 DOI: *https://doij.org/10.10000/IJLSI.112673*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 4

2025

Watching the Watchers: AI Surveillance, Privacy, and India's Constitutional Vacuum in the Shadow of the EU AI Act

NIHARIKA PURI[1]

ABSTRACT

This paper examines gaps in India's regulation of AI driven surveillance related to privacy and civil liberties. Laws have been passed the pace that AI surveillance is being adopted in corporate workplaces and government facial recognition systems. The Supreme Court's K.S. Puttaswamy (2017) ruling on the right to privacy as a fundamental right does not mean however, that India has specific regulations nor effective enforcement of AI surveillance. Corporate surveillance is virtually unregulated and government surveillance is too easily lead astray with tools like facial recognition systems.

The paper compares India's approach to those of the U.S., EU and China, commenting on the EU's rights focused AI Act, the U.S.'s stop gap measures and China's state driven approach. The paper advocates for India to creating a coherent legal framework between technological innovation and protection of fundamental rights, and implements the globalization precedents and strengthened accountability mechanisms to prevent enhanced AI surveillance.

I. INTRODUCTION

AI's quick growth has turned surveillance into a strong tool for governments and businesses to control things. Technologies like face scanning guessing what might happen, and digging through data in real-time are now used more and more in public and private areas in India. Police use face scanning to watch protests, while bosses use AI programs to keep an eye on workers. These practices bring up big questions about privacy, who's responsible, and people's rights.

India's drive to create a wide-reaching ***Automated Facial Recognition System (AFRS)***, put forward by the National Crime Records Bureau, points to a bold step towards centralized surveillance infrastructure. At the same time, businesses use AI-powered tools at work with little to no oversight. Even as these projects grow bigger, India doesn't have a complete set of

[1] Author is a Student at Symbiosis Law School, Pune, India.

 [ISSN 2581-9453]

laws to control AI surveillance.[2] Current rules like the Information Technology Act, 2000 and data rules for different sectors are old or too scattered to deal with new risks.

This paper looks at the main legal and policy hurdles around AI surveillance in India checking how both the government and companies use it. It asks if today's laws can ensure people are held responsible and rights are protected. The paper also looks at rules from around the world to suggest practical changes that fit India's democratic and tech landscape.

LITERATURE REVIEW

SOURCE	FINDINGS/INSIGHTS	IMPLICATIONS FOR INDIAN LEGAL FRAMEWORK	INTERRELATION WITH TOPIC	RECOMMENDATIONS/FUTURE DIRECTIONS
Divij Joshi, "AI governance in India – law, policy, and political economy" (2024)[3]	Examining the place of AI governance within the Indian law and political economy, Joshi outlines the areas where law is not well developed and where a general AI policy is urgently needed in India.	India's current regulatory framework on AI does not provide a systematic and holistic governance framework that could result in the risks of privacy, security and the civil liberties.	This work directly addresses the role of AI governance within India's legal system, focusing on political economy, regulation, and societal impact.	To enable and ensure responsible development of AI in India, a national AI strategy with legal, industry and ethical frameworks should be created in India.
Vijay Prakash v. Union of India (2009)[4]	The critical factor in this case is guarding civil liberties as they relate to the technological	This ruling emphasizes the fact that India's laws need to strike the right	This case touches upon surveillance laws and AI governance, as it deals with the	Legal protections for privacy in the digital age are now being carved out in a more clear cut manner, need

[2] *Jhalak Kakkar et al., The Surveillance Law Landscape in India and the Impact of Puttaswamy, CCG Report (July 2023),* https://papers.ssrn.com.
[3] ***Divij Joshi**, AI Governance in India – Law, Policy and Political Economy, COMM. RES. & PRAC. (2024),* https://discovery.ucl.ac.uk.
[4] *Vijay Prakash v. Union of India, (2009) SCC OnLine Del 2189 (India).*

	advancement in the age of digital age.	balance between privacy rights and technological progress, especially with respect to surveillance technologies.	protection of privacy when the new technologies are the ones of AI.	to be integrated in to the governance of AI, and the courts need to have oversight.
China's AI Surveillance Model and PIPL, 2021[5]	AI surveillance is used heavily in China's version of this surveillance model and it is still a major point of conversation in global AI ethics and governance. The Personal Information Protection Law (PIPL) focuses on privacy in AI applications.	Given AI's growing influence, India needs to adopt similar data privacy laws to stop AI surveillance from being unchecked.	This source provides a comparative view to AI surveillance: other countries, especially China, are regulating AI technologies and surveillance.	India should consider implementing a similar legal framework for AI surveillance, focusing on both privacy protection and transparency in AI applications.
Lukmaan IAS, "The Legal Gaps in India's Unregulated AI"[6]	This article identifies gaps in the existing legal frameworks governing AI in India, pointing out the lack of	The absence of regulations on AI governance leads to potential misuse and risks related to data privacy,	Directly links to AI governance by emphasizing the critical need for a regulatory framework to manage the ethical,	India must pass AI-specific laws that address ethical concerns, data protection, and AI accountability, with provisions for regular

[5] *Personal Information Protection Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) (China), translated in* https://www.chinalawtranslate.com/en/pipl/.

