surveillance becomes entrenched infrastructure.

Rationale and Significance of the Study

Artificial intelligence–based surveillance has emerged as a central feature of contemporary governance in

Cross Ref DOI: https://dx.doi.org/10.22161/ijtle.4.3.17

India, reshaping how the State monitors, regulates, and manages populations. Technologies such as facial recognition, automated CCTV analytics, and predictive policing systems are increasingly embedded in everyday administrative and security practices. However, their rapid deployment has occurred in the absence of a dedicated and coherent legal framework tailored to the distinctive nature of AI-driven surveillance. Laws currently governing surveillance and data processing were conceived for earlier technological contexts and offer limited guidance on issues such as algorithmic decision-making, large-scale data integration, and automated identification. This disconnect between technological capability and legal preparedness forms the core rationale for undertaking the present study.

The study is significant because it addresses the growing tension between technological efficiency and constitutional governance. AI-powered surveillance has far-reaching implications for privacy, equality, and personal autonomy, particularly when systems function with minimal transparency or oversight. By examining these technologies through constitutional principles and judicial standards, the research contributes to a deeper understanding of how fundamental rights may be affected in practice. The findings of this study are relevant not only for academic discourse but also for legislators, courts, and regulatory bodies seeking to design effective oversight mechanisms. By clarifying legal responsibilities and identifying structural gaps, the research underscores the role of law as a normative guide capable of shaping responsible, accountable, and rights-respecting use of AI surveillance in a democratic society.

Objectives:

i. To examine the constitutional basis governing AI-powered surveillance in India.
ii. To analyse the adequacy of existing statutory frameworks regulating AI-based surveillance practices.

III. AI-POWERED SURVEILLANCE: CONCEPTUAL FRAMEWORK

Meaning and Typology of AI Surveillance Systems

AI surveillance systems are advanced monitoring frameworks that use artificial intelligence techniques such as machine learning, computer vision, and algorithmic decision-making to collect, process, and interpret data about individuals and groups. These systems are designed not merely to observe but to identify, classify, predict, and infer behaviour from large, continuously expanding datasets. A defining characteristic of AI surveillance is automation: decisions or risk assessments are generated with minimal human involvement, often through self-learning algorithms that evolve over time (Lyon, 2018). As a result, AI surveillance operates at a scale, speed, and depth that far exceed those of earlier monitoring technologies.

Facial Recognition, Predictive Policing, Data Analytics, and Biometrics

Facial recognition technology (FRT) is one of the most visible forms of AI surveillance, using biometric identifiers to match facial images captured by cameras with databases for identification or verification. Predictive policing systems apply algorithmic models to historical crime data to forecast crime hotspots or assess the likelihood of future offending, thereby influencing policing priorities (Perry et al., 2013). Data analytics–based surveillance integrates information from multiple sources—such as mobile data, CCTV feeds, financial records, and social media—to construct behavioural profiles and detect patterns. Biometric surveillance extends beyond facial recognition to include fingerprints, iris scans, voice recognition, and gait analysis, enabling persistent identification across different physical and digital environments (Jain et al., 2011).

Distinction Between Traditional and AI-Enabled Surveillance

Traditional surveillance systems are generally reactive, limited in scope, and dependent on direct human observation or manual data review. They typically focus on specific individuals or locations and require significant human discretion. In contrast, AI-enabled surveillance is proactive, continuous, and predictive, capable of analysing vast datasets in real time and generating probabilistic assessments about future behaviour (Citron & Pasquale, 2014). This shift transforms surveillance from episodic monitoring into a permanent infrastructure of observation, raising heightened legal concerns regarding transparency, accountability, proportionality, and the protection of fundamental rights.

Evolution of Surveillance Laws in India

The surveillance framework in India has evolved through distinct historical phases shaped by political authority, constitutional change, and technological advancement. Each phase reflects changing State priorities and expanding surveillance capacities, often

Cross Ref DOI: https://dx.doi.org/10.22161/ijtle.4.3.17

without corresponding development of comprehensive safeguards.

