International Journal of Advanced Research and Development
www.multireviewjournal.com
ISSN: 2455-4030
Received: 25-11-2025, Accepted: 20-01-2026, Published: 04-02-2026
Volume 11, Issue 1, 2026, Page No. 56-60

Balancing AI-driven surveillance in India: legal aspects of digital privacy dilemmas

Sneha Purohit
Research Scholar, Department of Law, Jagannath University, Jaipur, Rajasthan, India

Abstract
Artificial intelligence (AI) is being quickly incorporated into India's legal industry, bringing with it previously unheard-of efficiencies and revolutionising tasks like contract administration, predictive analytics, and legal research. However, given the lack of AI-specific laws in India, this integration also poses serious privacy and data protection issues. The Artificial Intelligence Act (AIA) of the European Union, on the other hand, offers a thorough framework that sets strict criteria for privacy, responsibility, and openness in AI applications, especially in high-stakes domains like law.
In addition to evaluating the inadequacies in India's legislative framework in comparison to the EU's approach, this paper explores the privacy and ethical hazards connected with AI in India's legal services and provide practical suggestions for deploying AI responsibly within India's legal context. This article promotes an Indian regulatory framework that protects privacy, guarantees responsibility, and upholds public trust in AI-augmented legal services through a thematic examination of ethical, technical, and legal issues as well as real-world case examples. The results highlight how urgently AI-specific regulations are needed in order to comply with global norms and handle the intricate privacy issues that AI presents to the Indian legal industry.

Keywords: Balancing AI driven, surveillance, digital privacy, data protection, artificial intelligence, indian legal services

Introduction
Artificial intelligence (AI) is transforming a number of industries globally by providing improvements in speed, accuracy, and efficiency. AI is revolutionising legal research, case analysis, predictive analytics, and document review—tasks that have historically been completed by human specialists. In countries like India, where the legal system faces significant obstacles because of heavy caseloads, limited resources, and a protracted backlog of cases, these AI-driven technologies are especially tempting. AI can improve accessibility and make legal procedures quicker and more economical for clients and practitioners by automating repetitive operations and offering predictive insights. However, there are serious privacy, data security, and ethical issues with the increasing use of AI in legal services. Access to sensitive personal data, such as client information, case histories, and private legal communications, is frequently necessary for AI models used in legal applications. Clients and legal professionals may be exposed to biases in AI algorithms, illegal data access, and breaches as a result of this data. Furthermore, a lot of AI systems operate as "black boxes," where the decision-making procedures are difficult to understand. This puts accountability and transparency—values essential to the legal system—at risk. Global legislative frameworks to control the creation and application of AI systems are evolving in response to these issues. For example, the Artificial Intelligence Act (AIA) was introduced by the European Union. This regulatory framework places stringent restrictions on high-risk applications, such as those utilised in legal and judicial settings, and classifies AI applications according to their level of danger. In order to protect people's rights when using AI technologies, the AIA requires adherence to privacy, transparency, and accountability criteria. India, on the other hand, relies on general data protection regulations like the Digital Personal Data Protection Act (DPDPA) of 2023 and lacks a comprehensive legal framework that tackles AI's particular privacy and data protection challenges.

Surveillance In India
As technology has advanced, surveillance has changed dramatically. Surveillance is essential to security, law enforcement, and business operations, from conventional monitoring methods to complex systems utilising artificial intelligence and massive data collection. State and private entities in India have developed a number of techniques as a result of the expansion of surveillance technologies.
Even while the idea of surveillance has changed over time, there is still no precise, widely recognised definition, particularly when it comes to contemporary technologies. The debate over what surveillance actually entails nowadays has become more complex due to the emergence of new monitoring techniques like "sousveillance", in which people observe those in positions of authority. According to Ross Bellaby, surveillance encompasses more than just CCTV monitoring. It now includes digital surveillance techniques like "dataveillance" and data mining, in which a person's identity, movements, relationships, and activities are continuously monitored and examined.

