INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

AI SURVEILLANCE AND CRIMINAL JUSTICE: A CONSTITUTIONAL ANALYSIS OF PRIVACY, POLICING, AND PREDICTIVE TECHNOLOGIES IN INDIA

AUTHORED BY - K JANAKI PRIYA

ABSTRACT

The rapid integration of artificial intelligence (AI) into criminal justice systems has fundamentally transformed traditional models of policing, investigation, and surveillance. Technologies such as facial recognition systems, predictive policing algorithms, biometric identification, and real-time data analytics are increasingly being deployed by law enforcement agencies in India. While these innovations promise enhanced efficiency, crime prevention, and administrative convenience, they simultaneously raise significant constitutional and legal concerns, particularly in relation to the right to privacy, due process, and civil liberties.

This research paper critically examines the use of AI-driven surveillance within the Indian criminal justice framework, with a primary focus on its compatibility with the right to privacy as recognised under Article 21 of the Constitution of India. The landmark judgment in Justice K.S. Puttaswamy v Union of India serves as the foundational basis for analysing informational privacy and the principles of legality, necessity, and proportionality.

The study further evaluates the absence of a comprehensive legal framework governing AI surveillance in India and highlights the risks of mass surveillance, algorithmic bias, lack of transparency, and potential misuse of personal data by state authorities. A comparative analysis with jurisdictions such as the European Union and the United States is undertaken to identify best practices and regulatory models.

The paper argues that while AI surveillance can be a powerful tool for law enforcement, its unregulated use poses a serious threat to constitutional freedoms. It concludes by advocating for a robust legislative framework that ensures accountability, transparency, and judicial oversight, thereby striking a balance between state security and individual rights.

ISSN: 2582-6433

KEYWORDS: Artificial Intelligence; Criminal Law; Surveillance; Right to Privacy; Article 21; Predictive Policing; Facial Recognition; Data Protection; Constitutional Law; Algorithmic Bias.

INTRODUCTION

The evolution of technology has consistently reshaped the contours of criminal law and law enforcement. In the 21st century, artificial intelligence (AI) has emerged as one of the most transformative tools in policing and criminal justice administration. From predictive policing algorithms to facial recognition systems and automated surveillance networks, AI-driven technologies are increasingly being integrated into the investigative and preventive functions of the State. In India, law enforcement agencies have begun adopting such tools to enhance efficiency, monitor criminal activity, and ensure public safety. However, this technological shift raises critical constitutional, legal, and ethical concerns.

At the heart of this debate lies the tension between State surveillance and individual privacy. The right to privacy, once considered implicit, has now been unequivocally recognised as a fundamental right under Article 21 of the Constitution by the Supreme Court in Justice K.S. Puttaswamy v Union of India.[1] The Court held that privacy includes informational autonomy and the right of individuals to control the dissemination and use of their personal data. This judgment has far-reaching implications for the legality of AI-based surveillance mechanisms, particularly those involving large-scale data collection and analysis.

Despite this constitutional recognition, India lacks a comprehensive statutory framework specifically regulating the use of AI in criminal justice. Existing laws such as the Information Technology Act, 2000 and provisions of the Code of Criminal Procedure, 1973 provide limited and fragmented safeguards.[2] Consequently, the deployment of AI surveillance technologies often operates in a legal grey area, raising concerns regarding arbitrary state action, lack of accountability, and potential misuse.

Furthermore, AI systems are not inherently neutral. Predictive policing tools, for instance, rely on historical data, which may reflect existing societal biases. This creates a risk of reinforcing

[1] *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.
[2] Information Technology Act 2000; Code of Criminal Procedure 1973.

ISSN: 2582-6433

discrimination against marginalised communities, thereby undermining the principles of equality and fairness enshrined in the Constitution.[3] The opacity of algorithmic decision-making further complicates matters, as individuals subjected to surveillance may have little or no recourse to challenge such actions.