Colonial Origins of Surveillance Laws

The foundations of surveillance law in India were laid during the British colonial period, when monitoring was used as an instrument of political control and administrative security. The Indian Telegraph Act, 1885, empowered the colonial government to intercept communications on grounds of public safety and State security, granting the executive wide discretionary authority. Surveillance during this era focused on tracking nationalist movements, political communication, and public dissent, operating in the absence of constitutional protections or judicial oversight. This period established a centralised and control-oriented surveillance structure prioritising State interests over individual liberties.

Post-Independence Legal Developments

Following independence, India retained much of the colonial surveillance apparatus but situated it within a constitutional framework that recognised fundamental rights. Statutes such as the Code of Criminal Procedure, 1973, provided legal authority for investigation and monitoring, while communication interception continued under the Telegraph Act through executive rules. Judicial scrutiny gradually expanded, particularly through interpretations of Articles 14, 19, and 21, culminating in the recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017). Despite this progress, surveillance regulation remained fragmented and largely executive-driven, lacking a unified legislative framework (Kakkar et al., 2023).

Transition from Manual to Digital and AI-Based Surveillance

The shift from manual surveillance to digital monitoring began with the growth of electronic communication and data networks. The Information Technology Act, 2000, enabled lawful interception and monitoring of digital data, reflecting the State's response to cyber and security challenges. In recent years, surveillance has evolved further into AI-based systems that incorporate biometrics, facial recognition, and predictive analytics, transforming it into a continuous, automated process. This technological shift has outpaced legal reform, intensifying concerns related to proportionality, transparency, and constitutional accountability (Lyon, 2018).

Constitutional Foundations Governing Surveillance in India

The constitutional regulation of surveillance in India is anchored in the protection of fundamental rights and the requirement that State power be exercised in a non-arbitrary, proportionate, and procedurally fair manner. Surveillance is constitutionally permissible only when it conforms to these foundational principles.

Right to Privacy under Article 21

Surveillance directly implicates the right to privacy under Article 21, which encompasses personal autonomy, dignity, and informational self-determination. In *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), the Supreme Court affirmed privacy as a fundamental right and laid down a threefold test for State intrusion: the existence of a valid law, a legitimate State aim, and proportionality, along with procedural safeguards. This framework requires that surveillance measures must not be based solely on executive discretion and must be narrowly tailored to achieve their stated objectives (Puttaswamy, 2017). Any form of unchecked or mass surveillance would therefore be constitutionally suspect.

Articles 14 and 19: Equality, Freedom, and Proportionality

Surveillance practices must also comply with Article 14, which prohibits arbitrariness and discriminatory treatment. Algorithm-driven or selective surveillance that disproportionately targets specific groups may violate the principle of equality before the law. Further, Article 19 freedoms, including speech, movement, and association, are indirectly affected when pervasive monitoring creates a chilling effect on lawful expression and participation (Citron & Pasquale, 2014). The Supreme Court has increasingly applied the doctrine of proportionality to assess whether restrictions on these freedoms are necessary and least intrusive, as emphasised in *Anuradha Bhasin v. Union of India* (2020).

Doctrine of Reasonableness and Procedural Safeguards

The doctrine of reasonableness requires surveillance to be accompanied by procedural safeguards such as prior authorisation, recorded reasons, limited duration, and periodic review. In *PUCL v. Union of India* (1997), the Court held that telephone interception constitutes a serious privacy intrusion and mandated procedural controls to prevent abuse. Collectively, these constitutional principles ensure that surveillance

Cross Ref DOI: https://dx.doi.org/10.22161/ijtle.4.3.17

remains lawful, accountable, and consistent with democratic governance.

Statutory Framework Regulating AI-Based Surveillance in India

India does not yet have a dedicated statute governing AI-powered surveillance. Instead, regulation is derived from a combination of general surveillance laws, data protection legislation, and executive guidelines, which together form a fragmented statutory framework.

Information Technology Act, 2000 and Allied Rules

The **Information Technology Act, 2000,** provides the principal legal basis for digital surveillance in India. Sections 69, 69A, and 69B empower the State to intercept, monitor, and decrypt electronic information in the interests of sovereignty, security, public order, and crime prevention. These powers are operationalised through the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009. While the Act enables digital interception, it does not specifically regulate AI-driven analytics, automated profiling, or algorithmic decision-making, leaving significant gaps in accountability and transparency (Kakkar et al., 2023).

