INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

SURVELLANCE IN THE AGE OF AI: RETHINKING THE RIGHT TO PRIVACY

AUTHOR – ARYAN SISODIA, STUDENT AT AMITY LAW SCHOOL, AMITY UNIVERSITY, NOIDA

BEST CITATION – ARYAN SISODIA, SURVELLANCE IN THE AGE OF AI: RETHINKING THE RIGHT TO PRIVACY, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (6) OF 2026, PG. 98-104, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/IJLRV6I612

ABSTRACT

The recent development of Artificial Intelligence (AI) has changed th e surveillance systems around the world. AI-based tools of surveillance such as facial recognition systems are used by the government and the private sector to target individuals and predict their crimes. Though these innovations are beneficial in terms of security, efficiency and governance, they also create major issues concerning the violation of the right to privacy. This paper critically discusses how AI-powered surveillance can be used to strip individuals of their privacy rights, especially the Indian setting, and judge the suitability of existing laws. It also discusses why regulatory protection is necessary to bring about a balance between technological advancements and constitutional liberties.

1. INTRODUCTION

Surveillance using Artificial Intelligence (AI) is a paradigm shift in how governments and organizations track their citizens, places, and processes. It entails using sophisticated technologies like machine learning algorithms, facial recognition systems, biometric identification tools, and predictive analytics to gather, process, and analyze a substantial volume of data. In contrast to the conventional surveillance systems, AI-proficiency systems can independently study behavioural trends, detect anomalies, and even offer proactive forecasts, thus considerably increasing the bounds and effectiveness of surveillance.[236]

Today, the world's governments are adopting AI-driven surveillance into their administrative systems to conduct surveillance on crime, counter-terrorist operation, border security, and delivery of state services. An example of this application is that facial recognition technologies identify suspects on the go, and predictive policing algorithms help law enforcement organizations to distribute resources according to the anticipated criminal behavior. Though on the one hand, these technologies offer enhanced security and administrative efficiency, they also evoke serious issues when it comes to civil liberties, specifically the loss of individual privacy.

The ubiquitous aspect of AI surveillance allows constant and many times invisible surveillance, making it hard to determine when it is a matter of national security or a question of oppressive state regulation. In comparison to the traditional surveillance that tends to be focused and time-limited, AI systems allow conducting mass surveillance by combining information gathered through various means, such as social media, cameras in the streets, and government databases. Such an ability leads to the establishment of comprehensive digital profiles of persons, without knowledge or consent, which compromises the principle of informational self-determination.[237]

The constitutional acknowledgment of the right to privacy as a fundamental right in the Indian context through the Constitution under Article 21

[236] Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies 45–47 (Harvard Univ. Press 2018).

[237] Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement 21–25 (N.Y.U. Press 2017).

of the Constitution has given a pivotal element to the debate on surveillance. The Supreme Court had considered the importance of privacy through its landmark case; Justice K.S. Puttaswamy (Retd.), v. Union of India, which affirmed that any invasion of privacy should meet the necessity, legality, and proportionality tests. It is this jurisprudential framework that starts to come into place notably in assessing the validity of the AI-driven surveillance practices.[238]

The interplay of AI and surveillance presents a number of tricky legal and ethical challenges. Among the major issues is the absence of informed consent in gathering and processing data. People commonly do not even know how much of their information is being tracked, collected and processed. Also, AI systems can be vulnerable to biases in their training data, which can result into discriminatory results, especially against marginalized groups. The lack of transparency in decision-making also makes accountability more complex, as one cannot easily determine how decisions are arrived at and who is in charge of committing a possible rights violation.

Furthermore, the key undermining impact of broadening surveillance ability will be a chilling effect to the basic rights, which include freedom in speech and expression. The consciousness or awareness of constant surveillance can lead to people not practicing peaceful dissent and hence compromising democracy. Without effective legal protections and control methods, AI-driven surveillance is highly likely to fall into the wrong hands to be used against political or to discriminate against individuals.[239]

Thus, although the use of AI-supported surveillance promises are difficult to ignore, it presents high risks to privacy and civil liberties. This requires careful balancing the state interests and individual rights, and a system of law that would be the guaranty of transparency, accountability and the adherence to the constitutional premises.