Rapid AI Adoption and Technological Advancements in India
India, the second most populous country in the world and one that is developing quickly, has embraced technology innovations at a rate never seen before. With more than a billion mobile users and a growing digital ecosystem that promotes technological accessibility, India is home to one of the biggest mobile-using populations. This change has been expedited by the advent of artificial intelligence (AI), as people depend more and more on AI-driven products for productivity, convenience, and creativity in a variety of industries.

AI applications have been used in a variety of Indian sectors in recent years:

- **Cinematography:** AI applications have been used in a variety of Indian sectors in recent years:
- **Medical Field and Robotics:** AI is utilised to improve healthcare through patient management, robotic surgery, diagnostics, and predictive analytics.
- **Education:** AI-driven systems facilitate student evaluations, individualised instruction, and educational administration.
- **Legal Sector:** AI is transforming case management, contract analysis, predictive analytics, and case research by providing legal professionals with quicker, data-driven decision-making tools.

Particularly notable are the extent and application of AI in India's legal sector. While judicial authorities investigate AI for case management and workflow optimisation, legal professionals use AI for activities like document review, legal research, and case outcome prediction. AI presents viable ways to expedite legal procedures in light of India's heavy caseload and backlogs. However, its use raises concerns about accountability, prejudice, and privacy, particularly in high-stakes situations.

Privacy and Data Security in AI-Driven Legal Services: An International and Indian Viewpoint

There are two sides to AI-driven legal services applications. They can lessen manual labour and boost efficiency, but they also pose hazards to data security and privacy. By creating particular privacy safeguards for high-stakes AI applications through the AIA, the European Union has taken the lead globally. This rule introduces steps to minimise algorithmic bias and protect individual privacy in addition to requiring responsibility and openness. Strict data openness, fairness, and explainability requirements must be met by AI systems in high-risk industries in order to guarantee that automated choices can be tracked down and defended. However, India has not yet put in place an equivalent AI-specific legislative structure. Although the DPDPA 2023 offers a fundamental framework for data security, it ignores the complexities of AI, like algorithmic transparency, bias reduction, and accountability for automated decision making. Because AI algorithms frequently handle sensitive data, creating questions about privacy, security, and fairness, this regulatory gap poses difficulties for Indian legal services. Particularly in India's socio-culturally varied environment, AI systems may unintentionally reinforce biases in past data, producing discriminating results.

AI-Driven Legal Services In India: Privacy Difficulties

The use of AI in India's legal system has raised grave worries about sensitive and personal data privacy. It is crucial to comprehend the type and extent of AI applications being used in the Indian judiciary before discussing these privacy consequences.

The Indian Judiciary's AI Projects

Artificial intelligence (AI) has been used by the Indian judiciary to improve accessibility, expedite procedures, and boost the effectiveness of court cases. Among the notable uses of AI are:

- **Translation:** Hindi, Tamil, Punjabi, Marathi, Malayalam, Bangla, Telugu, Kannada, Nepali, and Urdu are among the vernacular languages into which the Supreme Court uses artificial intelligence to translate court orders and documents. By offering crucial legal papers in their native tongues, this program increases individuals' accessibility.
- **Legal Studies:** AI tools make legal research more thorough and efficient, allowing for faster and more precise case law interpretation.
- **Automation of Processes:** The Supreme Court of India currently uses AI to automate a number of procedures, which minimises human mistake and manual labour.
- **Transcription of Oral Arguments**: Oral arguments for Constitution Bench cases are automatically transcribed by AI-based transcription systems, maintaining accurate records and making future references easier.

Case Law and Precedent Support:

The Judges are assisted by the Supreme Court Portal for Assistance in Court Efficiency (SUPACE), which offers pertinent case laws and precedents. Judges can make more accurate decisions by using this technology to swiftly find reliable sources.

- **Automated Submission:** By directly extracting data from case papers, Nyaay AI, created by Indika AI, streamlines document processing and saves time by automating filing.
- **Defect Detection in Filings:** AI finds filing flaws, cutting down on delays brought on by inaccurate or missing documentation.
- **Case Triaging and Bunching:** Critical issues are handled quickly thanks to AI algorithms that priorities and classify instances according to urgency.
- **Research on Judgment :** AI facilitates judgement study, allowing judges to examine prior rulings and make informed conclusions.