Code of Criminal Procedure and Police Powers

The **Code of Criminal Procedure, 1973 (CrPC)** authorises police surveillance and investigation through provisions related to search, seizure, and monitoring for criminal investigation. These powers were originally designed for manual policing and individualised suspicion. When extended to AI-based tools such as predictive policing or facial recognition, the CrPC lacks explicit safeguards to address mass data processing, algorithmic bias, or automated suspicion, raising concerns about proportionality and misuse.

Digital Personal Data Protection Act, 2023

The **Digital Personal Data Protection Act, 2023,** establishes a framework for lawful data processing, consent, and individual rights. However, it grants broad exemptions to the State for surveillance-related processing on grounds of national security and public order. These exemptions significantly limit the Act's effectiveness in restraining AI-based surveillance practices.

Sector-Specific Regulations and Executive Guidelines

AI surveillance is further governed by sector-specific rules and executive guidelines, such as CCTV norms, policing advisories, and facial recognition tenders. These instruments lack statutory force and independent oversight, resulting in uneven safeguards and limited legal accountability.

Judicial Approach to Surveillance and Privacy

The Indian judiciary has played a crucial role in shaping the legal boundaries of surveillance by interpreting constitutional guarantees in response to evolving technologies. Courts have increasingly recognised that surveillance, particularly when technology-driven, poses serious risks to privacy, liberty, and democratic freedoms.

Landmark Supreme Court Judgments

i Justice K.S. Puttaswamy (Retd.) v. Union of India (2017): The Supreme Court unanimously recognised the right to privacy as a fundamental right under Article 21. It held that any State surveillance must satisfy the tests of legality, legitimate aim, necessity, proportionality, and procedural safeguards, making privacy the constitutional foundation for reviewing surveillance practices.

ii PUCL v. Union of India (1997): This case dealt with telephone tapping and held that interception of communications constitutes an invasion of privacy. The Court mandated procedural safeguards such as prior authorisation, limited duration, and review committees to prevent arbitrary surveillance.

iii Anuradha Bhasin v. Union of India (2020): The Court examined restrictions on internet access and held that indefinite surveillance-related restrictions are unconstitutional. It emphasised proportionality, necessity, reasoned orders, and periodic review, reinforcing transparency in surveillance measures.

iv People's Union for Civil Liberties v. Union of India (Aadhaar Case) (2018): While upholding Aadhaar, the Court restricted data use and retention, disallowed private-sector access, and stressed purpose limitation. The judgment clarified that large-scale data collection must operate within strict constitutional limits.

v Paramvir Singh Saini v. Baljit Singh (2020): The Court directed the installation of CCTV cameras in police stations, highlighting surveillance as a tool for accountability. It also mandated oversight committees, recognising that surveillance must balance transparency with privacy protection.

High Court Rulings on Facial Recognition and CCTV Surveillance

High Courts have begun addressing the legality of facial recognition technology (FRT) and CCTV surveillance through public interest litigation. Courts have issued notices and sought State responses in cases challenging police use of FRT without statutory backing, reflecting concern over unchecked deployment (Elonnai Hickok et al., 2021). In matters relating to CCTV surveillance, courts have emphasised the need for controlled access and oversight, balancing privacy concerns with legitimate policing needs.

Emerging Judicial Trends in AI Governance

An emerging trend in Indian jurisprudence is the insistence on accountability, transparency, and institutional safeguards in technology-driven surveillance. Judicial directions on CCTV installation in police stations underscore the need for oversight structures and review mechanisms (Paramvir Singh, 2020). Collectively, these decisions indicate a cautious yet evolving judicial approach toward governing AI-enabled surveillance within constitutional limits.

AI Surveillance, Data Protection, and Informational Privacy

AI-powered surveillance systems intensify the interaction between State monitoring and informational privacy by enabling large-scale, automated processing of personal data. The legal challenges arise from how data are collected, analysed, and used, often without clear safeguards.

Data Collection, Consent, and Purpose Limitation

AI surveillance relies on continuous data collection from multiple sources, including CCTV footage, biometric databases, communication records, and location data. Such collection frequently occurs without meaningful consent, particularly in public spaces where individuals lack realistic choice (Solove, 2010). Data protection principles require that personal data be collected for specific, explicit, and lawful purposes and not repurposed for any other purpose. However, AI systems enable function creep, allowing data gathered for one purpose—such as traffic management or security—to be reused for unrelated surveillance activities. This undermines purpose limitation and weakens individual control over personal information.

