Volume 44, March 2026 ISSN 2581-5504

"Eyes Everywhere: AI Surveillance is Threat to Fundamental Rights"

Prakriti
L.L.M., (AI Data Protection and Technology Law)
Dhirubhai Ambani University,
Gandhinagar

I. ABSTRACT

The swift development of artificial intelligence-driven surveillance technology, such as facial recognition software, automated law enforcement tools, and large-scale data analytics, has impacted contemporary governance and security practices. Although these technologies are usually defended on the grounds of effectiveness, crime prevention, and national security, they gravely compromise fundamental rights[1], such as, equality, dignity, and freedom of speech. The main inquiry issue this study aims to address is whether existing legal and constitutional frameworks are adequate to regulate AI-based surveillance and prevent the degradation of fundamental rights in democratic countries.

While topics such as data protection and online security have received more scholarly consideration, there is a clear research gap[2] in the form of inadequate normative analysis that connects AI surveillance techniques with human rights law and constitutional rights jurisprudence. Because most of the information that is now published focuses on either general data protection principles or technological efficiency, challenges like accountability, proportionality, and democratic supervision of AI-enabled surveillance[3] systems remain unfinished. This study explores laws, judicial decisions, international human rights treaties, and constitutional requirements using a doctrinal and qualitative research technique. Furthermore, it draws parallels with countries such as the US, India, and the EU.

The deployment of AI spying without robust legal safeguards runs the risk of normalizing widespread surveillance and undermining the rule of law, the study claims. It concludes by emphasizing the need for rights-based regulatory frameworks, transparency standards, and practical remedies to ensure that technological advancements don't reach the expense fundamental freedoms. With the goal to analyze the significant threats that Artificial Intelligence (AI)[4] presents to fundamental rights and constitutional principles in the digital era, this thesis addresses the regulation of facial recognition technology (FRT).

The study analyzes how of FRT, especially and public surveillance, increases risks to privacy, data security, and freedom of speech and, most importantly, access effective remedies by

[1] , 'The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression', Journal of, Vol 30, No 1, 2019, pp. 40-52.
[2] P. N. Howard, The digital origins of dictatorship and democracy: Information technology and political Islam, Oxford University Press (Oxford: United Kingdom), 2010.
[3] Feldstein, S. (2019). *The global expansion of AI surveillance* (Vol. 17, No. 9, pp. 1-42). Washington, DC: Carnegie Endowment for International Peace.
[4] Atif, M., & Alamgir, A. (2025). The Illusion of Security: How AI-Powered Surveillance Erodes Privacy, Amplifies Inequality, and Redefines Democracy in the Digital Age. *Social Science Review Archives*, *3*(4), 1516-1528.

Volume 44, March 2026 ISSN 2581-5504

placing it at the nexus[5] of technological innovation and legal frameworks. The study presents, a methodological procedure intended to foresee and reduce the problems associated with high-risk AI systems.

Keywords**:** Artificial intelligence Surveillance, Right to Privacy, Fundamental rights, Facial Recognition Technology, Digital Personal Data Protection Act.

II. INTRODUCTION

The growth of technology has brought about remarkable transformations in modern human societies. most developments is rise (AI), which companies, other collect, analyze, and use information[6]. AI surveillance technology, such as facial recognition cameras, biometric databases, predictive policing tools, and large-scale data analytics, are being used more often in cities, airports, train stations, schools, and public spaces. The aforementioned technologies allow authorities to monitor individuals in real time and examine vast volumes of personal data. The following piece first evaluates the limited proof on the efficacy of several surveillance tools[7]. Next, the degree to which their use has been—and, statute and evidentiary law—is considered. This assessment obtaining and analyzing previously collected, computational methods.

Even while AI tracking provides more efficiency and public safety, it raises serious concerns about human liberties and fundamental rights. In democracies, continual surveillance can have a chilling effect on people's behavior by limiting their freedom of expression, association, and personal autonomy. Scholars claim that uncontrolled monitoring technology might transform democratic governance into an ongoing surveillance system. In India, surveillance technology has grown significantly in recent years. Government attempts like AI-enabled law enforcement systems[8], predictive policing tools, and show increasing dependence on monitoring. Proponents claim that these forms of technology help combat crimes such as terrorism and human trafficking. The lack of comprehensive laws directing AI monitoring, according to critics, elevates the potential of misuse and arbitrary government action. The Indian constitution guarantees some essential rights that are personally impacted by surveillance technologies[9], freedom privacy. Article 19 safeguards freedoms such as speech, expression, and association. Article 14 guarantees equality before the law. AI monitoring equipment have

[5] Chan, H. W. H., & Lo, N. P. K. (2025). A study on human rights impact with the advancement of artificial intelligence. *Journal of Posthumanism*, *5*(2), 1114-1153.