Some contend that by rigorously following precedents, reducing individual biases, and effectively processing enormous volumes of data, artificial intelligence (AI) can improve the fairness of judgements. These projects reflect important breakthroughs in the functioning of the Indian court. Despite its advantages, AI poses serious ethical and privacy issues, especially with regard to data security, accountability, and transparency. A strong regulatory framework is necessary to handle these issues and safeguard citizens' rights when using AI in such delicate areas.

Mechanisms for National Security and Surveillance

In light of the growing threat of terrorism, cybercrime, and foreign espionage, national security has become the most important issue facing the Indian state. To counter such dangers, the government has created a variety of legal tools and monitoring systems, often at the sacrifice of openness and individual privacy.

One of the most important legislative tools is the Information Technology Act, 2000 (particularly Section 69), which gives the government the authority to monitor, intercept, or decrypt any information for reasons of national security, public order preservation, or sovereignty. Similarly, Section 5(2) of the Indian Telegraph Act 1885 permits telephone interception under extremely vague and expansive standards, typically with minimal verification.

India has also developed extensive monitoring programs. The government can monitor all conversations without the telecom service providers' prior consent thanks to the Central Monitoring System (CMS). The Defence Research and Development Organisation (DRDO) created NETRA, which keeps an eye on internet traffic and generates suspicious leads when specific keywords are found. NATGRID is a surveillance architecture that combines data gathered by multiple government entities.

Additionally, because they focus sensitive data, biometric and demographic data collection schemes like Aadhaar have raised certain privacy-related issues. Despite its goal of delivering services efficiently, Aadhaar is vulnerable to profiling and abuse because it is connected with other databases.

The government claims that these systems are justifiable on the grounds of national security (to protect the nation and deter crime). However, the lack of legal protection, transparency, and judicial checks and balances makes these instruments susceptible to misuse and arbitrary surveillance.

Even while the state has a legitimate role in maintaining security, the unrestricted expansion of its monitoring capabilities poses a threat to constitutional liberties. Without legislative control and clarity, such systems have the potential to work against the democracies they are meant to support.

Privacy Concerns & Constitutional Conflict

Significant concerns over people' privacy and constitutional protection were raised by India's high rates of encryption gaps and digital surveillance. The topic of whether the state is permitted to monitor internet traffic, mobile device usage, and interpersonal communication becomes increasingly dubious in terms of consent, transparency, and legality as more and more data is made available to the public.

India has not been able to establish a trademark registration system since it lacked a uniform data protection mechanism until the Digital Personal Data Protection (DPDP) Act, 2023 was passed. The lack of clear guidelines for data collection, use, and storage left citizens vulnerable to unlawful intrusions by the government and non-state actors. The DPDP Act is an improvement, but it still lacks a number of features, including protection against state surveillance and non-state inspection.

An example of how people might be put in danger by unmonitored spying is the employment of the Israeli business Pegasus malware by Indian authorities to spy on journalists, activists, and opposition members. The problem with press intrusion is that, despite the invasion of privacy, Pegasus's actions stifled free speech, which calls into question the right to free speech under Article 19 of the Constitution.

Overall, a portion of Article 21 that includes the right to life and personal liberty is at risk owing process-less digital surveillance. The Supreme Court's 2017 Puttaswamy ruling reaffirmed that privacy is a basic right, whereas systems like CMS and NATGRID operate in legal limbo and are typically not scrutinised by courts or even the legislature.

Furthermore, the foundation of any privacy framework is consent, which is often undermined by government-led activities. Citizens have little control over their information due to ambiguous regulations governing data sharing or the obligation to integrate Aadhaar with a service.

It is an ecology of unrestrained monitoring that illustrates two conflicting civil interests found in the constitution: the state has a right to security, which is frequently acquired in an unlawful manner. Online surveillance will become an oppressive tool rather than a security one unless there are strong procedural protections, data protection enforcement, judicial scrutiny, etc.