Globally, jurisdictions such as the European Union have taken significant steps to regulate data protection and AI through instruments like the General Data Protection Regulation (GDPR), which emphasises transparency, consent, and accountability.[4] In contrast, India is still in the process of developing a cohesive regulatory framework, making it imperative to examine whether current practices align with constitutional mandates.

This research paper seeks to critically analyse the intersection of AI surveillance and criminal law in India. It explores whether the deployment of such technologies satisfies the constitutional tests of legality, necessity, and proportionality, and whether adequate safeguards exist to prevent abuse. By examining judicial precedents, statutory provisions, and comparative legal frameworks, the paper aims to contribute to the ongoing discourse on balancing technological advancement with the protection of fundamental rights.

HYPOTHESIS

The increasing deployment of artificial intelligence–based surveillance technologies in India's criminal justice system, in the absence of a comprehensive legal and regulatory framework, results in a disproportionate infringement of the fundamental right to privacy under Article 21 of the Constitution. Such use fails to consistently satisfy the constitutional tests of legality, necessity, and proportionality as laid down in Justice K.S. Puttaswamy v Union of India, thereby necessitating robust statutory safeguards, institutional oversight, and accountability mechanisms.

RESEARCH QUESTIONS

1. To what extent does the use of AI-driven surveillance technologies by law enforcement agencies in India infringe upon the right to privacy under Article 21 of the Constitution?

[3] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press 2017).
[4] Regulation (EU) 2016/679 (General Data Protection Regulation).

ISSN: 2582-6433

2. Whether the existing legal framework, including the Information Technology Act, 2000 and criminal procedural laws, is adequate to regulate AI-based surveillance in criminal justice?
3. Do AI surveillance mechanisms comply with the constitutional principles of legality, necessity, and proportionality established in *Puttaswamy*?
4. What are the risks associated with algorithmic bias, data misuse, and mass surveillance in the Indian context?
5. What regulatory lessons can India derive from international jurisdictions such as the European Union and the United States in governing AI surveillance?

OBJECTIVES OF THE STUDY

The present research aims to achieve the following objectives:

- To critically analyse the role and application of artificial intelligence in criminal justice, particularly in surveillance and policing.
- To examine the constitutional dimensions of privacy and personal liberty in light of AI-based technologies.
- To evaluate the adequacy of existing statutory and regulatory frameworks governing surveillance in India.
- To identify the legal, ethical, and social challenges posed by AI surveillance, including issues of bias, transparency, and accountability.
- To undertake a comparative analysis of international legal frameworks regulating AI and data protection.
- To propose recommendations for developing a comprehensive and constitutionally compliant regulatory framework for AI surveillance in India.

RESEARCH METHODOLOGY

This research paper adopts a **doctrinal (black-letter law) methodology**, which primarily involves the systematic analysis of legal principles, statutory provisions, and judicial precedents relevant to the subject of artificial intelligence–based surveillance in criminal law. The doctrinal approach is particularly suitable for this study as it seeks to examine the constitutional validity and legal implications of emerging technologies within the existing framework of Indian law.

ISSN: 2582-6433

The research relies extensively on **primary sources**, including constitutional provisions, statutes, and judicial decisions. Special emphasis is placed on the interpretation of Article 21 of the Constitution of India in light of the landmark judgment in Justice K.S. Puttaswamy v Union of India,[5] which laid down the foundational principles governing the right to privacy. Additionally, statutory instruments such as the Information Technology Act, 2000, and relevant provisions of the Code of Criminal Procedure, 1973 have been examined to assess their applicability to AI-driven surveillance mechanisms.[6]

The study also incorporates **secondary sources**, including academic commentaries, scholarly articles, books, law commission reports, and policy papers. Works by leading scholars on surveillance, data protection, and criminal justice have been analysed to understand theoretical perspectives and practical concerns associated with AI technologies.[7] These sources provide critical insights into issues such as algorithmic bias, mass surveillance, and the ethical implications of predictive policing.