[6] F. Pasquale, The black box society: The secret algorithms that control money and information, Harvard University Press (Cambridge, Massachusetts: United States of America), 2015.

[7] N. Ettlinger, 'Algorithmic affordances for productive resistance', Big Data & Society, Vol 5, No 1, 2018.

[8] Ünver, H. A. (2024). Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights. *Depth Analysis requested by the Subcommittee on Human Rights (DROI) of the European Parliament, Policy Department for External Relations, Directorate-General for External Policies of the Union, PE*, *754*.

[9] V. Eubanks, Automating inequality: How high-tech tools profile, police, and punish the poor, St. Martin's Press (New York, New York State: United States of America), 2018

the potential to violate basic constitutional freedoms if they are used without adequate protections.

The intention of this study is to figure out if AI-driven monitoring represents a danger to India's basic freedoms. The study looks at the constitutional basis of privacy rights, considers the ethical and legal[10] concerns regarding AI monitoring, and assesses important court decisions. It also recommends regulatory measures to ensure that technology progress is consistent with constitutional norms. The typical on a basis, including, smart monitoring, automated. Despite their extensive usage, little is known about the effectiveness of these surveillance technologies[11] in achieving governmental goals, as well as their reliability and empirical validity. The Civil Liberties, and Justice and Home Affairs Council (LIBE) Inquiry into the pervasive surveillance of EU people was the first comprehensive inquiry into the claims made by former NSA employee Edward Snowden and their impact on the fundamental rights of EU citizens. The European Parliament knew that we had already begun the legislative process with the data safeguarding laws and directive, which have given us a unique perspective on privacy concerns worldwide, in addition to Edward Snowden's revealing testimony. As a result, the investigation was able to be more thorough from the outset, covering both the areas where the EU has ownership and the areas where EU nationals have concerns. Given that the EU has already decided to completely overhaul its own outdated internet, privacy, and data collection laws, the Snowden accusations come at a critical juncture for the continent. This new information, which demonstrated the previously undiscovered scope of communication surveillance of common people by intelligence authorities worldwide, has led to a lack of confidence that heads of state and the EU are not guaranteeing adequate protections for citizens and upholding the fundamental values enshrined in both the European Convention on Human Rights and the Charter of the Fundamental Rights. Given that the EU has already decided to completely overhaul its own outdated internet, privacy, and data collection laws, the Snowden accusations come at a critical juncture for the continent. This new information, which demonstrated the previously undiscovered scope of communication surveillance of common people by intelligence authorities worldwide, has led to a lack of confidence that heads of state and the EU are not guaranteeing adequate protections for citizens and upholding the fundamental values enshrined in both the European Convention on Human Rights and the Charter of the Fundamental Rights. The goal of this study is not to develop new legal theory or make theoretical contributions. In order to provide an organized framework for evaluating and suggesting regulations on unacceptable risk AI systems, it makes use of the central tenet of legal positivism. This article explains the necessity for a legal framework that methodically adheres to the principles of the rule of law and human-rights-based approach, rather than evaluating or assessing pertinent legal provisions or their effectiveness. Furthermore, the purpose of this essay is to demonstrate the possible role of law in controlling and evaluating

[10] Watt, E. (2017). The right to privacy and the future of mass surveillance. *The International Journal of Human Rights*, *21*(7), 773-799.

[11] Al-Bayed, M. H., Haddad, I., Abu-Nasser, B. S., & Abu-Naser, S. S. (2025). Surveillance in the Age of AI: Navigating Ethical Boundaries and Human Rights.

the consequences of unacceptable risk AI systems rather than to debate the boundaries of the relevant legal frameworks. It continues by outlining the nature of states' duties to regulate unacceptable risk AI systems and arguing government agencies have an international need to regulate their usage domestically in order to protect the rule of law. Lastly, the paper assesses the legal implications of states' incapacity to control these kinds of devices and looks at possible legal remedies. The article offers an overview of a number of relevant EU regulations rather than a thorough case study. The article's conclusion is that any regulations must certainly follow the law.