Finding a balance between the needs of national security and constitutional privacy is now essential to averting dangers to democracy.

The Constitutional Dilemma

The fundamental constitutional conundrum is how to strike a balance between the right to privacy and national security. The government frequently uses public order, cyber security, and counterterrorism as justifications for increased surveillance. Puttaswamy, however, requires that proportionality be met by any incursion.

These constitutional restrictions are emphasised by court rulings. The Supreme Court emphasised that limitations on digital communication must be reasonable and proportionate in Anuradha Bhasin v. Union of India, (2020) 3 SCC 637. The Court broadened the definition of "procedure established by law" in Maneka Gandhi v. Union of India, AIR 1978 SC 597, mandating that any process limiting liberty be reasonable and fair.

Despite these ideals, current surveillance methods run the risk of stifling free expression, suppressing dissent, and facilitating algorithmic discrimination. Concerns about democratic accountability and the separation of powers are raised by the executive branch's concentration of informational power. Differentiating between lawful surveillance and arbitrary intrusion becomes more challenging in the absence of significant oversight.

Constitutional Provisions

Article 21 of the Constitution, which protects the right to life and personal liberty, it is the cornerstone of privacy rights in India. A nine-judge Supreme Court bench unanimously ruled in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 that the right to privacy is a fundamental right inherent in Article 21 and Part III of the Constitution. The Court ruled that the right to be left alone, informational self-determination, and decisional autonomy are the three fundamental components of privacy.

Both Article 19(1)(d), which protects freedom of travel, and Article 19(1)(a), which guarantees freedom of speech and expression, have important privacy implications. By monitoring and possibly discouraging legitimate expression and travel, surveillance, especially AI-enabled surveillance, can have a chilling impact on these liberties.

Statutory Framework

India's legal structure for protecting privacy is still disjointed and unable to deal with issues related to AI spying. Although it was passed before to the widespread use of AI technology, the Information Technology Act, 2000

(IT Act) regulates electronic data. While Section 72A of the IT Act makes it illegal to disclose personal information without authorisation, Section 43A mandates that body corporate establish acceptable security procedures for sensitive personal data. However, these laws do not specifically target AI-based processing and include substantial exclusions for government organisations.

India's first comprehensive data protection law is the Digital Personal Data Protection Act, 2023 (DPDP Act), which was approved by the president in August 2023. Consent, purpose limitation, and data minimisation are concepts established by the Act. However, detractors contend that Section 17's substantial exclusions for government agencies particularly with regard to "sovereignty and integrity of India" and "security of the State" create gaps that could allow for widespread AI spying without sufficient protections.

Biometric data collection is governed by sector-specific laws like the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, which have also been the focus of privacy lawsuits. Although they govern telecommunication interception, the Telegraph Act of 1885 and the Indian Telegraph Rules of 1951 are outdated and unsuited to deal with contemporary AI spying capabilities.

Legislation expressly governing algorithmic decision-making or artificial intelligence is conspicuously lacking. When AI systems violate privacy rights, the lack of AI-specific regulations raises questions about responsibility, transparency, and liability.

Gaps in the Current Legal Framework

The Digital Personal Data Protection (DPDP) Act, which effectively supersedes the Personal Data Protection Bill (PDPB) drafts, has prevented India from losing its progress as a digital governance system. Even while this is a significant step in the direction of safeguarding citizens' data rights, there are still significant gaps in the laws governing surveillance, judicial supervision, and accountability.

The DPDP Act introduces very basic concepts of data protection, such as permission, purpose limitation, and data minimisation. However, it has broad exceptions that allow the government to disregard many of these safeguards on the grounds of public order, national security, or sovereignty. This makes it possible for a wide range of unlawful monitoring to occur with limited options for recourse.

Furthermore, the Act lacks a robust, independent Data Protection Authority that might question or audit government monitoring programs. The administration is deemed to have a significant deal of discretion over this authority granted by the DPDP Act, raising the question of whether its judgements are being made impartially.

