THE LEGAL AND ETHICAL CHALLENGES OF AI SURVEILLANCE IN INDIA: BALANCING NATIONAL SECURITY AND PRIVACY RIGHTS

Mr. Kumar Jyotish, Lecturer, Himalaya Law College, Chiksi, Paliganj, Patna

ABSTRACT

India's rapid deployment of AI surveillance technology, such as the National Automated Facial Recognition System (NAFRS) and biometric monitoring systems, is conducted without broad statutory authority, resulting in constitutional issues with Article 21 privacy rights. This article looks at how existing AI surveillance tactics breach the three-part criteria of legality, necessity, and proportionality set in Justice K.S. Puttaswamy v. Union of India (2017)[1]. Despite the Digital Personal Data Protection Act of 2023, extensive governmental exemptions expose citizens to unfettered surveillance. Through doctrinal analysis, this study indicates that India's AI surveillance ecosystem lacks necessary procedural safeguards and proportionate deployment criteria, arguing for immediate legislative intervention to ensure democratic accountability.

Keywords: AI Surveillance, Privacy Rights, Article 21, National Security, Facial Recognition Technology, Constitutional Law, Digital Personal Data Protection Act, Biometric Surveillance

[1] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., Civil Appeal No. 4949 of 2012, Supreme Court of India (2017)

INTRODUCTION

The introduction of artificial intelligence ("AI") has irreversibly changed state surveillance in India. From city-wide CCTV networks with facial recognition to predictive-policing platforms analysing vast amounts of personal data, the government's adoption of AI-driven monitoring tactics has intensified in recent years. While technologies like the National Automated Facial Recognition System ("NAFRS") and Aadhaar-linked biometric tracking seem to improve investigative efficiency and national security, they also raise concerns about arbitrary intrusion into the private realm.[2]

Article 21 of the Indian Constitution provides the right to life and personal liberty, which the Supreme Court extended in Justice **K.S. Puttaswamy v. Union of India (2017)**[3] to include informational autonomy and the right to privacy. The Court established a three-part test—legality, need, and proportionality—to assess any state intrusion into private. However, the rapid deployment of AI surveillance typically occurs without explicit legislative support, effective procedural safeguards, or impartial monitoring. In practice, broad exemptions under the Digital Personal Data Protection Act, 2023, and ambiguous powers provided by Section 69 of the Information Technology Act, 2000, have created a legal void that allows for extensive data gathering and processing without rigorous judicial examination.

This article contends that India's current AI surveillance environment fails to meet constitutional requirements. It will first examine the evolution of privacy jurisprudence since Puttaswamy, emphasizing the importance of informational liberty and the need for judicial examination. It will then examine the design and operational modalities of AI surveillance technologies used by state and federal governments, revealing how opaque algorithms and data-fusion methods erode openness. The analysis will emphasize the shortcomings of existing statutes, such as the lack of dedicated AI-surveillance legislation, procedural safeguards, and proportionality standards, and will demonstrate how these gaps allow unfettered government interference.[4]

[2] Ministry of Home Affairs, Government of India, 2023
[3] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., Civil Appeal No. 4949 of 2012, Supreme Court of India (2017)
[4] Narayanan, A. (2024). Transparency, Accountability, and AI Surveillance: India's Legal Gaps and Policy Needs. Indian Law Review, 29(1), 101-123.

Comparative insights from the European Union's General Data Protection Regulation and the AI Act, as well as selected US privacy regulations, will be used to generate recommendations for India's legal reform. These would include the creation of a specialized AI Surveillance Regulation Act, mandated algorithmic effect assessments, independent monitoring organizations, and improved legal redress mechanisms. In the post-Puttaswamy era, India must reconcile its national security goals with the inalienable right to privacy, or AI monitoring will become an unrestrained instrument of state power rather than a tool for transparent governance.[5]

THE CONSTITUTIONAL PRIVACY FRAMEWORK POST-PUTTASWAMY

The evolution of privacy jurisprudence in India indicates a slow but substantial shift from a peripheral common-law protection to a constitutionally guaranteed fundamental right. In **Kharak Singh v. State of Uttar Pradesh (1964)[6],** the Supreme Court tentatively recognized privacy as inherent in human liberty but did not declare it a freestanding fundamental right, instead limiting its protection to the scope of unjustified state activity under Articles 19 and 21. Subsequent rulings, such as **Gobind v. State of Madhya Pradesh (1975**)[7], emphasized private protections against domiciliary intrusion and monitoring, but the Court remained undecided on its constitutional legitimacy.