III. HISTORICAL AND CONSTITUTIONAL BACKGROUND

The Indian Telegraph Act of 1885 and the postal Service Act of 1898, two colonial-era statutes that permitted the state to undertake Surveillance with no accountability, have continuously dominated India for "public emergency" or "national security"[12] without particular, insufficient criteria, upholds this practice in the post-independence era.

i. **Evolution of Surveillance -** Surveillance has been utilized for decades by states to safeguard security and social order. Traditional surveillance methods encompassed manual record-keeping, informant networks, and physical monitoring. However, the digital revolution has impacted monitoring techniques. Artificial intelligence has made it feasible for governments to manage massive amounts of data, empowering them to automatically monitor citizens on a scale never seen before. ***The following AI surveillance systems are now in use:***

- Facial Recognition Technology (FRT)
- Biometric identification systems
- Predictive policing algorithms
- Big data analytics
- Automated video surveillance

These technologies allow authorities to keep an eye on people's whereabouts, analyze behavioral patterns, and predict potential criminal activity. In the past, governments have used surveillance as a vital instrument to ensure national security, maintain law and order, and monitor potential threats. The primary sources of surveillance in the past were human observation, physical monitoring[13], and intelligence networks. Ancient and medieval kings routinely recruited spies and informants to learn about political opponents and potential uprisings. Throughout the colonial era, monitoring grew more and more formalized under British administration. The colonial government enacted laws that allowed them to monitor political activists and suppress resistance. Surveillance was used to maintain colonial control

[12] Margulies, P. (2016). Surveillance by algorithm: The nsa, computerized intelligence collection, and human rights. *Fla. L. Rev.*, *68*, 1045.
[13] Lyon, D. (2007). Surveillance studies : An overview. Cambridge: polity press

Volume 44, March 2026 ISSN 2581-5504

and quell nationalist movements. Widespread state monitoring was the result of these efforts, and this had an effect on the judicial system[14].

ii. **Constitutional Protection of Fundamental Rights -** The Indian Constitution protects individual freedom from state interference by guaranteeing a few essential rights. One of these rights' most pressing issues in the digital age is privacy. In Justice K.S. Puttaswamy v. Union of India (2017)[15], a Supreme Court decided that the right to privacy is a fundamental right under Article 21 of the Constitution[16]. Additionally developed a three-part test for determining whether government steps that encroach on privacy are constitutional legality the action must have a sound legal basis. Requirement are based on the pursue a legitimate governmental objective. Proportionality of the incursion must match the objective. This decision expanded the constitutional protections against arbitrary snooping.

Any government activity, must adhere to principles of fairness and nondiscrimination. For example, facial recognition systems may misidentify certain groups of people more frequently than others. The equality principle of Article 14 may be violated by these outcomes. Article 19 of the Constitution protects a number of essential rights necessary for a democratic society. These include: **Article 19(1)(a):** Freedom of opinion and speech AI surveillance systems that constantly monitor public spaces may discourage individuals from exercising **Article 19(1)(b):** The right to peaceful assembly and Article 19(1)(c): The freedom to form associations. One of the most invasive, inaccurate, and privacy-conscious biometrics in use today is FRT. "Two prominent biometric metrics to show the identifying power are False Rejection Rate (FRR) and False Acceptance Rate." In other words, the results of applying facial recognition algorithms to photographs and videos that people may be accurate or deceptive in terms of acceptance or rejection. Hundreds of people are still misunderstood despite an improvement in facial recognition accuracy. When estimating and analyzing error rates, care must be used considering certain groups comprising individuals "may be more likely to be wrongly match others." States must also take steps to stop the infringement of other rights, including those in cyberspace. For example, the state must intervene to protect residents against abuse by both state personnel and other individuals. It is important to keep in mind how important non-state actors are and how they relate to the state. If the state took part, attribution may be shown. Are states still responsible for protecting rights and freedoms when a private actor acts on their behalf, for example, through a concession, public-private partnership, or as a biometric data collector who sells the data to the state which until a legally specified procedure is followed, is one of the most important provisions in the constitution that protects individual freedom.

[14] Al-Bayed, M. H., Haddad, I., Abu-Nasser, B. S., & Abu-Naser, S. S. (2025). Surveillance in the Age of AI: Navigating Ethical Boundaries and Human Rights.

[15] Buolamwini, J. (2024). *Unmasking AI: My mission to protect what is human in a world of machines*. Random House.