Risks of Profiling, Bias, and Algorithmic Opacity

AI surveillance systems often rely on profiling and predictive analytics to assess behaviour or risk. Such profiling can reinforce social biases embedded in training data, resulting in discriminatory outcomes against marginalised groups (Buolamwini & Gebru, 2018). Algorithmic opacity further complicates oversight, as decision-making processes are frequently inaccessible or incomprehensible even to system operators. This “black box” nature makes it difficult to identify errors, contest adverse outcomes, or assess compliance with constitutional standards (Pasquale, 2015).

Accountability and Transparency Challenges

i. Opaque Decision-Making and Algorithmic Black Boxes: AI surveillance systems often operate through complex algorithms that are neither transparent to the public nor to the implementing authorities. This opacity makes it difficult to understand how decisions are made, assess accuracy, or identify bias, thereby limiting meaningful legal scrutiny and due process (Pasquale, 2015).

ii. Absence of Independent Oversight Mechanisms: Many AI surveillance deployments are authorised through executive decisions or administrative guidelines rather than detailed legislation. The lack of independent supervisory bodies and regular audits weakens accountability and increases the risk of arbitrary or excessive surveillance (Kakkar et al., 2023).

iii. Limited Public Disclosure and Informed Participation: Information about the scope, purpose, and operation of AI surveillance systems is rarely disclosed proactively. This restricts public awareness and prevents affected individuals from exercising data protection rights or challenging unlawful monitoring (Solove, 2010).

iv. Weak Grievance Redressal and Remedy Frameworks: Individuals subjected to AI-based surveillance often lack effective mechanisms to contest errors, misuse, or discriminatory outcomes. The absence of clear complaint procedures and remedial avenues undermines transparency and weakens trust in governance systems (Citron & Pasquale, 2014).

National Security, Public Order, and State Surveillance

State surveillance in India is frequently justified on grounds of national security and maintenance of public order. While these objectives are constitutionally recognised, their pursuit must remain consistent with fundamental rights and the rule of law.

Balancing Security Imperatives with Civil Liberties

Indian constitutional jurisprudence accepts that civil liberties may be restricted in exceptional circumstances, but such restrictions cannot be absolute. The Supreme Court has consistently held that national security does not create a rights-free zone and that State action must remain subject to constitutional scrutiny. Scholarly analysis emphasises that excessive reliance on security justifications risks transforming temporary exceptions into permanent governance tools, thereby weakening democratic accountability (Bhatia, 2019). The balance lies in ensuring that surveillance measures are narrowly tailored, legally authorised, and proportionate to the threat addressed.

Use of AI Surveillance in Policing and Intelligence

AI-enabled surveillance tools, such as facial recognition systems, predictive policing software, and real-time data analytics, are increasingly used by law enforcement and intelligence agencies. These systems expand surveillance from targeted monitoring to population-level observation and inference. Legal scholars caution that AI-driven intelligence practices amplify risks of profiling, bias, and erroneous suspicion, especially when algorithmic outputs are treated as neutral or objective (Ferguson, 2017). Without statutory clarity, such tools can blur the boundary between preventive security and intrusive monitoring.

Legal Limits on Mass and Real-Time Surveillance

Mass and real-time surveillance raise the gravest constitutional concerns because they often lack individualised suspicion and continuous oversight. Comparative constitutional scholarship highlights that bulk surveillance threatens informational privacy by normalising constant observation (Richards, 2012). Indian constitutional doctrine requires clear legal authority, strict necessity, temporal limits, and independent oversight. In the absence of these safeguards, AI-enabled mass surveillance risks violating the principles of proportionality and due process, even when justified by security or public order concerns.