[6] ***Lukmaan IAS**, The Legal Gaps in India's Unregulated AI Surveillance, LUKMAAN IAS BLOG (Dec. 2024),* https://blog.lukmaanias.com.

	comprehensive regulations and standards for AI deployment.	discrimination, and lack of accountability.	legal, and social implications of AI technologies.	reviews and updates to keep pace with technological advances.
Aparna Chandra & Vrinda Bhandari, "Understanding Surveillance Law in India post-Puttaswamy" (NUJS L. Rev. 2019)[7]	Post Puttaswamy jurisprudence on surveillance and privacy rights in India is analysed by the article. It shows how surveillance technologies require legal frameworks to be developed.	Indian legal frameworks need to develop for AI surveillance tools so that they do not encroach upon the right to privacy and violate the right to mass surveillance without safeguards.	It explores the laws on privacy and surveillance in depth and how they connect with new technologies to put forth an analysis on how AI Governance mesh with new technologies based on the intersection of surveillance laws.	India should come up with specific AI surveillance regulations to protect privacy rights while allowing the legitimate use of AI technologies without violating civil liberties.
G. Akhtar & A. Choudhary, "Digital Surveillance and Civil Liberties in India" (2021)[8]	This work critiques India's digital surveillance approach and how digital tools such as AI are being used for surveillance purposes when there are no safeguards in place.	In AI, there is a requirement for a legal overhaul to protect civil liberties from excessive surveillance. Since the regulation of AI surveillance is an area that India's legal framework lacks, it has to	It connects to AI governance as well as things to do with AI technologies and violation of privacy in India's digital landscape.	To strengthen civil liberties protection in India, it is important to put in place specific safeguards for AI driven surveillance, make AI based surveillance practices transparent and accountable.

[7] ***Aparna Chandra & Vrinda Bhandari***, *Understanding Surveillance Law in India Post-Puttaswamy, 12 NUJS L. REV. 103 (2019).*
[8] ***G. Akhtar & A. Choudhary***, *Digital Surveillance and Civil Liberties in India, GIGA FOCUS ASIA No. 6 (2021),* https://www.giga-hamburg.de.

		fill the gaps.		

II. RESEARCH QUESTIONS

1. **What is the state of India's current AI surveillance legal framework when it comes to corporations and the Government, and what are the gaps or challenges?**

This question asks for how Indian laws and regulations (including constitutional principles, statutes and policies) relate to AI driven surveillance and what is lacking or lacking in the frameworks.

2. **Where and how are AI surveillance conducted by private companies and state agencies in India affecting privacy and civil liberties, and which resulting concerns exist regarding corporate overreach and government abuse?**

The question asks about the real world implications of AI surveillance in terms of privacy infringements, violation of rights, misuse of surveillance powers, and so on, in the Indian context. It calls for deconstructing typical examples of corporate surveillance (workplace monitoring, data collection), governmental surveillance (mass facial recognition, prediction policing), in the name of evaluating their social effects.

3. **Global jurisdictions (amongst other such as US, EU, or China) have what approach on AI driven surveillance regulation, and what comparative insights or lessons for India?**

This question explores how others have grappled with AI surveillance through the lens of legislation, regulations, and even judicial oversight, in order to context the Indian state's situation within the global field and to point to life lessons or warning tales that can inform the creation of Indian law and policy.

4. **What is lacking in the procedural safeguards in India's AI surveillance ecosystem and how does this violate India's constitutional guarantee of due process and procedural dignity: and what reforms are needed to reintroduce a democratic accountability in this space.**

This question looks at how the lack of safeguards in AI surveillance goes against constitutional due process and procedural dignity. It focuses on issues like transparency, the ability to challenge decisions, and ways to fix mistakes.

III. CRITICAL ANALYSIS: AI SURVEILLANCE IN INDIA

Corporate Use of AI Surveillance in India

AI surveillance tools have become increasingly popular in India, especially in the hands of private corporations to improve security, productivity and efficiency. However, there are no particular laws against corporate surveillance and this is very serious legal and ethical issue. After COVID, AI based CCTV, biometric attendance and employee monitoring software have become the norm.

Surveillance is justified by corporations as a necessity for safety and performance. For example, facial recognition at malls, remote worker monitoring, biometric attendance systems are the examples. However, these are largely unregulated, and therefore, have key concerns:

1. **Lack of Legal Framework**

There are no specific laws governing the issue of workplace surveillance in India. General principles such as contract law or the right to privacy may protect to some extent, but there are no clear rules of surveillance. Very often employees sign consent forms without knowing what they are signing or having a true choice.