The fact that significant monitoring projects like CMS, NETRA, and NATGRID have been conducted without actual parliamentary authority exacerbates these issues. These programs are based on executive orders and pre-colonial laws like the IT Act of 2000 and the Telegraph Act of 1885, which were not intended for widespread monitoring in the absence of a specific democratic culture.

India still has a long way to go when it comes to filling the legal void surrounding surveillance, even if it has subsequently made significant progress in creating legal frameworks to protect data. Structural adjustments, unambiguous legislation, and checks on the executive branch are the only ways to close this gap.

Conclusion

Artificial intelligence (AI) has the potential to increase access to justice, decrease case backlogs, and improve efficiency in India's legal systems. But this development also raises important questions about ethical governance, responsibility, and privacy especially in the absence of AI-specific legal frameworks. Although it establishes the framework for data protection, the Digital Personal Data Protection Act (DPDPA) 2023 does not address the particular difficulties presented by AI in legal situations. The Artificial Intelligence Act (AIA) of the European Union, in contrast, requires stringent protections for high-risk applications, including legal technology, and offers a framework for classifying AI systems by risk. Such clarity is lacking in India's current regulatory framework, which leaves gaps in explainability, openness, and bias mitigation.

Current legal frameworks are insufficient for algorithmic monitoring because they were created for surveillance in the analogue age. Although the DPDP Act is a step forward, its exemptions allow for widespread government monitoring without adequate protections. Although judicial theory has developed significant concepts, it finds it difficult to deal with the size and complexity of AI systems.

Acknowledging that security and privacy don't have to conflict is necessary to go forward. Constitutional rights can be upheld and appropriate security measures made possible by well-crafted legislative frameworks. But striking this equilibrium requires technical know-how, political resolve, and a sincere dedication to democratic principles.

As India’s positions itself as a global technology leader, the choices made today regarding AI surveillance will define not only the privacy rights of current citizens but the nature of Indian democracy itself.

References

1. Kumar. Data Protection and Civil Liberties in India. New Delhi: Sage Publications, 2022, 112.
2. Banshal SK. Data Security and Ethical Considerations in Embedded AI Systems. In: Embedded Artificial Intelligence. Chapman and Hall/CRC, 2025, 279-292.
3. Bhattacharjee B. Facial Recognition Technology Balancing Ethical Considerations and Privacy Rights. Available at SSRN 4885585, 2024.
4. Chaudhary G. Unveiling the black box: Bringing algorithmic transparency to AI. Masaryk University Journal of Law and Technology,2024:18(1):93-122.
5. Dandotiya AS, Gupta SK, Dandotiya N, Sharma MP. AI in everyday life: transforming society. Navi International Book Publication house, 2024.
6. Negi Advocate C. In the Era of Artificial Intelligence (AI): Analyzing the Transformative Role of Technology in the Legal Arena. Available at SSRN 4677039, 2023.
7. Nithya M, Harini S, Kavyadharshini S, Srinidhi K. AI-Driven Legal Automation to Enhance Legal Processes with Natural Language Processing. In: 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS). IEEE, 2024, 1246-1253.
8. Rafiq J. Harnessing the Power of Artificial Intelligence in Indian Justice System: An Empirical Study. National Journal of Cyber Security Law,2024:7(1):18-37.

9. Rajendran RK, Vetrivel S, NR WB. The Role of AI in Enhancing Access to Justice and Legal Services. In: Exploration of AI in Contemporary Legal Systems. IGI Global Scientific Publishing, 2025, 139-162.
10. Renuka O, Radha Krishnan N, Priya BS, Jhansy A, Ezekiel S. Data Privacy and Protection: Legal and Ethical Challenges. Emerging Threats and Countermeasures in Cybersecurity, 2025, 433-465.
11. Sundara K, Narendran N. The Digital Personal Data Protection Act, 2023: analysing India's dynamic approach to data protection. Computer Law Review International,2023:24(5):129-141.
12. Prabhavathi N, Durai K. Role of Artificial Intelligence In Access To Justice And Justice Delivery In India. Library of Progress-Library Science, Information Technology Computer, 2024, 44(3).