Furthermore, a **comparative research method** has been employed to evaluate how other jurisdictions regulate AI surveillance and data protection. Legal frameworks such as the European Union's General Data Protection Regulation (GDPR) have been studied to identify best practices relating to transparency, accountability, and individual consent.[8] This comparative analysis enables the identification of regulatory gaps in the Indian context and assists in formulating informed recommendations.

The research is largely **analytical and descriptive** in nature. It not only explains the current legal position but also critically evaluates whether existing laws adequately address the challenges posed by AI surveillance. The study applies constitutional tests such as legality, necessity, and proportionality to assess the validity of state actions involving surveillance technologies.

However, the research is subject to certain limitations. Given the relatively recent emergence of AI technologies in criminal justice, there is a limited body of judicial precedent directly

[5] *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.
[6] Information Technology Act 2000; Code of Criminal Procedure 1973.
[7] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press 2017); Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019).
[8] Regulation (EU) 2016/679 (General Data Protection Regulation).

ISSN: 2582-6433

addressing these issues in India. Consequently, the study relies on analogous legal principles and comparative jurisprudence to bridge this gap.

LITERATURE REVIEW

The intersection of artificial intelligence, surveillance, and criminal justice has attracted significant scholarly attention in recent years. The growing reliance on data-driven policing and algorithmic decision-making has prompted critical debates regarding privacy, accountability, and the rule of law. This section reviews key academic contributions that inform the present study, with particular emphasis on surveillance theory, predictive policing, and constitutional protections.

One of the most influential contributions to the discourse on surveillance and data-driven policing is by Andrew Guthrie Ferguson, who, in *The Rise of Big Data Policing*, examines how predictive policing technologies rely on historical crime data to forecast future criminal activity.[9] Ferguson argues that while such systems may enhance efficiency, they risk perpetuating existing social and racial biases embedded within historical datasets. This insight is particularly relevant in the Indian context, where socio-economic disparities and systemic biases may be reflected in policing data, thereby raising concerns about fairness and equality before the law.

Similarly, Shoshana Zuboff's seminal work, *The Age of Surveillance Capitalism*, provides a broader theoretical framework for understanding the implications of mass data collection and surveillance.[10] Zuboff critiques the transformation of personal data into a commercial and political resource, arguing that unchecked surveillance undermines individual autonomy and democratic values. Although her analysis primarily focuses on corporate actors, its implications extend to state surveillance, especially where governments deploy AI technologies without adequate safeguards.

In the Indian context, scholars have increasingly focused on the constitutional dimensions of privacy following the landmark decision in Justice K.S. Puttaswamy v Union of India.[11] Legal

[9] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press 2017).
[10] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019).
[11] *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.

ISSN: 2582-6433

commentators have emphasised that the recognition of privacy as a fundamental right imposes a positive obligation on the State to ensure that any intrusion into personal liberty is backed by law and satisfies the tests of necessity and proportionality. Scholars such as Gautam Bhatia have argued that the *Puttaswamy* judgment represents a transformative moment in Indian constitutional law, establishing a rights-based framework for evaluating surveillance practices.[12]

Further, academic literature has examined the concept of **algorithmic opacity** or the "black box" nature of AI systems. Frank Pasquale, in *The Black Box Society*, highlights the dangers of decision-making processes that are not transparent or easily understood.[13] In the context of criminal justice, such opacity can hinder accountability, as individuals subjected to surveillance or predictive assessments may lack the means to challenge or even comprehend the basis of such decisions.

Another critical strand of literature focuses on **data protection and regulatory frameworks**. The European Union's approach, particularly through the GDPR, has been widely analysed as a model for balancing innovation with fundamental rights.[14] Scholars have noted that principles such as data minimisation, purpose limitation, and informed consent are essential in regulating surveillance technologies. In contrast, Indian scholarship frequently highlights the absence of a comprehensive data protection regime, which exacerbates the risks associated with AI deployment in law enforcement.

Additionally, literature on **human rights and technology** underscores the need for international norms governing AI use. Reports by organisations such as the United Nations and various human rights bodies emphasise that surveillance technologies must comply with established human rights standards, including legality, necessity, and proportionality.[15] These principles align closely with the constitutional framework articulated in *Puttaswamy* and provide a useful benchmark for evaluating domestic practices.