[16] Gregory, S. (2019). Cameras everywhere revisited: How digital technologies and social media aid and inhibit human rights documentation and advocacy. *Journal of Human Rights Practice*, *11*(2), 373-392.

iii. **Earlier Judicial Developments -** Previously the Puttaswamy verdict, was not specifically recognized. In Kharak Singh v. State of Uttar Pradesh (1963)[17], Supreme Court discussed police monitoring techniques, but it did not fully recognize privacy as a basic right. Subsequently, the Puttaswamy decision reversed earlier rulings and established privacy as a fundamental constitutional. International initiatives to control AI have already begun. In May 2019, the OECD established its AI standards. Accountability, robust security and safety, human-centered values and justice, sustainable development and well-being, inclusive growth, and transparency and explainability are the five complementing values-based standards for innovative and trustworthy AI. The widespread use of AI, including FRT as an AI-enhanced technology, should be in line with the principles of democracy, human rights, and the rule of law, according to these criteria.

iv. **Legislative Evelution-** India has implemented regulations on digital governance to regulate 2023[18] aims to protect people's personal information and ensure responsible data processing. The opponents argue that the bill's broad exclusions for government entities would permit espionage without enough oversight. Therefore, the legal framework governing AI surveillance is still deficient even in the presence of constitutional protections[19]. People all through the country have simultaneously embraced AI-driven technologies without fully comprehending their implications for data security, privacy, and protection. When surveillance technologies, like biometric travel systems like DigiYatra, are marketed as seamless, time-saving breakthroughs rather than monitoring mechanisms, it is important to think about whether citizens can really be held accountable for a lack of awareness. In this blog post, we go over AI-driven surveillance technologies that have emerged or gained traction in 2025 and look at whether there is a solid legal basis for deploying or expanding such technologies in a way that is necessary, acceptable, and legal. The urge to uphold human rights and democratic standards is what makes the rule of law so important. Most significantly, social justice, equity, and sufficient legal remedies depend on the legal ideas derived from the rule of law—legal stability, legality, and clarity. In June 2019, the G20 approved the rules for responsible stewardship of AI. Throughout the life of AI systems, the G20 promised to protect democratic values, human rights, and the rule of law. These ideas are essential for creating legislation related to FRT in particular and AI in general.

There are some additional Provisions and Statutory Sections involved:

[17] Milanovic, M. (2015). Human rights treaties and foreign surveillance: Privacy in the digital age. *Harv. Int'l LJ*, *56*, 81.

[18] Feldstein, S. (2019). *The road to digital unfreedom: How artificial intelligence is reshaping repression*. *Journal of Democracy, 30*(1), 40–52.

[19] Metcalf, T. R., & Metcalf, B. D. (2012). *A concise history of modern India* (3rd ed.). Cambridge: Cambridge University Press.

- **CONSTITUTION OF INDIA**
  a. **Article 14 – Right to Equality -** under the law. AI surveillance systems may violate Article 14 if algorithmic bias leads to the discriminatory targeting of particular communities.
  b. **Article19(1)(a) – Freedom of Speech and Expression -** People may be discouraged from demonstrating or expressing their discontent if there is constant surveillance.
  c. Article 19(1)(b) – Right to Assemble Peacefully
  d. Article 19(1)(c) – Freedom of Association
  e. Article 21 – Right to Life and Personal Liberty
- **RELEVANT STATUTORY PROVISIONS**

Information Technology Act, 2000:

a. Section 69 - Authorizes the federal or state governments to monitor, intercept, or decrypt data in order to maintain public order, security, or sovereignty.
b. Section 69A - Gives the power to limit public access to online information for reasons pertaining to national security or public order**.**
c. **Section 72A -** Criminalizes the sharing of personal information without authorization.

- **Digital Personal Data Protection Act, 2023**

a. Section 4 – Lawful Processing of Personal Data - Only with agreement and for justifiable causes may personal data be handled.
b. Section 6 – Consent of data Principal
c. Section 8 – Duties of data Fiduciaries
d. Section17 – Exemptions for Government Agencies - Gives certain exceptions to state agencies, raising concerns about potential misuse of observation power.

IV. Legislative Framework Related To Surveillance - The Constitution guarantees liberty and privacy, but many legislative regulations also regulate data collection and surveillance. One important piece of law that allows the government to monitor or intercept digital communications under certain circumstances is the Information Technology Act of 2000. Under Section 69, the government may keep an eye on, intercept, or decrypt information for the purpose of maintaining national security[20] or public order. Section 69A allows authorities to ban online content that jeopardizes security or sovereignty. Despite the fact that these regulations are intended to protect national interests, some argue that they may permit disproportionate surveillance if strong control measures are not in place. Another new law is the Digital Personal Data Protection Act of 2023[21].