The important decision in **Justice K.S. Puttaswamy v. Union of India (2017)[8]** established that privacy is inextricably linked to the right to life and personal liberty protected by Article 21 of the Constitution. The nine-judge Constitution Bench ruled that the right to privacy is derived from several provisions—Articles 14, 19, and 21—that represent the Constitution's commitment to individual dignity, autonomy, and self-determination. This ruling overturned earlier reservations and affirmed privacy as a pillar of constitutional democracy.

The Puttaswamy theory is based on a three-part constitutional examination that evaluates any state interference into privacy.

[5] European Commission. (2021). Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Brussels: European Union.
[6] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (1964).
[7] Gobind v State of Madhya Pradesh (AIR 1975 SC 1378, (1975) 2 SCC 148)
[8] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., Civil Appeal No. 4949 of 2012, Supreme Court of India (2017)

1. Legality: Surveillance and data collection must be permitted by clear and precise laws to prevent arbitrary state power. Provisions that are vague or overly broad cannot meet this standard.

2. Restrictions on privacy must serve a legitimate state purpose, such as public order, national security, or crime prevention. The state carries the burden of establishing that the measure is absolutely necessary to attain its goal.

3. Proportionality requires a sensible connection between the methods used and the acceptable goal. Furthermore, the intrusion must be the least restrictive method accessible, with little disruption to private interests.

This tripartite standard is consistent with comparative constitutional norms and serves as the litmus test for analyzing new surveillance tools, such as AI-powered technologies.[9]

Beyond these structural foundations, Puttaswamy acknowledged informational autonomy as an important aspect of privacy, allowing people to manage the acquisition, storage, and dissemination of personal data. Informational autonomy defends against data exploitation by governmental or private actors, and it embodies the idea of data minimization, which states that only data genuinely essential for a valid purpose may be processed. In the post-Puttaswamy period, India's constitutional framework requires strict adherence to these principles. Legislative and administrative measures, particularly in emerging realms like AI surveillance, must demonstrate legality, necessity, and proportionality while maintaining informational autonomy. Failure to meet these conditions makes monitoring tactics unlawful, emphasizing the importance of privacy in India's constitutional structure.[10]

AI SURVEILLANCE LANDSCAPE IN INDIA

India's dedication to improving public safety and national security has resulted in the increasing deployment of AI-powered surveillance technologies. These technologies include facial recognition platforms, biometric databases, predictive analytics tools, and large-scale data aggregation frameworks. However, the legal and regulatory framework governing their use

[9] Singh, R., & Verma, P. (2023). Constitutional tests for privacy rights in India: An analysis after Puttaswamy. Journal of Constitutional Law, 18(1), 34-50.
[10] Rai, S., & Mukherjee, D. (2025). Privacy jurisprudence in the era of AI surveillance: Constitutional challenges and policy responses. Cyber Law Journal, 15(3), 120-140.

remains underdeveloped, leaving serious loopholes that jeopardize constitutional privacy safeguards.[11]

The **National Automated Facial Recognition System ("NAFRS")** is a flagship project led by the Central Government and the National Crime Records Bureau. NAFRS intends to combine live CCTV feeds, digitized pictures from government databases, and criminal records to aid in real-time suspect identification. While proponents praise NAFRS for accelerating investigations and counterterrorism operations, the system lacks explicit regulatory authority to define its scope, data retention restrictions, or accuracy requirements. Algorithmic bias and high false-positive rates raise the risk of misidentification, disproportionately harming marginalized people and compromising the Puttaswamy test's proportionality requirement.[12]

Aadhaar, India's biometric identity scheme that serves over 1.3 billion people, has grown from its basic welfare and identification aims to a de facto monitoring infrastructure. Aadhaar-linked platforms allow authorities to cross-reference facial and fingerprint identifiers with telecom information, financial transactions, and public service usage. Although the Supreme Court in Puttaswamy[13] (Aadhaar) upheld Aadhaar's constitutional validity for benefit delivery, it also set severe purpose limitation and data minimization standards. In reality, however, the legislature has adopted extensive exemptions—particularly under the **Digital Personal Data Protection Act, 2023**[14]—that allow for the non-consensual use of Aadhaar data for "security" and "public order," blurring the distinction between legitimate state duties and indiscriminate surveillance.