[12] Gautam Bhatia, *The Transformative Constitution* (HarperCollins India 2019).
[13] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).
[14] Regulation (EU) 2016/679 (General Data Protection Regulation).
[15] United Nations Human Rights Council, 'The Right to Privacy in the Digital Age' (2018).

ISSN: 2582-6433

Despite the growing body of literature, there remains a significant gap in scholarship specifically addressing the intersection of AI surveillance and Indian criminal law. Much of the existing work is either theoretical or focused on data protection in general, rather than the specific implications for policing and criminal justice. This research seeks to bridge that gap by providing a focused, doctrinal, and comparative analysis of AI surveillance within the Indian legal framework.

1. Concept and Evolution of AI Surveillance in Criminal Justice

Artificial Intelligence (AI) has emerged as a transformative force in modern criminal justice systems, fundamentally altering traditional methods of policing and investigation. AI surveillance refers to the use of machine learning algorithms, data analytics, facial recognition systems, and predictive tools to monitor, identify, and analyse criminal behaviour. These technologies operate by processing vast datasets, enabling law enforcement agencies to identify patterns, predict potential criminal activity, and respond proactively.

In India, the adoption of AI surveillance tools has accelerated in recent years. Systems such as facial recognition technology (FRT), automated number plate recognition (ANPR), and predictive policing software have been deployed in various states. These tools aim to enhance efficiency and reduce crime rates; however, their deployment raises significant concerns regarding legality and oversight. Unlike traditional surveillance methods, AI surveillance operates on a scale and speed that can potentially result in mass surveillance, thereby impacting a large section of the population indiscriminately.

The evolution of surveillance from physical monitoring to digital and algorithmic tracking represents a shift from targeted investigation to preventive and often speculative policing. This transformation necessitates a re-evaluation of existing legal frameworks to ensure that technological advancements do not outpace constitutional protections.

2. Constitutional Framework: Right to Privacy and Article 21

The constitutional validity of AI surveillance must be examined in light of the right to privacy under Article 21 of the Constitution of India. The Supreme Court in Justice K.S. Puttaswamy v Union of India unequivocally recognised privacy as a fundamental right, encompassing informational privacy, bodily autonomy, and decisional freedom.[16]

[16] *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.

ISSN: 2582-6433

The Court laid down a threefold test to determine the legitimacy of state interference with privacy:

- **Legality**: The existence of a valid law
- **Necessity**: A legitimate state aim
- **Proportionality**: Rational nexus between means and objective

AI surveillance technologies often struggle to satisfy these requirements. Firstly, there is no specific legislation in India governing the use of AI in criminal justice. Secondly, while crime prevention constitutes a legitimate aim, the indiscriminate collection of data may fail the necessity test. Finally, the proportionality requirement is frequently undermined when surveillance measures are excessive or lack adequate safeguards.

The absence of procedural safeguards and judicial oversight further exacerbates the risk of arbitrary state action, thereby undermining constitutional guarantees.

3. Legal Framework Governing Surveillance in India

India's current legal framework for surveillance is fragmented and inadequate in addressing AI-driven technologies. Key legislations include the Information Technology Act, 2000, and the Code of Criminal Procedure, 1973.[17]

The Information Technology Act provides certain provisions relating to data interception and monitoring, particularly under Section 69, which empowers the government to intercept, monitor, or decrypt information in the interest of sovereignty and security. However, these provisions were not designed to regulate advanced AI technologies and lack specific safeguards for algorithmic accountability.

Similarly, the Code of Criminal Procedure contains provisions relating to search, seizure, and investigation, but it does not contemplate the use of automated surveillance systems or predictive analytics. Consequently, the legal framework fails to address critical issues such as data retention, algorithmic transparency, and individual rights against automated decision-making.

This regulatory gap creates a legal vacuum, allowing law enforcement agencies to deploy AI technologies without clear statutory backing or accountability mechanisms.