[20] Coeckelbergh, M. (2024). *Why AI undermines democracy and what to do about it*. John Wiley & Sons.
[21] Walsh, P. F., & Miller, S. (2016). Rethinking 'Five Eyes' security intelligence collection policies and practice post Snowden. *Intelligence and National Security*, *31*(3), 345-368.

Volume 44, March 2026 ISSN 2581-5504

V. **Constitutional Challenges in the age of AI Surveillance -** Constitutional law now faces additional challenges due to artificial intelligence. When surveillance technologies were much less advanced, traditional legal frameworks were developed. By collecting and analyzing data on an unprecedented scale, AI surveillance technologies allow authorities to continuously watch large populations. This raises important questions about the limits of state authority, protecting individual privacy, and finding a balance between security and liberty[22]**.** There may be an increasing necessity for courts to interpret constitutional principles in light of technological developments. A concern for modern constitutional law is ensuring that technology advancement does not jeopardize the fundamental rights guaranteed by the Constitution.

VI. PROBLEM AND REASONS: CHALLENGES OF AI SURVEILLANCE

AI-powered surveillance is turning public spaces into digital panopticons. Automated monitoring, behavioral analytics, and facial recognition technologies are being used for surveillance in 75 of the 176 countries. The rapid and sometimes unchecked use of this technology poses grave concerns to fundamental human rights since it is a "double-edged sword[23]" that prioritizes security over privacy and dignity. Numerous federal and state rules and regulations control the use of the aforementioned surveillance technology.

Outlines minimal conditions government follow, will be primary focus of this examination, but some of this legislation will be referenced below. Seizures of "persons, houses, papers, and effects" are prohibited under the Fourth Amendment, which also requires warrants to be seized. Techno-Solutionism in Governance: Driven by efficiency, governments employ AI to monitor public order, security, and welfare, often prioritizing "smart" control over fundamental rights. Cost-Effectiveness for States: AI surveillance is less expensive than traditional, human-intensive policing, allowing states to monitor broad populations with less resources. "Surveillance Capitalism" and Data Mining: Businesses gather massive, non-consensual datasets to train AI, often repurposing public data (like social media photos) for surveillance, seeing people as "disembodied data." For instance, when AI is used in video data analytics, a straightforward command such as "detect women in pink saree" could return the results of every woman in the region where the software is used who is wearing pink sarees. However, broad surveillance is made possible by the employment of FRT systems without explicit legal authorization, necessity judgments, or proportionality constraints. There is now no structure in place to limit the State's widespread use of such unwanted technology, nor are there any ways to put checks and balances in place. There are concerns about the transparency and accountability of surveillance methods due to government organizations' unrestricted and unregulated use of facial recognition technologies. For instance, when AI is used in video data

[22] Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, *4*, 100005.
[23] Keay, J. (2000). *India: A history*. New York: Grove Press.

analytics, a straightforward command such as "detect women in pink saree" could return the results of every woman in the region where the software is used who is wearing pink sarees. However, broad surveillance is made possible by the employment of FRT systems without explicit legal authorization, necessity judgments, or proportionality constraints. There is now no structure in place to limit the State's widespread use of such unwanted technology, nor are there any ways to put checks and balances in place. There are concerns about the transparency and accountability of surveillance methods due to government organizations' unrestricted and unregulated use of facial recognition technologies. The use of this word violates the rights to nondiscrimination, equality, and privacy. Since there was no clear guidance on how and where the technology may be used and who might be placed on a watchlist, a data protection impact assessment was inadequate and did not comply with the Data Protection Act 2018 Pt 3 s.64(3) (see footnote 29). Because the police had not taken reasonable steps to investigate whether the technology had a racial or gender bias, as required by the public sector fairness obligation, the Court also decided that there are fundamental deficiencies in the legal framework regulating the use of FRT. There have also been regional initiatives. For example, the European Union has discussed in great detail how AI will impact general legal ideas and the legislation. Neither a comparative study nor an exploration of the European framework are the goals of this research. Rather, the objective is to draw attention to these regional initiatives, which might provide valuable insights into the development of global legislation, and to show how important it is for countries to try to regulate the usage of AI-enhanced technologies. For example, the GDPR, which was approved in 2016, applies to AI at the European level for the same reason as well as for limitations, such as ban.