Ethical and Human Rights Concerns in AI Surveillance

i. Ethical and Human Rights Concerns

The expansion of AI-powered surveillance raises serious ethical and human rights concerns, particularly where continuous monitoring intersects with democratic freedoms, equality, and international legal obligations.

ii. Chilling Effect on Free Speech and Association

Pervasive surveillance can discourage individuals from exercising fundamental freedoms of speech, expression, and association. When people are aware that their movements, communications, or gatherings are subject to monitoring, they may self-censor lawful activities to avoid scrutiny. Human rights scholars have observed that surveillance alters behaviour not through direct coercion but through the constant possibility of observation, thereby weakening democratic participation and dissent (Richards, 2012). International human rights bodies similarly recognise that surveillance, even when justified on security grounds, can have disproportionate effects on civil liberties if not strictly regulated (UN Human Rights Committee, 2018).

iii. Discrimination, Bias, and Exclusion Risks

AI surveillance systems frequently rely on historical datasets and algorithmic models that may embed social and institutional biases. When used for identification or risk assessment, such systems can disproportionately target marginalised communities, leading to unequal treatment and exclusion. Empirical research demonstrates that facial recognition technologies often produce higher error rates for women and minority groups, increasing the risk of misidentification and unjustified intervention (Buolamwini & Gebru, 2018). These outcomes conflict with principles of equality and non-discrimination that form the core of human rights law.

iv. International Human Rights Standards

International human rights instruments impose clear limits on surveillance practices. The International Covenant on Civil and Political Rights guarantees privacy, freedom of expression, and freedom of association, permitting restrictions only when lawful, necessary, and proportionate (ICCPR, 1966). The UN Special Rapporteur on the right to privacy has emphasised that mass and AI-enabled surveillance require heightened safeguards, transparency, and oversight to remain compatible with human rights norms (Cannataci, 2016).

IV. REGULATORY GAPS AND IMPLEMENTATION CHALLENGES IN INDIA

i *Absence of AI-Specific Surveillance Legislation:* India lacks a comprehensive law specifically regulating AI-powered surveillance, leading to reliance on outdated, fragmented statutes that do not address algorithmic decision-making.

ii *Overbroad Executive Discretion:* Surveillance authorisations are often issued through executive rules or administrative orders, limiting legislative scrutiny and increasing risks of arbitrary deployment.

iii *Weak Oversight and Audit Mechanisms:* There is no independent supervisory authority with clear powers to audit AI surveillance systems, assess compliance, or impose penalties.

iv *Broad National Security Exemptions:* Data protection and surveillance frameworks provide wide exemptions for State agencies on security grounds, diluting enforceable privacy safeguards.

v *Algorithmic Opacity and Lack of Explainability:* Many AI systems operate as “black boxes,” making it difficult to evaluate accuracy, bias, or compliance with constitutional standards.

vi *Risk of Bias and Discriminatory Outcomes:* AI surveillance tools may embed historical or social biases, disproportionately affecting marginalised communities without adequate corrective mechanisms.

vii *Function Creep and Secondary Use of Data:* Data collected for limited purposes is often reused across agencies and objectives, undermining purpose limitation and proportionality.

viii *Inadequate Public Transparency:* Limited disclosure regarding procurement, deployment, and scope of AI surveillance prevents informed public debate and accountability.

ix *Lack of Effective Remedies and Grievance Redressal:* Individuals subjected to AI-based surveillance face significant barriers in challenging errors, misuse, or rights violations.

x *Institutional Capacity and Technical Gaps:* Implementing agencies often lack trained personnel and standardised protocols to manage AI systems responsibly, increasing operational and legal risks.

Way Forward: Legal and Policy Recommendations

The rapid expansion of AI-powered surveillance in India calls for a structured legal and policy response that aligns technological governance with constitutional values and human rights standards.

Need for Comprehensive AI Surveillance Regulation

India requires a dedicated statutory framework specifically governing AI-based surveillance systems. Such legislation should clearly define permissible uses, limit deployment to legitimate and necessary objectives, and prohibit indiscriminate or mass surveillance. Legal provisions must mandate purpose limitation, data minimisation, and time-bound retention, while requiring prior authorisation for surveillance measures. Scholars emphasise that AI surveillance regulation should move beyond executive guidelines and establish enforceable rights and duties through parliamentary legislation. A rights-based framework would ensure consistency with constitutional proportionality and international human rights norms.