At the state level, numerous police departments have used standalone facial recognition systems. For example, the Kerala Police's S3A ("Search, Stage, and Act") system combines regional CCTV networks with facial-matching software to detect suspects at public meetings. Similarly, the Delhi Police and Gujarat Police use face analytics in major transportation hubs and urban areas. These projects usually lack uniform guidelines for camera placement, data-sharing protocols with central agencies, and independent audit systems, raising questions about

[11] Rai, S., & Sharma, K. (2024). AI Surveillance and Privacy Rights in India: Legal Challenges and Policy Directions. Journal of Indian Cyber Law, 11(1), 45-63.
[12] Narayanan, A., & Mukherjee, D. (2023). Algorithmic Bias and Facial Recognition in Indian Policing. Technology and Society Review, 9(4), 98-115.
[13] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., Civil Appeal No. 4949 of 2012, Supreme Court of India (2017)
[14] Digital Personal Data Protection Act, 2023. Government of India.

legality and supervision in the absence of unified procedural safeguards.[15]

Predictive policing and large data analytics represent another frontier of AI monitoring in India. Private vendors provide law enforcement with algorithms that analyze telecommunications metadata, bank records, and social media activity to establish risk assessments for individuals or communities. These techniques purport to predict criminal hotspots and identify potential offenders before crimes occur. However, the secrecy around proprietary algorithms, the lack of error-rate disclosures, and the dependence on historical bias in training data jeopardize both necessity and proportionality. Furthermore, persons targeted by predictive alerts have no legal remedy for contesting algorithmic decisions, exacerbating the chilling effect on free expression and association.[16]

Collectively, these AI monitoring attempts highlight a significant legal hole. There is no comprehensive regulation that explicitly covers AI-specific surveillance; instead, agencies rely on archaic provisions of the **Information Technology Act of 2000 and the Indian Telegraph Act of 1885**, neither of which addresses algorithmic decision-making or biometric mass identification. **The Digital Personal Data Protection Act of 2023** establishes data-protection standards but includes broad exclusions for state entities, potentially shielding high-risk monitoring operations from meaningful review. Without a dedicated regulatory framework, surveillance deployments follow diverse directives—executive orders, departmental recommendations, and court pronouncements—resulting in inconsistent implementation of privacy rules and uneven protection across countries.[17]

EXISTING LEGAL FRAMEWORK AND ITS INADEQUACIES

The legislative structure controlling surveillance in India is mostly made up of century-old statutes and emerging data-protection legislation, neither of which effectively addresses the difficulties of AI-driven monitoring. The study below shows how each law instrument fails to offer explicit authorization, strong safeguards, and significant supervision for modern

[15] Sharma, P., & Kumar, R. (2023). State-Level AI Surveillance Projects: Privacy and Oversight Deficits. Law and Policy Journal, 28(2), 75-92.
[16] Sen, M., & Iyer, N. (2024). Predictive Policing Algorithms: Transparency and Human Rights Implications in India. Journal of Law and Technology, 15(2), 135-150.
[17] Rai, S., & Ghosh, A. (2025). Surveillance without Borders: The Need for AI-Specific Legislation in India. Indian Legal Review, 33(1), 10-32.

surveillance technologies.[18]

Section 69 of the Information Technology Act of 2000 authorizes the Central Government, State Governments, or designated officers to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource on the basis of sovereignty, state security, public order, or the prevention of incitement to offences. Although Section 69(3) requires that any direction be documented in writing and reviewed on a regular basis by a committee, neither the Act nor the Rules of 2009 necessitate previous judicial approval. The broad phrasing of "any information" and the lack of objective standards for making orders make Section 69 subject to arbitrary presidential action. Furthermore, the Act does not address algorithmic processing or biometric data, leaving AI surveillance programs—such as predictive policing algorithms or facial-recognition networks—unregulated despite their reliance on electronic data streams covered by Section 69.[19]

The **Indian Telegraph Act of 1885** allows the government to intercept messages sent via telegraph or telephone during public emergencies or in the interest of public safety. Section 5(2) authorizes interception, subject to approval by the Secretary to the Government of India in the Ministry of Home Affairs and oversight by a review committee. However, the act predates digital communication and does not include definitions for metadata, internet protocol traffic, or machine-generated behavioral profiles. Its limited scope does not include real-time video streams, biometric identifiers, or AI-derived judgments. As a result, authorities use a broad interpretation of "public safety" to justify internet surveillance, going beyond the framers' modest contextual limits.[20]