i. **Threat to Privacy** - AI surveillance systems collect vast quantities of personal data, including biometric identifiers, facial photos, location data, and behavioral patterns. People's private lives might be significantly violated[24] by such data collection. When legal safeguards are ambiguous, surveillance systems may operate with little oversight. Scholars warn that widespread use of facial recognition technology might lead to violations of Article 21 and mass surveillance.
ii. **Algorithmic Bias and Discrimination –** AI systems are based on algorithms created on large datasets. If these datasets contain biases, the resulting algorithms may provide discriminatory outcomes. It has been demonstrated that some racial or ethnic groups make more mistakes while utilizing facial recognition technology. In a multicultural country like India, such mistakes might disproportionately affect the poor**.**
iii. **Lack of Transparency and Accountability -** Numerous AI systems operate as "black box" technologies, meaning that their decision-making processes are hidden. Individuals who are the target of surveillance systems may not comprehend how the

[24] Ünver, H. A. (2024). Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights. *Depth Analysis requested by the Subcommittee on Human Rights (DROI) of the European Parliament, Policy Department for External Relations, Directorate-General for External Policies of the Union, PE*, *754*.

algorithm arrived at its conclusion, why they were spotted, or how to challenge the verdict[25]. This lack of transparency threatens rule law.

iv. **Chilling Effort on Freedom -** Excessive surveillance may discourage citizens from exercising their fundamental rights. If people believe they are being watched, they may not participate in protests, express their dissatisfaction, or become active in politics. Such chilling adverse effects pose a danger to political participation and freedom of expression.

v. Risk of Surveillance State - If surveillance technologies spread uncontrolled, societies may gradually transform into surveillance regimes, where rulers constantly monitor individuals. Experts warn that if AI spying is used without adequate safeguards, intrusive methods of surveillance that are incompatible[26] with democratic values may become commonplace. The creation of a surveillance state, in which governments employ state-of-the-art technology to continually watch citizens, is one of the most grave worries regarding AI espionage. Authorities are able to gather and analyze enormous volumes of data from CCTV cameras, phones, biometric databases, and internet activity because of AI technology. Initiatives like India's vast biometric identification schemes and face recognition technologies raise concerns about widespread surveillance[27].

VII. ANALYSIS: THE IMPACT ON SOCIETY AND LAW

The "Black Box" Problem: AI systems violate procedural justice and fairness criteria since they are opaque and often hide the decision-making process.A culture of mistrust is fostered via lateral surveillance (community monitors), which is comparable to mass surveillance systems in totalitarian countries. False Positives & Inaccuracy: AI, especially FRT, has high error rates (up to 98%), which can lead to incorrect arrests, particularly of people of color. The "Datafication" of Humans: The transformation of human identity into quantifiable data, which may be used by political or corporate entities to manipulate individuals, enables predictive behavior. Urgent Need for "Red Lines": Advocacy groups like European Digital Rights are pushing for a ban on high-risk AI, especially face recognition in public spaces, in order to establish a "red line" against the most harmful uses. The European Parliament adopted final amendments to the Act on 14 June 2023 and it was approved on 8 December 2023. The Act on Artificial Intelligence includes the objective of ensuring that "AI systems… are safe and respect existing law on fundamental rights and Union values; ensure[ing] legal certainty.

[25] J. S. Marcus, N. Poitiers, M. De Ridder and P. Weil, 'The decoupling of Russia: high-tech goods and components', Bruegel, 28 March 2022.
[26] J. Jones, 'Deepfake of purported Putin declaring martial law fits disturbing pattern', MSNBC, 7 June 2023
[27] S. Petrella, C. Miller, and B. Cooper, 'Russia's artificial intelligence strategy: the role of state-owned firms', Orbis, Vol 65, No 1, 2021, pp. 75-100

Volume 44, March 2026 ISSN 2581-5504

VIII. LEGAL ANALYSIS OF AI SURVEILLANCE

If surveillance technologies continue to spread uncontrolled, society may eventually turn into a surveillance regime in which the ruling class constantly monitors its citizens. Experts warn that if AI espionage is used without adequate protections, invasive surveillance methods that are incompatible with democratic values may become common.

- **Legality -** Legal analysis of AI surveillance reveals a growing conflict between state security goals and constitutional protections. By 2026, arguments regarding monitoring in the international legal arena have been superseded by active enforcement of rights-based frameworks[28]. For surveillance to be constitutional, it must be authorized by law. As of right now, India lacks a comprehensive law that specifically regulates AI surveillance technologies.
- **Necessity -** State surveillance must serve a legitimate goal, such as maintaining national security or deterring crime. Widespread monitoring without a clear justification[29] might not satisfy the necessity requirement, despite the legitimacy of these objectives.
- **Proportionality -** The proportionality test states that surveillance techniques must not be out of proportion to the intended outcome. Widespread facial recognition technology that tracks[30] millions of individuals might undermine this notion.
- **Data Protection Concerns -** The Digital Personal Data Protection Act, which attempts to regulate data processing, mostly excludes government organizations. Critics claim that these exclusions might weaken privacy protections.