2. **Lack of Transparency**

Companies have no legal mandates to disclose what they collect or use, beyond certain pages only. For instance, facial recognition systems can also gather biometric data (such as facial recognition systems) without user consent or even their knowledge and thus render transparency and accountability.

3. **Data Use and Consent**

The Digital Personal Data Protection Act (DPDPA) 2023 has a provision of lawful use of data but does not specifically mention workplace or consumer surveillance.[9] It does not also have clear consent mechanisms and privacy rights are unprotected.

4. **Ethical Concerns**

Because AI tools can take action based on behaviour, productivity, or habits, they may profile people so that they are evaluated unfairly or undeservedly. These systems lack oversight, and hardly ever are errors or biases challenged, and if they have been affected, they have no recourse.

[9] *Digital Personal Data Protection Act, 2023, India Code (2023).*

5. Corporate-Government Data Sharing

There is a risk of misuse in the overlap between corporate and state surveillance. Private firms collect the data and can share it with government agencies, but there are no rules that govern such exchanges and heighten privacy threats.

Corporate AI surveillance in India is largely unregulated, prone to privacy breach, unfair outcome as well as lacking accountability. We urgently need specific legislation on how AI is and should be used, transparent, consented and redressed.

Government AI Surveillance and Overreach in India

AI surveillance technologies have been fast deployed on the governmental side in India due to security concerns and the need to be more efficient in governance. Yet, such technologies as facial recognition systems, big data analytics, and predictive policing have expanded to great concern about privacy and human rights.

1. Facial Recognition and Surveillance Systems

The NCRB has launched the Automated Facial Recognition System (AFRS) which is a central facial image database to help law enforcement. Despite this, public use of FRT (e.g., CAA, farmers' protests) without clear legal periphery has led to profiling and suppression of dissent; threatening free speech and political participation.

2. Accuracy and Bias Issues

Indian authorities' use of FRT, however, has been poor; error rates are reportedly as high as 98%. They also cause the tools to misidentify individuals, which poses a threat to due process. In addition, they are more prone to error for women and darker skinned people, which puts marginalized communities at a higher risk.

3. Mass Surveillance and Data Privacy

It is also used for mass data collection beyond policing. The 'Social Registry' that we are proposing here is an attempt to incorporate Aadhaar and welfare schemes data for the purpose of service delivery to targeted sections of the population. This however creates problems regarding privacy, data misuse and the establishment of a surveillance state without any valid precautions.

4. Predictive Policing and Algorithmic Bias

Data from social media, crime stats, local even all of these are being used to make predications on crimes using the AI tools. Such systems without proper oversight can reinforce existing

biases in unfair ways and cause more over policing and discrimination intentionally without proper oversight.

5. Lack of Oversight and Regulation

Because AI surveillance is absent of regulatory controls, it removes the distinction between lawful and unlawful surveillance (e.g., wiretaps). Such activities have no independent authority—such as a privacy regulator—to oversee this. The lack of accountability removes the citizens from unchecked state surveillance.

6. Constitutional and Human Rights Concerns

The Supreme Court in Puttaswamy v. UOI, stated privacy as a fundamental right. However, AI surveillance paves the way for inappropriately applying the principles of legality, necessity, and proportionality, thereby making them unconstitutional for lack of enabling legislation.

The Puttaswamy judgment affirms that privacy exists, but it is devoid of procedural pathways — how the citizens can know, object, appeal or correct the use of AI surveillance.

IV. Comparative Analysis of AI Surveillance Regulations – USA, EU, and China

ASPECT	UNITED STATES	EUROPEAN UNION	CHINA
Overall Approach	Fragmented, reactive, with minimal federal oversight. Strong civil society role.	Precautionary, rights-based, and comprehensive regulation. Strong legal safeguards.	Surveillance-heavy, centralized state control. Legal reforms more focused on controlling corporations than the state.
Legal Basis	Sector-specific laws (e.g., ECPA, CCPA), constitutional principles (esp. Fourth Amendment).	GDPR (2018), Charter of Fundamental Rights (Art. 7 & 8), EU AI Act (2024).[10]	Cybersecurity Law (2017), Data Security Law (2021), Personal Information Protection Law

[10] *Charter of Fundamental Rights of the European Union, 2012 O.J. (C 326) 391.*