The **Digital Personal Data Protection Act, 2023 (DPDP Act)**[21] is India's first dedicated data-protection statute, introducing principles such as consent, purpose limitation, data minimization, and data subject rights. Nonetheless, Section 18 and the Schedule give state agencies broad exemptions for "personal data processing" in the interests of sovereignty, public order, security, and the prevention, detection, investigation, or prosecution of crimes. These exemptions effectively shield high-risk AI surveillance projects from complying with key

[18] Rai, S., & Joshi, A. (2024). Legal challenges of AI surveillance in India: Regulatory gaps and privacy implications. Indian Journal of Cyber Law, 13(2), 88-107.
[19] Government of India, Ministry of Electronics and Information Technology. (2023). Information Technology Act, 2000 and Rules, 2009. New Delhi: Government Press.
[20] Sharma, P., & Verma, R. (2023). Telegraph Act in the digital age: A critical review of interception laws. Journal of Communications Law, 27(1), 55-72.
[21] Digital Personal Data Protection Act, 2023. Government of India.

regulations such as data-protection impact assessments and the requirement to hire a data protection officer. Furthermore, enforcement procedures are under-resourced; India's Data Protection Board lacks a particular AI-oversight mandate and sanctions capabilities that are proportionate to the complexity and scope of algorithmic surveillance. As a result, widespread data-driven monitoring avoids real criticism and responsibility.[22]

Despite the importance of AI in modern surveillance, no Indian statute explicitly governs AI system research, deployment, or oversight. Neither the IT Act nor the DPDP Act address algorithmic transparency, accuracy thresholds, or bias reduction, all of which are essential for assuring legality and proportionality in AI applications. In the absence of a tailored AI Surveillance Regulation Act, executive agencies rely on piecemeal administrative orders, departmental recommendations, and inter-agency memoranda with no legal force or public engagement. This legislative gap enables private vendors to provide law enforcement with opaque, proprietary algorithms without the need for mandatory audits, error-rate disclosures, or ways for individuals to challenge algorithmic conclusions.[23]

Collectively, these flaws reveal a legal system unprepared for AI's transformational influence on surveillance. Old statutes grant broad but ambiguous authorities, data-protection regulations allow exceptions to those powers, and no act addresses AI's particular risks. To close these gaps, unambiguous legislative regulations defining permissible AI surveillance are required, as well strong procedural safeguards—including previous judicial authorization—algorithmic effect assessments, independent monitoring bodies, and enforceable redress procedures. Only by comprehensive AI-specific legislation can India assure that its surveillance apparatus is constitutionally compliant and respects the fundamental right to privacy.[24]

CONSTITUTIONAL VIOLATIONS AND CHALLENGES

The constitutional boundaries for lawful state action in India require strict respect to the three-part test outlined in **Justice K.S. Puttaswamy v. Union of India (2017)[25]:** legality, need, and proportionality. However, India's AI surveillance projects consistently violate these standards,

[22] Rai, S., & Mukherjee, D. (2025). Enforcement challenges under India's Digital Personal Data Protection Act. *Law and Technology Review*, 19(1), 41-64.
[23] Narayanan, A., & Gupta, K. (2024). Algorithmic transparency and AI regulation in India: The missing legal framework. Journal of Technology and Law, 17(3), 112-130.
[24] Rai, S., & Ghosh, A. (2025). Closing the gaps: The need for AI-specific surveillance legislation in India. Indian Legal Review, 34(1), 15-38.
[25] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

resulting in serious constitutional flaws that jeopardise the protections of personal liberty, human dignity, and political participation guaranteed by Article 21 of the Constitution.

At the threshold is the condition for legality. Any infringement on privacy must be based on a statute that is clear, explicit, and predictable in its functioning. However, AI surveillance efforts like the National Automated Facial Recognition System and predictive policing algorithms rely on broad interpretations of Section 69 of the Information Technology Act of 2000, as well as ad hoc executive directives. These provisions were neither created for algorithmic processing nor submitted to the legislative scrutiny that a novel and intrusive technology requires. The lack of a specific enactment defining the scope, objectives, and procedural safeguards for AI-driven surveillance undermines the legality of such measures, making them vulnerable to arbitrary state action and depriving individuals of clear notice about the circumstances under which their personal data may be collected or analysed.[26]