IX. CASE LAWS

- **Justice K.S. Puttaswamy v. Union of India(2017)[31]**

In decision, the was declared. The Supreme council decided that privacy is necessary for life and liberty in accordance with Article 21. A nine-judge ruling, the judgment states that includes both informational privacy and protection against governmental surveillance. The Court created the proportionality, necessity, and legality standards for invasions of privacy.

- **Justice K.S. Puttaswamy (Aadhaar) v. Union of India(2018)[32]**

The Court maintained the Aadhaar system while placing limitations in order to protect privacy and ensure the proper use of biometric data. The Supreme Court upheld privacy rights while maintaining the validity of the Aadhaar scheme. The Court emphasized that biometric data

[28] Custers, B. (2022). New digital rights: Imagining additional fundamental rights for the digital era. *Computer Law & Security Review*, *44*, 105636.
[29] Custers, B. (2022). New digital rights: Imagining additional fundamental rights for the digital era. *Computer Law & Security Review*, *44*, 105636.
[30] Pantserev, K. A. (2020). The malicious use of AI-based deepfake technology as the new threat to psychological security and political stability. In *Cyber defence in the age of AI, smart societies and augmented humanity* (pp. 37-55). Cham: Springer International Publishing.
[31] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (Supreme Court of India).
[32] Justice K.S. Puttaswamy (Aadhaar) v. Union of India(2018)1 SCC 1 (Supreme Court of India).

collection must follow proportionality and be used only for permitted purposes. Despite its fragmentation and ambiguity, the AI Act is a first regional step—the first in the world—for a regulatory framework on AI with the aim of protecting the principles of basic rights, the rule of law, democracy, nondiscrimination, data protection, and human dignity. It provides a framework for the restricted use of facial recognition together with safeguards for the ideas of legality and legal certainty. Nonetheless, a more comprehensive legal analysis and a more lucid description of biometric data security that went beyond internal market concerns might have been offered. For face recognition and other unacceptable risk AI technology, a general statement such as "use of 'real time' remote biometric identification systems in publicly accessible spaces" is unsuitable.

- **Selvi v. State of Karnataka(2010)[33]**

The Court determined one's right to mental privacy and personal freedom is violated when techniques like marco-analysis are used against their permission. The Court claims that employing techniques like as brain mapping, polygraph tests, and narco-analysis without a person's consent violates their Article 21 right to mental privacy and personal freedom. The decision maintained the principle that individuals cannot be subjected to intrusive governmental actions without their consent.

- **Kharak Singh v. State of Uttar Pradesh(1963)[34]**

This ruling not only addressed police snooping but also laid the foundation for privacy jurisprudence. Police monitoring techniques including overnight domiciliary inspections were examined by the Supreme Court. The Court ruled that such surveillance violated the guarantee of personal liberty found in Article 21. Despite the majority's limited acknowledgment of privacy as a fundamental right, Justice Subba Rao's dissent later influenced the development of privacy law.

X. SUGGESTIONS

- **Comprehensive AI Regulation** - India should enact a special AI legislation law governing surveillance technology. Enforce "Ban on Highly Risky AI" by establishing clear limits on the use of AI for pervasive oversight, including and social scoring systems.Enact Strict Data Protection regulations: should include more stringent consent requirements, deliberate restrictions, and fewer exemptions for government entities. Mandatory AI Impact Assessments (AIA): Public and private entities should be obliged to conduct AI Impact Assessments in order to evaluate potential human rights abuses prior to deploying AI in sensitive domains like employment, law enforcement, or healthcare. Establish Independent Oversight committees: Independent,

[33] Selvi v. State of Karnataka(2010)7 SCC 263 (Supreme Court of India).
[34] Kharak Singh v. State of Uttar Pradesh, AIR 1963SC 1295(Supreme Court of India)

multidisciplinary, and multi-stakeholder committees[35] should be formed to handle citizen complaints and carry out quarterly audits of surveillance systems.