			(PIPL, 2021).[11]
AI-Specific Regulation	No comprehensive federal AI law. Some city/state bans on facial recognition.	EU AI Act (2024): Risk-tiered approach; bans, high-risk obligations, oversight bodies.	No specific AI law yet, but AI integrated into surveillance systems and guided by security laws.
Use of Facial Recognition	Used by federal agencies (FBI, DHS); local bans in cities like SF and Boston; reversals in some states due to crime concerns.	Generally banned in public spaces for law enforcement (with narrow exceptions). Emphasis on necessity, proportionality, and human oversight.	Widely deployed for policing, urban management, and social control. Emotion, gait, and biometric recognition used extensively.
Oversight Mechanisms	Limited federal oversight. Internal agency policies. Public pressure and lawsuits (e.g., Clearview AI litigation under BIPA).	Independent regulators like Data Protection Authorities. EU AI Office will oversee AI Act. Strong enforcement under GDPR.	No independent external oversight over state surveillance. Internal CCP mechanisms control compliance. Public interest is not the priority.
Redress Mechanisms	Tort law, class actions (e.g., under Illinois' BIPA). Civil society litigation (ACLU lawsuits).	Data subject rights: access, correction, erasure, objection. Strong enforcement via DPA fines.	Individual rights exist under PIPL but are not enforceable against state actions; no real recourse against government misuse.

[11] *Personal Information Protection Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) (China),* http://www.npc.gov.cn/englishnpc/c23934/202112/89fb32838a814ffcbdb29b66e45370e5.shtml.

Public-Private Balance	Corporations have wide leeway unless state law applies. Tech firms hold immense surveillance data.	Balanced: Both public and private sector regulated under GDPR and AI Act. Clear accountability mechanisms.	Private actors are increasingly regulated (PIPL), but state retains unchecked surveillance authority.
Key Recent Developments	Local bans/reversals on facial recognition. - Lawsuits against private actors (e.g., Clearview). - NIST studies facial recognition bias. - Push for federal regulation gaining ground.	AI Act passed (2024). - Ban on real-time biometric ID in public places. - Heavy fines for non-compliance. - Sandboxes for AI innovation.	Nationwide surveillance rollout. - Uyghur surveillance case raised global concern. - PIPL enacted but state exceptions remain dominant.
Civil Liberties Protections	Fourth Amendment protections, but courts slow to adapt to new tech. No absolute ban on mass surveillance.	Strong civil rights focus. Surveillance only if necessary, proportional, and rights-respecting.	Minimal focus. State interest in control overrides individual rights. Surveillance justified by "stability maintenance."
Bias, Transparency, and Accuracy Audits	NIST conducts facial recognition bias tests. No mandated audits. Voluntary for firms.	Mandatory bias/accuracy testing for high-risk AI. Public registers and conformity assessments required.	No public audit mechanisms. Accuracy favoured only if it improves state objectives (e.g., criminal identification).
Regulatory Philosophy	Innovation first, regulate later. Market-driven with some	Precautionary principle. Regulate in advance, even at the	Control-driven. Innovation harnessed to enhance state

	reactive protections.	cost of delaying tech.	surveillance and social control.
Lessons for India	Avoid waiting for harm to regulate. - Introduce accuracy/bias audits. - Consider state-level innovation in absence of central law. - Build civil society capacity.	Pre-classify AI risks. - Ban harmful practices before entrenchment. - Create independent AI oversight. - Ensure rights-based governance with transparency.	Example of overreach: India must avoid unchecked state surveillance. - Avoid vague "national interest" exemptions. - Strong independent oversight and legal remedies needed.

V. CONCLUSION

India's AI surveillance regime in the private and public sphere operates in a legal grey zone as the rules around it are still very loose justifications are rather weak, and there is no oversight. There are serious risks: violating the privacy of individuals, shutting down free speech and democratic participation, computer discrimination, unbridled state power.

In the current state of affairs, there still exist robust legislation, oversight, and safeguards against abuses of power, discrimination, and violations of privacy rights for the individuals. What is pressing is compulsory basic legislation covering AI surveillance, drawing comparative red lines, and safeguarding the rights of individuals. Without such protections at the hands of AI surveillance, India's rapid advancement of AI surveillance could lead to a surveillance state, undermining very much the freedoms and rights of which the democratic framework hopes to protect.

In order to address this, India must urgently:

- Dedicate legislation such as enacted specifying definitions and that purpose is limited and that data minimization is regulated.
- Require public and private actors to perform mandate impact assessments for all high risk AI deployment.
- Introduce transparency requirements, including the public disclosure of accuracy rates, specific uses, disclosure of use of AI tool.

 [ISSN 2581-9453]

- Provision of rights to the individuals; such as notice, access, correction and redress mechanisms.
- Create a binding duty auditor / supervisor authority on ai and digital surveillance.

In essence, integrating AI surveillance in India with constitutional values and international human rights standards is neither merely a question of the regulation; it is also a question of democracy.

We need to move beyond surveillance as a privacy breach, and expose it as a democratic procedural failure.

*****