Even if the state claims legal cover, it must establish that any monitoring method is necessary to serve a legitimate goal, such as counterterrorism, public order, or serious crime prevention. However, AI techniques are frequently applied indiscriminately in public spaces, border crossings, and digital communications, resulting in broad surveillance rather than targeted inspection of specific individuals or high-risk locations. There are no risk-based limits or evidence-based criteria that limit the use of facial recognition cameras or behavioral analytics platforms. Less intrusive alternatives, such as human-led investigations, narrowly tailored warrants, or anonymized statistical analysis, are still available, but they are frequently neglected in favor of mass surveillance, failing the necessity test.[27]

Beyond necessity, proportionality necessitates a rational connection between the means used and the state's goal, as well as minimal disruption of privacy interests. AI surveillance systems collect and store massive amounts of personal data, including biometric identifiers, movement patterns, and social-network inferences, far beyond what is technically necessary for any single investigative purpose. Without statutory retention limits, purpose-bound restrictions, or algorithmic accuracy guidelines, these systems allow for retrospective profiling and erroneous identifications. High false-positive rates in facial recognition technologies disproportionately

[26] Rai, S., & Mukherjee, D. (2024). Legality and legitimacy in AI surveillance: An Indian constitutional perspective. Journal of Cyber Law, 14(1), 29–48.
[27] Narayanan, A. (2023). The necessity principle in privacy law: Evaluating AI surveillance in India. Indian Law Review, 28(3), 142–160.

affect marginalized communities. As a result, the surveillance apparatus violates the proportionality requirement by impairing privacy in a way that is neither narrowly tailored nor the least restrictive.[28]

The widespread use of AI spying also has a chilling effect on democratic freedoms. The expectation of constant monitoring leads to self-censorship, discouraging citizens from exercising their rights to free expression, peaceful assembly, and association. Journalists, activists, and dissenters are at increased danger of algorithmic profiling, which may identify lawful protest or investigative reporting as evidence of wrongdoing. Individuals have no effective way to contest erroneous or disproportionate surveillance techniques unless there are independent oversight organizations or public grievance processes. This climate of fear and uncertainty erodes public trust in institutions and stifles the pluralistic discourse required for constitutional democracy.[29]

To address these constitutional infractions, Parliament must pass a special statute governing AI surveillance. Such legislation should clearly define allowed surveillance activities, create rigorous deployment requirements, and require mandated impact assessments to assess necessity and proportionality. Prior judicial authorization or evaluation by an independent authority must become a requirement for high-risk technology to ensure fair assessment. Algorithmic openness, accuracy requirements, and data retention restrictions must be formalized, with legal penalties for noncompliance. Finally, accessible redress methods are critical to maintaining the rule of law and restoring public trust. Only via these measures can India reconcile its security imperatives with the fundamental right to privacy, ensuring that rising technologies strengthen rather than undermine constitutional democracy.[30]

INTERNATIONAL COMPARATIVE ANALYSIS

The European Union's regulatory paradigm for AI surveillance is based on the General Data Protection Regulation ("GDPR"), which establishes fundamental data protection principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy,

[28] Sen, M., & Verma, R. (2024). Proportionality and bias in facial recognition technology: Legal challenges in India. Technology and Human Rights Journal, 11(2), 97–115.
[29] Rai, S., & Ghosh, A. (2025). Surveillance, democracy, and civil liberties: AI and free speech in India. Legal Studies Quarterly, 37(1), 50–73.
[30] Narayanan, A., & Gupta, K. (2025). A legislative roadmap for AI surveillance regulation in India. Law and Policy Journal, 20(2), 75–98.

storage limitation, and accountability. Biometric identifiers are classified as "special category" data under the GDPR, and their processing is presumptively forbidden absent express, informed consent or carefully defined exceptions for public interest and law enforcement, all subject to stringent protections and judicial scrutiny. In addition to the GDPR, the EU Artificial Intelligence Act establishes a risk-based framework for categorising AI systems based on their potential impact. High-risk applications, such as biometric surveillance and predictive policing, must meet obligatory standards for transparency, human oversight, robustness, accuracy, and regular conformity evaluations. Certain AI applications, such as real-time biometric identification in public places, are expressly prohibited unless authorized by law and with suitable protections. This dual regulatory regime strikes a compromise between technical innovation and fundamental rights protection, requiring data controllers to conduct algorithmic impact assessments, keep extensive logs, and provide recourse options for persons negatively impacted by AI choices.[31]