- **Strong Judicial Oversight** - Court clearance is required for surveillance systems in order to prevent abuse. Durable Proportionality Test: As emphasized in cases like Puttaswamy v. Union of India, conduct a rigorous proportionality test (legality, necessity, and appropriateness) before to employing surveillance tactics.
- Accountability for Misuse: Create strong accountability frameworks to hold developers and users (governments or employers) responsible for harm caused by algorithmic errors or inappropriate use of surveillance.
- **Transparency and Accountability** - Authorities employing AI systems must reveal the purpose of surveillance, data retention policies, and algorithmic decision-making processes. "Privacy-by-Design" and "Contestability-by-Design": Incorporate ethical principles into the technological design process, ensuring that systems are auditable, traceable, and accessible to human intervention.
- **Bias Mitigation & Transparency:** Statistics and algorithmic accuracy rates should be made public in order to prevent AI from exacerbating historical inequalities, especially for disadvantaged groups.Data Minimization: Maintain the notion that the quantity of surveillance data gathered should s absolutely necessary for a legitimate[36], specific.
- **Data protection Safeguards** - Personal information should only be collected and securely stored when absolutely necessary. Global Standards for AI Ethics: A consistent, rights-based approach to AI governance should be created in order to prevent "regulatory arbitrage," in which companies migrate to nations with laxer legislation. Strong export regulations should be implemented for surveillance technology that poses a major threat to human rights.
- **Independent Oversight Bodies** - Independent regulatory bodies should monitor the use of surveillance technologies.
- **Public Awareness** - When utilizing the internet, people should be informed of their rights and protections. Fund public awareness campaigns that teach individuals how to exercise their rights and how AI will impact their lives to promote AI literacy. Public Participation in Governance: Ensure that citizens and civil society organizations have a say in the laws governing their surveillance.

XI. CONCLUSION

Artificial intelligence surveillance is one of the worst risks to fundamental rights in the digital age. These technologies offer useful tools for governance and crime prevention, but their unchecked expansion might endanger liberty, privacy, and democratic liberties. When privacy

[35] Pantserev, K. A. (2020). The malicious use of AI-based deepfake technology as the new threat to psychological security and political stability. In *Cyber defence in the age of AI, smart societies and augmented humanity* (pp. 37-55). Cham: Springer International Publishing.

[36] Aloisi, A., & De Stefano, V. (2022). Essential jobs, remote work and digital surveillance: Addressing the COVID-19 pandemic panopticon. *International Labour Review*, *161*(2), 289-314.

Volume 44, March 2026 ISSN 2581-5504

was recognized, India's constitutional law experienced a radical transformation. But the rapid AI that may not be adequately addressed by existing laws. The risk of widespread monitoring and possible misuse of personal data is increased by the lack of comprehensive regulation governing AI surveillance. Such methods may breach in the absence of explicit legislative protections.

India must implement a strong legislative framework that guarantees accountability, transparency, and the appropriate use of surveillance technology in order to strike a balance between technological progress and human freedoms. To stop abuse, independent regulatory organizations, data security measures, and judicial control are crucial. In the end, the problem is constitutional rather than just technological. A democratic society must make sure that artificial intelligence advances citizens' interests rather than jeopardizing their rights. The capacity to balance the growth of technology with the preservation of fundamental liberties will determine the future of digital governance in India. For scholars doing more study on the subject, this page will be a very useful resource and starting point.

Specifically, it made the connection between vulnerability and the legal challenges surrounding AI, a conversation that is desperately required on many levels. It provided a comprehensive summary of the many legal problems, gaps, difficulties, and impacted human rights concepts related to AI. It also described three essential actions that must be done to protect the most vulnerable members of society. Many of the subjects being studied have significant socioeconomic and human rights implications.

BIBLIOGRAPHY

- Abernathy, M. Glenn Civil Liberties under the Constitution. New York: Harper & Row, Third Edition, (1977).
- Allen, Anita. Why Privacy Isn’t Everything: Feminist Reflections on Personal Accountability. Lanham, MD: Rowman & Littlefield Publishers, (2003).
- Allen, Anita. Uneasy Access: Privacy for Women in a Free Society. Totowa, NJ: Rowman and Littlefield, (1988).
- Altman, I. The Environment and Social Behavior: Privacy Personal Space Territory Crowding, (1975). Austin, M.M & Vidal-Naquet, P. Economic & Social History of Ancient Greece. California: University of California Press, First Edition, (1973).
- Bainbridge, David. Introduction to Information Technology Law. Harlow: Pearson/Longman, Sixth Edition, (2007).