4. Predictive Policing and Algorithmic Bias

[17] Information Technology Act 2000; Code of Criminal Procedure 1973.

ISSN: 2582-6433

Predictive policing is one of the most controversial applications of AI in criminal justice. These systems analyse historical crime data to forecast future criminal activity and allocate police resources accordingly. While such tools may enhance efficiency, they are inherently dependent on the quality and neutrality of the data used.

As highlighted by Andrew Ferguson, predictive policing systems often reinforce existing biases present in historical datasets.[18] In societies with entrenched inequalities, such as India, this can lead to disproportionate targeting of marginalised communities, thereby violating the principle of equality before the law under Article 14.

Algorithmic bias is further exacerbated by the lack of transparency in AI systems. The "black box" nature of algorithms makes it difficult to understand how decisions are made, thereby limiting accountability and judicial scrutiny. This raises serious concerns regarding due process, as individuals may be subjected to surveillance or suspicion without clear justification.

5. Facial Recognition Technology and Mass Surveillance

Facial recognition technology (FRT) represents one of the most intrusive forms of AI surveillance. It enables the identification of individuals in real time by analysing biometric data captured through cameras. In India, FRT has been used in public spaces, protests, and law enforcement operations.

While FRT can be a valuable tool in identifying suspects, its widespread use raises concerns about mass surveillance and chilling effects on fundamental freedoms such as the right to freedom of expression and assembly. The indiscriminate use of such technology may deter individuals from participating in lawful activities due to fear of constant monitoring.

Moreover, studies have shown that facial recognition systems are prone to errors, particularly in identifying individuals from diverse demographic backgrounds. This increases the risk of wrongful identification and potential miscarriages of justice.

6. Comparative Analysis: International Approaches

A comparative analysis reveals that several jurisdictions have taken proactive steps to regulate AI surveillance. The European Union, through the General Data Protection Regulation (GDPR), imposes strict requirements on data processing, including principles of transparency, accountability, and consent.[19]

[18] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press 2017).

[19] Regulation (EU) 2016/679 (General Data Protection Regulation).

ISSN: 2582-6433

Additionally, the EU has proposed the Artificial Intelligence Act, which seeks to classify AI systems based on risk and impose corresponding regulatory obligations. High-risk systems, such as those used in law enforcement, are subject to stringent requirements, including human oversight and risk assessments.

In the United States, while there is no comprehensive federal legislation governing AI, certain states have introduced regulations restricting the use of facial recognition technology by law enforcement agencies.

These international approaches highlight the importance of a structured regulatory framework that balances innovation with the protection of fundamental rights.

7. Challenges and Concerns

The deployment of AI surveillance in criminal justice raises several critical challenges:

- **Lack of Transparency**: AI systems often operate as opaque "black boxes."
- **Absence of Accountability**: Limited mechanisms to hold authorities accountable for misuse.
- **Data Privacy Risks**: Large-scale collection and storage of personal data.
- **Potential for Abuse**: Surveillance tools may be used for political or discriminatory purposes.
- **Chilling Effect**: Impact on fundamental freedoms such as speech and assembly.

These challenges underscore the urgent need for a comprehensive regulatory framework governing AI surveillance in India.

CONCLUSION

The integration of artificial intelligence into the criminal justice system marks a significant shift in the nature of policing and surveillance. While AI-driven technologies such as predictive policing, facial recognition, and data analytics offer considerable advantages in enhancing efficiency and crime prevention, their deployment raises serious constitutional and legal concerns. The central issue lies in balancing the legitimate interests of the State in maintaining law and order with the protection of individual rights and liberties.

The recognition of the right to privacy as a fundamental right in Justice K.S. Puttaswamy v Union of India has fundamentally altered the constitutional landscape in India. Any form of surveillance, including AI-based mechanisms, must now satisfy the tests of legality, necessity, and proportionality. However, as this research has demonstrated, the current use of AI

ISSN: 2582-6433

surveillance technologies in India often operates in a legal vacuum, lacking a clear statutory foundation and adequate safeguards.