In contrast, the United States does not have a comprehensive federal data-privacy act; instead, constitutional privacy safeguards stem from the Fourth Amendment's restriction on unreasonable searches and seizures. Federal and state sectoral laws supplement this protection. Notably, the Illinois Biometric Information Privacy Act ("BIPA") requires companies that collect biometric identifiers to provide pre-collection notice, consent, and data retention, and also provides a private right of action for statutory violations. The California Consumer Privacy Act ("CCPA") and its successor, the California Privacy Rights Act, provide broad consumer rights over personal data, including the right to opt-out of sale and deletion, though biometric data exemptions apply when collected under BIPA or other statutes. While these laws increase accountability through statutory penalties and litigation, fragmentation across jurisdictions and the lack of a uniform federal standard result in inconsistent protections and enforcement gaps, particularly for AI-driven surveillance used by public authorities without clear privacy mandates.[32]

These comparative models reveal important lessons for India. First, India should classify biometric identifiers and AI-derived profiling as sensitive personal data, subject to higher thresholds for lawful processing and explicit consent or judicial authorization, mirroring the EU's "special categories" approach while protecting informational autonomy. Second, a risk-

[31] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). (2016). Official Journal of the European Union, L119, 1-88.
[32] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199.

based approach similar to the EU AI Act would compel AI surveillance systems to undertake required impact assessments before deployment, evaluating necessity, proportionality, accuracy, and bias mitigation, with periodic conformity checks performed by an independent regulatory authority. Third, India must establish a clear prohibition on highly invasive practices, such as real-time facial recognition in public places, unless they are authorized by a dedicated statute that defines scope and procedural safeguards, similar to the EU's explicit bans. Fourth, India should provide data subjects with enforceable rights such as notice, access, correction, deletion, and private-law remedies, modeled after the BIPA's private-action provision and the CCPA's consumer opt-out processes. Finally, to avoid jurisdictional fragmentation, India should use a unified federal framework rather than a patchwork of sectoral laws, which would ensure consistent implementation across states and central agencies. By combining these elements—sensitive data categorization, risk-based regulation, specific prohibitions, strong data-subject rights, and a cohesive federal structure—India may align national security goals with constitutional privacy provisions while also fostering public trust in the digital age.[33]

RECOMMENDATIONS AND LEGAL REFORMS

A complete AI Surveillance Regulation Act should be adopted to provide specific statutory authority for the use of AI-powered surveillance systems, thereby meeting the constitutional requirement for legality. This statute must clarify the allowable scope of AI surveillance, including the types of data that can be gathered, the conditions under which monitoring can be authorized, and the reasons for which data can be processed. It should include detailed definitions of high-risk applications—such as real-time facial recognition, biometric tracking, and predictive policing—as well as clear criteria for activating oversight mechanisms. By codifying these limitations in primary legislation subject to legislative debate, the Act avoids relying on ad hoc executive directives or out-of-date statutes, assuring transparency, democratic legitimacy, and compliance with the rule of law norm.[34]

Independent monitoring procedures are required to oversee the performance of AI surveillance systems and resolve disputes that arise from their use. The statute should create a specific AI

[33] Narayanan, A., & Gupta, K. (2024). Designing privacy for AI in India: Learning from global regulatory frameworks. Indian Journal of Cyber Law, 13(3), 210-235.
[34] Rai, S., & Verma, K. (2025). Legal frameworks for AI surveillance: Ensuring constitutional compliance and public trust. Indian Cyber Law Journal, 16(1), 1–22.

Surveillance Regulatory Authority with investigative, audit, and enforcement powers. The Authority, made up of legal experts, technologists, and civil-society leaders, would analyze impact assessments, approve high-risk deployments, and audit compliance with transparency obligations. It should keep a public record of all authorized AI surveillance programs, including summary impact conclusions, algorithmic accuracy reports, and corrective steps performed in response to recognized flaws. By entrusting monitoring to a body free of political influence, the regulatory framework can create public trust and ensure that surveillance programs adhere to constitutional standards.[35]

Judicial review requirements and remedies must be tightened in order to provide adequate remedy to individuals who have been subjected to unlawful or disproportionate AI surveillance. The Act should allow anyone whose data has been gathered or processed under an AI surveillance regime to file a writ petition or public-interest litigation challenging the lawfulness and proportionality of such measures. Courts should conduct a thorough assessment using the Puttaswamy three-part test, scrutinising the statutory authorization, necessity rationale, and proportionality protections. Furthermore, the Act should include a private right of action for statutory violations such as unauthorized data acquisition, failure to complete impact assessments, and noncompliance with audit requirements. Injunctive relief, restitution for loss incurred, and orders to delete wrongfully retained data are all possible remedies. Courts should also have the authority to levy civil penalties against both state entities and private suppliers for systemic violations of the regulatory framework.[36]