2. UNDERSTANDING AI-POWERED SURVEILLANCE

The scope of AI-powered surveillance is a wide range of sophisticated technologies that deploy artificial intelligence and machine learning to gather, track, and assess human behavior with the use of big data analytics. In contrast to older surveillance solutions, which use manual surveillance and processing of limited amounts of data, AI-mediated solutions can analyze massive amounts of data in real-time and, thus, considerably increase the size, speed, and precision of surveillance activities.

Facial Recognition Systems (FRS) among the best technologies in this category applies biometric mapping in association to identity people by their facial features. Within such systems, they are actively used within the community in areas like the airport, aboard the railways, and even in urban areas, where the law enforcement agencies can identify the suspects as well as missing individuals. Nevertheless, issues have been blamed towards their accuracy especially concerning the racial and gender biases that may be present in the training data.

Predictive policing algorithms are another important aspect; predictive algorithms study the past crime data to predict possible offenses. Such systems help the authorities to distribute resources more effectively as they are able to detect high-risk regions and people. On the one hand, predictive policing can enhance crime prevention; on the other hand, it runs the risk of supporting the already existing biases in the criminal justice system, which causes discriminatory focusing on the marginalized communities.[240]

Another essential aspect of AI surveillance is smart CCTV systems and video analytics. These networks combine AI features with the existing closed-circuit television networks and enable

[238] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 180–185 (India).
[239] Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934, 1945–50 (2013).
[240] Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement 32–35 (N.Y.U. Press 2017).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 6 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

automated monitoring of suspicious behavioral patterns, crowd patterns, as well as real-time warnings. In contrast to traditional CCTV that may involve supervision of cameras by humans, AI-based systems can constantly process video feeds, thus making it possible to have extensive surveillance without any interruptions.

Moreover, it is showing biometric identification systems such as fingerprint identification, iris identification, and DNA profiling that are extensively utilized in the determination of identity and authentication of identity. Massive biometric databases like Aadhaar have also increased the range of surveillance in India where there is a connection of personal identity to various public and non-public services. Such systems, though efficient and helpful in service delivery, cause serious cracks on issues of data security, consent and possible misuse.[241]

All of these technologies are processing vast amounts of personal information to find patterns, discover abnormal behavior, and forecast actions. The combination of various data sources, such as social media, financial history, and the data on the geolocation allow forming detailed digital biographies of people. This is both advantageous in terms of governance and security, but it simplifies mass surveillance, which is exercised frequently, without the knowledge or significant consent of the individuals.

Such concerns are even aggravated by the fact that AI algorithms are opaque, which means that people usually do not know how their data is gathered, processed, and utilized. Such non-transparency harms the notion of accountability and asks some serious questions concerning the alternative of AI-based surveillance to democratic processes and basic rights.[242]

3. RIGHT TO PRIVACY; LEGAL FRAMEWORK.

3.1 India Happy constitutional protection.

In India, the right to privacy has developed over time due to judicial interpretation and is today bound as a fundamental right in Article 21 on the Constitution, which assures of right to life and personal liberty. The landmark case of Justice K.S. Puttaswamy (Retd.) v. Union of India was one of the major shifts in the law on the Indian constitution where the court ruled that privacy is fundamental to human dignity and autonomy.[243]

In this case, the Supreme Court has expressed that privacy is multidimensional, which encompasses bodily privacy, informational privacy and decisional autonomy. Noteworthy, the notion of the informational self-determination was acknowledged by the Court and it gave people the authority to manage their personal information. The ruling also put in place a three pronged test to any restriction to privacy namely, legality, necessity and proportionality.

This framework comes especially to the evaluation of AI-enhanced surveillance since the methods usually imply data gathering and processing at a large scale by the state. Any tools of surveillance should therefore be covered by law, have state purpose and must be reasonable in terms of the access they seek.