Strengthening Judicial and Parliamentary Oversight

Robust oversight is essential to prevent misuse of surveillance powers. Judicial oversight mechanisms should include independent authorisation and periodic review of AI surveillance measures, particularly where real-time or large-scale monitoring is involved. Parliamentary oversight through standing committees and reporting obligations can enhance democratic accountability by subjecting surveillance practices to legislative scrutiny. Comparative studies highlight that oversight institutions play a critical role in balancing security needs with civil liberties in democratic systems (European Union Agency for Fundamental Rights, 2020).

Incorporating Transparency, Auditability, and Accountability

Transparency must be embedded through public disclosure of surveillance policies, procurement processes, and operational standards. Mandatory algorithmic audits and impact assessments can help identify bias, inaccuracies, and rights risks. Clear accountability frameworks, including grievance redressal mechanisms and remedies for affected individuals, are necessary to uphold trust and the rule of law. Incorporating these safeguards would align AI surveillance governance with principles of fairness, accountability, and constitutional morality (Pasquale, 2015).

V. CONCLUSION

The expansion of AI-powered surveillance in India marks a critical juncture for constitutional governance, where technological capability increasingly intersects with fundamental rights. As discussed throughout this study, existing surveillance practices operate within a fragmented legal framework that was largely designed for earlier forms of monitoring and is ill-equipped to address the scale, automation, and opacity of AI-enabled systems. While national security and public order remain legitimate State objectives, their pursuit through advanced surveillance technologies raises serious concerns relating to privacy, equality, freedom of expression, and procedural fairness.

Judicial interventions, particularly after the recognition of the right to privacy as a fundamental right, have laid down clear constitutional standards of legality, necessity, proportionality, and accountability. However, the absence of comprehensive legislation and effective oversight mechanisms continues to allow broad executive discretion in the deployment of AI surveillance. Ethical and human rights challenges—such as profiling, bias, chilling effects on democratic participation, and lack of transparency—further underline the risks of unchecked technological governance.

The way forward requires a rights-centred legal framework that clearly regulates AI-based surveillance through statutory authorisation, judicial and parliamentary oversight, and enforceable safeguards. Embedding transparency, auditability, and accountability into surveillance systems is essential to ensure public trust and constitutional compliance. Ultimately, law must function not merely as an enabling tool for surveillance technologies but as a protective framework that preserves human dignity, democratic values, and the rule of law in the age of artificial intelligence.

REFERENCES

[1] Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency* (pp. 77–91). PMLR.

[2] Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Wash. L. Rev.*, *89*, 1.

[3] Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. In *the black box society*. Harvard University Press.

[4] Feldstein, S. (2019). *The global expansion of AI surveillance* (Vol. 17, No. 9). Washington, DC: Carnegie Endowment for International Peace.

[5] Kakkar, J., Kaur, N., Aravindakshan, S., Mohan, S., Agarwal, S., Movva, S., ... & Bhandari, V. (2023). The Surveillance Law Landscape in India and the Impact of Puttaswamy. *Centre for Communication Governance*.

[6] Jain, A., Bolle, R., & Pankanti, S. (2011). Introduction to biometrics. In *Biometrics: personal identification in networked society* (pp. 1-41). Boston, MA: Springer US.

[7] Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. John Wiley & Sons.

[8] Perry, W. L. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. Rand Corporation.

[9] Hickok, E. et al. (2021). Facial Recognition Technology in India. *Centre for Internet and Society.*

[10] *Cannataci, J. A. (2016). Report of the Special Rapporteur on the right to privacy. Human Rights Council.*

[11] Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. In The rise of big data policing. *New York University Press.*

[12] Solove, D. J. (2010). *Understanding privacy*. Harvard University Press.

[13] Richards, N. M. (2012). The dangers of surveillance. *Harv. L. Rev.*, *126*, 1934.

[14] Government of India. (2023). *Digital Personal Data Protection Act, 2023*. Ministry of Law and Justice.

[15] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

[16] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

[17] PUCL v. Union of India, (1997) 1 SCC 301.

[18] Paramvir Singh Saini v. Baljit Singh, (2020) 3 SCC 636.

[19] People's Union for Civil Liberties v. Union of India, (2018) 9 SCC 1.

[20] International Covenant on Civil and Political Rights. (1966). United Nations.

[21] UN Human Rights Committee. (2018). *General Comment No. 16: Right to privacy*. United Nations.

[22] European Union Agency for Fundamental Rights. (2020). Getting the future right. Artificial intelligence and fundamental rights.