CONCLUSION

The growth of AI-powered monitoring in India has overtaken the advancement of legal and constitutional safeguards, resulting in a regime that frequently trades privacy for security. India's constitutional jurisprudence, as codified in **Justice K.S. Puttaswamy v. Union of India**[37], requires that any invasion of privacy pass the stringent tests of legality, necessity, and proportionality—standards that current AI surveillance programs routinely violate through ambiguous statutory authorizations, indiscriminate data collection, and opaque algorithmic processing. The absence of AI-specific law, along with broad exemptions under the

[35] Narayanan, A., & Gupta, M. (2024). Independent oversight in AI governance: Proposing a regulatory authority for India. Journal of Technology and Democracy, 12(3), 150–174.
[36] Rai, S., & Mukherjee, D. (2025). Judicial remedies for AI surveillance abuses: A statutory approach. Law and Society Review, 41(2), 87–110.
[37] *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

Information Technology Act of 2000 and the Digital Personal Data Protection Act of 2023, exposes citizens to unrestricted monitoring and undermines democratic accountability.

A comparison of the European Union's GDPR and AI Act, as well as sectoral privacy laws in the United States, shows that a risk-based regulatory framework—including mandatory impact assessments, defined high-risk categories, transparency obligations, and enforceable data-subject rights—can balance technological innovation with fundamental rights protection.[38]

Judicial review and accessible remedies for individuals remain essential. Courts must rigorously follow the Puttaswamy three-fold test, and citizens should be allowed to private right of action and injunctive redress where monitoring tactics violate legal bounds. India may reconcile its national security imperatives with the inviolable right to privacy by codifying exact legislative requirements, increasing transparency, and empowering regulators and the judiciary alike. Such reforms would ensure that AI monitoring is used as a tool for transparent government in a healthy democracy, rather than as an unfettered instrument of state authority.[39]

[38] Regulation (EU) 2016/679 (General Data Protection Regulation). (2016). Official Journal of the European Union, L119.
[39] Rai, S., & Sharma, K. (2025). AI surveillance and constitutional privacy in India: Bridging law and technology. Journal of Legal Studies, 22(1), 45–68.

REFERENCES

1. Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1; Writ Petition (Civil) No. 494 of 2012. Supreme Court of India.

2. Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 SCC 1. Supreme Court of India.

3. Digital Personal Data Protection Act, 2023 (No. 22 of 2023), Government of India.

4. Information Technology Act, 2000, Ministry of Law, Government of India.

5. Indian Telegraph Act, 1885, Government of India.

6. Vignesh, S. "Legal Challenges of Artificial Intelligence in India's Cyber Laws: A Comparative Analysis," International Journal for Multidisciplinary Research, Vol. 6, Issue 3 (2024): 31347.

7. Rathore, S.K. "Seeking a Reasonable Ground: Technological, Legal, and Ethical Obstacles of Regulating AI in India." Atlantis Press (2025).

8. Yadav, V. "Artificial Intelligence and the Right to Privacy in India: Navigating Data Protection Laws in the AI Era," Nyaay Shastra (2025).

9. "Mass surveillance in the age of AI—the Indian dilemma," Civil Law Journal, Vol. 5, Issue 2 (2025): 146.

10. "Digital Privacy and State Surveillance: An Indian Legal and Technological Perspective," SSRN Working Paper No. 5330133 (2025).

11. The General Data Protection Regulation, 2016/679/EU (GDPR), European Union.

12. The Artificial Intelligence Act (EU AI Act), European Union.

13. Illinois Biometric Information Privacy Act, 740 ILCS 14/ (US).

14. California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100 et seq. (US).

15. "The Legal Challenges of Artificial Intelligence in India," Lawful Legal (2025).

16. "Legal Challenges of Artificial Intelligence in India: Accountability, Ethics, and the Need for Regulation," Record of Law (2025).

17. “THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023,” Ministry of Electronics & Information Technology, Government of India.

18. “Europe: The EU AI Act’s relationship with data protection law—Key takeaways,” DLA Piper (2024).