3.2 Data Protection Framework

Reacting to the increasing awareness of the issue of data privacy, in 2023 India adopted the Digital Personal Data Protection Act, 2023, aimed at regulating the processing of personal data, and aiding the accountability of data fiduciaries. The Act presents some of the most important principles in lawful processing, limitation of purposes, minimization of the data and user consent.[244]

The law has however faced criticism especially on the wide exemption cases which are given to

[241] Clare Garvie et al., The Perpetual Line-Up: Unregulated Police Face Recognition in America 18–22 (Geo. L. Ctr. on Privacy & Tech. 2016).
[242] Bernard E. Harcourt, Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age 67–72 (Univ. of Chi. Press 2007).
[243] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶ 3 (India).
[244] Digital Personal Data Protection Act, No. 22 of 2023, §§ 4–8 (India).

government agencies. These exemptions can enable the state to avoid some of its commitments, as it serves the objectives of national security, order and other stated reasons. According to critics, this kind of provision would even render the law weak and provide loopholes that allow unrestrained surveillance.

Moreover, enforcement mechanisms of the Act are still developing and there are still concerns about independence and effectiveness of regulatory authorities. With AI-based surveillance, there are no strict security measures and surveillance controls hence it poses a substantial threat to personal privacy.

3.3 International Perspective

On the global front, the legal frameworks involved in data protection and privacy include detailed laws like the General Data Protection Regulation, which stipulate high level of protection of data at the international level. The GDPR focuses on the following principles: transparency, accountability, purpose limitation, and subject privacy rights, in particular, the right to access, rectify, and erase the personal data.[245]

The emphasis on informed consent and on the accountability of algorithms, especially in the context of automated decision-making and profiling is one of the most significant aspects of the GDPR. It further requires the impact assessment of data protection of high-risk processing operations such as large scale surveillance.

In a comparison with these hearty structures, the data protection regime in India is at its infantile phase. Although the Digital Personal Data Protection Act, 2023 is a great approach, it does not have some of the protections that exist in international regimes, especially state surveillance and algorithmic transparency.[246]

The difference in the two systems shows that the emergence of AI-driven surveillance requires a dedicated approach in legal changes within India to eliminate the peculiarities of this process so that technological innovations were not the reason to overlook the basic rights.

4. AI SURVEILLANCE AND ITS CONSEQUENCES ON PRIVACY.

The aspect of privacy in the modern society is dramatically changed by the introduction of AI-enabled surveillance technologies, given the extent and specifics of this concept. A significant influence is the birth of mass surveillance, which allows ensuring the constant control over people both in the open and privately. Facial recognition systems are one of the technologies that governments can use to monitor the movements of people resulting in the removal of anonymity in the lives of people. Such a continuous monitoring is why it can result in what can be commonly termed as a surveillance state whereby people are always under the scrutiny of the authorities thus putting into jeopardy the age-old expectation of privacy.[247]

Along with conducting mass surveillance, AI systems allow gathering and profiling numerous data. These systems combine personal information obtained through various means, such as biometric databases, web activities, financial operations, and geolocation information among others to create comprehensive behavioral profiles of individuals. These profiling technologies pose a profound concern on unauthorized use of data, data leakage and discrimination. Bias or partial data used to selectively execute an algorithmic decision-making process can disproportionately impact less privileged groups, resulting in unequal treatment and institutional discrimination.