The absence of a comprehensive regulatory framework exacerbates risks such as mass surveillance, algorithmic bias, lack of transparency, and potential misuse of personal data. Furthermore, the opaque nature of AI systems undermines accountability and due process, raising concerns about arbitrary state action and the erosion of civil liberties. The reliance on outdated legal provisions, which were not designed to address modern technological challenges, further highlights the inadequacy of the existing legal regime.

Comparative analysis reveals that jurisdictions such as the European Union have adopted robust regulatory frameworks that prioritise data protection, transparency, and accountability. India, by contrast, is still in the nascent stages of developing such a framework, making it imperative to adopt a proactive and rights-based approach to AI regulation.

In conclusion, while AI surveillance holds significant potential for improving criminal justice outcomes, its unregulated use poses a serious threat to constitutional freedoms. A careful and calibrated approach is required to ensure that technological advancements do not come at the cost of fundamental rights.

SUGGESTIONS AND RECOMMENDATIONS

In light of the findings of this research, the following recommendations are proposed:

1. Enactment of Comprehensive AI Legislation

India must introduce a dedicated legal framework regulating the use of artificial intelligence in criminal justice. Such legislation should clearly define the scope, limitations, and permissible uses of AI surveillance technologies.

2. Strengthening Data Protection Laws

A robust data protection regime is essential to safeguard personal information collected through surveillance systems. The law must incorporate principles such as data minimisation,

ISSN: 2582-6433

purpose limitation, and informed consent, drawing inspiration from international frameworks like the GDPR.[20]

3. Judicial Oversight and Accountability

The deployment of AI surveillance technologies should be subject to prior judicial approval and continuous oversight. Independent regulatory bodies should be established to monitor compliance and address grievances.

4. Ensuring Transparency and Explainability

AI systems used in criminal justice must be transparent and explainable. Authorities should be required to disclose the functioning and decision-making processes of such systems to ensure accountability.

5. Addressing Algorithmic Bias

Measures must be taken to identify and mitigate biases in AI systems. This includes regular audits, diverse datasets, and independent evaluations to ensure fairness and non-discrimination.

6. Limiting Mass Surveillance

The use of AI surveillance should be strictly limited to specific, legitimate purposes. Blanket or indiscriminate surveillance must be prohibited to prevent violations of fundamental rights.

7. Capacity Building and Training

Law enforcement agencies should be trained in the ethical and legal use of AI technologies. This will help ensure responsible deployment and minimise misuse.

8. Public Awareness and Participation

Public engagement is crucial in shaping policies related to AI surveillance. Transparent policymaking processes will enhance legitimacy and trust in the system.

[20] Regulation (EU) 2016/679 (General Data Protection Regulation).

ISSN: 2582-6433

BIBLIOGRAPHY

A. CASES

- *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1
- *Maneka Gandhi v Union of India* (1978) 1 SCC 248
- *People's Union for Civil Liberties (PUCL) v Union of India* (1997) 1 SCC 301

B. LEGISLATIONS

- Constitution of India, 1950
- Information Technology Act 2000
- Code of Criminal Procedure 1973
- Regulation (EU) 2016/679 (General Data Protection Regulation)

C. BOOKS

- Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (NYU Press 2017)
- Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019)
- Gautam Bhatia, *The Transformative Constitution* (HarperCollins India 2019)
- Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015)

D. JOURNAL ARTICLES

- Andrew D Selbst and Julia Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 *International Data Privacy Law* 233
- Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76
- Tal Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 *Seton Hall Law Review* 995

E. REPORTS AND ONLINE SOURCES

- United Nations Human Rights Council, 'The Right to Privacy in the Digital Age' (2018)
- NITI Aayog, *National Strategy for Artificial Intelligence* (2018)

ISSN: 2582-6433

- Justice B.N. Srikrishna Committee Report on Data Protection (2018)

F. MISCELLANEOUS

- Government of India reports and policy papers on surveillance and AI
- Relevant news articles and expert commentaries on AI policing in India