The other disastrous impact of AI-driven surveillance is that it sends a chilling effect on basic liberties. The fear of being watched all the

[245] Regulation (EU) 2016/679 of the European Parliament and of the Council, arts. 5–6, 2016 O.J. (L 119) 1 (General Data Protection Regulation).
[246] Apar Gupta & Raman Jit Singh Chima, The Personal Data Protection Bill and the Future of Privacy in India, 13 Indian J.L. & Tech. 1, 15–18 (2017).
[247] Shoshana Zuboff, The Age of Surveillance Capitalism 93–101 (PublicAffairs 2019).

time may make people not exercise their right to freedom of speech and expression, choice on whether to protest or to assemble. This process undermines the act of democracy because it precludes opposing the system and encourages free speech. Fears of being surveilled may cause individuals to self-censure their actions, views, and relationships and inhibit the vitality of democratic societies.[248]

Moreover, the lack of strong regulatory frameworks and mechanisms of monitoring and supervision escalates chances of misuse and abuse of surveillance technologies. Artificial intelligence devices can be used to spy on the political activities, discriminate against any opposition, activists or a particular community. Having all the surveillance in the hands of the state with no sufficient checks and balances poses the risk of arbitrary and disproportionate interference with individual rights. Lack of transparency in algorithmic processes also makes accountability a bit more problematic, as it is hard to challenge or question regimes of surveillance.

5. JUDICIAL APPROACH AND CASE LAWS

The Indian courts have had a leading influence in making the judicial discourse of privacy, and surveillance. The Supreme Court, in Justice K.S. Puttaswamy (Retd.) v. Union of India,[249] clearly adopted the right to privacy as a right given under the Constitution and under Art 21, the Supreme Court had clarified that the right to privacy was based on the fundamental rights. The Court stressed that privacy entailed informational self-determination and defense against random invasion by the state and thus provided the constitutional foundation of considering surveillance measures.

The Court had earlier on in the case of People's Union for Civil Liberties (PUCL) v. Union of India dealt with the problem of telephone tapping and specifying the procedures that had to be adhered to in order to guard against the misuse of surveillance activities. It believed that a violation of privacy was supposed to be justified in law and must follow the principles of necessity and proportionality.[250]

Equally, in the case of Anuradha Bhasin v. Union of India, the Supreme Court affirmed the relevance of proportionality and necessity in limiting fundamental rights especially in the case of internet shutdowns. The decision reinforced the idea that restraint should be on a case by case, temporary and reviewable by the courts.[251]

All these judicial declarations indicate the necessity of procedural protection, openness, and responsibility of surveillance practices. They determine that the surveillance, even that involving AI, should be conducted according to the constitutional standards and comply with the basic rights.

6. PROBLEMS IN GOVERNING AI SURVEILLANCE.

Surveillance operated by AI is a complicated issue that cannot be regulated by means of a unified legal system for such technologies. Current legislation may fail to provide sufficient means to address the complexity of AI systems and create loopholes and lack of clarity. This ambiguity raises the question of the legality and bounds of practices of surveillance.[252]

The technological complexity and opacity of AI systems can serve as another significant obstacle. Numerous AI algorithms act as black boxes, i.e., the process of decision making cannot be readily comprehended even by professionals. Such lack of transparency does not ensure accountability and fairness in the usage of such systems, especially in situations that require such systems in sensitive fields like law enforcement and national security.

These concerns are also compounded by lack of adequate mechanisms of oversight. To

[248] Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934, 1940–45 (2013).
[249] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, ¶¶ 180–185 (India).
[250] People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 S.C.C. 301 (India).
[251] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
[252] Andrew Guthrie Ferguson, The Rise of Big Data Policing 45–50 (N.Y.U. Press 2017).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 6 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

regulate effectively, independent supervising bodies should be in place where the bodies have the power to monitor, audit and review the surveillance activities. Nevertheless, these mechanisms are in most instances either too feeble or do not exist at all and the surveillance practices are allowed to proceed without being closely examined.[253]

Lastly, there is the natural conflict between the national security and individual privacy goals. On one hand, surveillance is somehow reasonable due to the security and the maintenance of the order within society; on the other hand, however, the uncontrolled and unregulated extension of surveillance may result in imbalanced disruption of the inherent rights. One of the most complicated issues with the regulation of AI-powered surveillance is to find a balance between these competing interests.

7. RECOMMENDATIONS

7.1 Enactment of Comprehensive Surveillance Law

India needs a specific, thoroughly built and strongly enforced system of law regarding surveillance, especially that of artificial intelligence. Currently, surveillance is controlled by the disjointed and obsolete legislations that fail to effectively adjust to the advances of contemporary AI-based innovations. The use of surveillance through special tools should be in a specific law that has clear scope and limits whose application is under the constitution. It must include this protection against arbitrariness or overuse of surveillance through prior authorization, necessity, proportionality, and periodic review.

7.2 Strengthening Data Protection Laws

Digital Personal Data Protection Act, 2023 is a step towards securing personal information in India; nevertheless, it needs reinforcement to ensure it impacts the problem of AI-established surveillance. Specifically, the general exemptions that have been extended to government agencies need to be tightened so as to avoid abuse. This law must have more specifics on data minimization, purpose limitation, and accountability and provide clear solutions to individuals in incidents of data breach or unjustified surveillance. Effective enforcement also requires increasing the self-reliance and ability of regulatory authorities.

7.3: Judiciary and parliamentary control.

The existence of stringent supervision systems is essential in making sure that surveillance authorities are used in a responsible manner. There should be independent surveillance oversight capacities like the judicial and parliamentary committees, which can review and scrutinize the surveillance practices. Judicial checks and balances, especially, can serve to curb capricious state conduct, by necessitating a prior justification of intrusive surveillance practices. Transparency and improving the democratic accountability can also be promoted by parliamentary scrutiny so that surveillance policies can be debated and reviewed.

7.4 Transparency and Accountability

Animal legitimacy of any system of surveillance includes transparency. The authorities should inform why, how, and how far surveillance technologies are used to the best of their ability without exposing national security. The accuracy, fairness, and legal standards of the AI systems should be audited regularly to measure the suitability of the systems. The use of public reporting mechanisms and independent audits can be used to create trust and safeguard against misuse of surveillance practices. Moreover, people must be allowed to demand information and query illegitimate surveillance measures.

7.5 Ethical AI Principles Adoption.

Ethical considerations should also control the manufacture and implementation of AI systems, which should be restricted to uphold privacy, fairness, and non-discrimination. The

[253] Tal Z. Zarsky, Transparent Predictions, 2013 U. Ill. L. Rev. 1503, 1510–12 (2013).

algorithms applied by AI must be created in a way that they propose the least amount of bias and guarantee fair results in the various facets of society. Should this default to unscrupulous folks, ethical AI systems must require explainability, responsibility and human control over the process of decision-making. With these principles incorporated into the design and deployment of AI, one can harmonize the technical innovation with the primary rights and democratic ideals.

8. CONCLUSION

AI surveillance is a critical and revolutionary solution to the contemporary governing practices and can bring a lot of value in terms of security, effectiveness, and governmental management. It also poses, however, serious threats to privacy protection and civil liberties. The fact that AI systems manage to gather, process, and process large volumes of personal data has changed the equilibrium between the power of states and the autonomy of individuals in fundamental ways.

Privacy is continually understood as a basic right in Justice K.S. Puttaswamy (Retd.) v. Union of India, as one measure of protecting individual freedom in the wake of technological progress. It stipulates that privacy violation should be reasonable, reasonable, and supported by law. It is this constitutional frame that offers a fundamental yardstick to assess the validity of AI-driven practices of surveillance.

Going forward, India needs to implement a powerful and an all inclusive legal and regulatory framework that would provide power of surveillance technologies to be used in a responsible and constitutional manner. This incorporates enhancing data protection legislations, creation of effective supervision, fostering transparency and responsibility. Simultaneously, the raised ethical issues should inform the creation and implementation of AI solutions to avoid discrimination and safeguard human dignity.

As it is, the task that lies ahead is to explore a fine line between using the advantages of AI-driven surveillance to serve the common good, and retain basic rights that have been at the core of a democratic society. Such a balance is the key to the successful achievement of the principle of individual freedom and privacy in the digital age that is not to be achieved at the cost of the technical advancements.