



AI Surveillance and the Right to Privacy: Balancing National Security and Article 21 of the Constitution

Lakshya Verma,

PhD Scholar at Graphic Era university, Dehradun

How to Cite this Article:

Verma, L. (2026). AI Surveillance and the Right to Privacy: Balancing National Security and Article 21 of the Constitution. International Journal of Creative and Open Research in Engineering and Management, <i>02</i>(9), 1-9. <https://doi.org/10.55041/ijcope.v2i9.116>

License:

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.



<https://doi.org/10.55041/ijcope.v2i9.116>

Abstract

The deployment of artificial intelligence in State surveillance, ranging from automated facial recognition to predictive policing analytics and communication-interception software, has outpaced the constitutional and statutory framework designed to govern it. This article critically examines the tension between the right to privacy, recognised as intrinsic to Article 21 of the Constitution of India in Justice K.S. Puttaswamy v. Union of India, and the State's invocation of national security to justify AI-enabled monitoring of citizens. It traces the statutory basis for interception and surveillance under the Indian Telegraph Act, 1885, the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, arguing that each contains broad executive exemptions that were framed before artificial intelligence made mass, continuous and predictive surveillance technically and economically feasible. The article evaluates the judiciary's proportionality doctrine as applied in Puttaswamy, the Aadhaar judgment, Anuradha Bhasin, and the Pegasus spyware proceedings in Manohar Lal Sharma v. Union of India, and finds that while the doctrine offers a sound analytical framework, its enforcement against opaque, AI-driven and classified surveillance systems remains weak. Drawing a brief comparison with the European Union's risk-based regulatory approach and the United States' judicial and statutory responses to algorithmic policing, the article identifies structural gaps, the absence of an independent authorisation mechanism, the lack of algorithmic

transparency, and the non-existence of a dedicated surveillance reform law, that leave Article 21 vulnerable in the age of artificial intelligence. It concludes with recommendations for a purpose-specific surveillance statute, independent oversight, and algorithmic accountability standards suited to the Indian constitutional order.

Keywords

Artificial intelligence; surveillance; right to privacy; Article 21; national security; facial recognition; Puttaswamy; proportionality; Digital Personal Data Protection Act; predictive policing.

I. Introduction

Artificial intelligence has transformed the technical capacity of the State to observe, identify, and predict the conduct of its citizens. Where surveillance once required the deployment of human resources to intercept a specific communication or follow a specific individual, contemporary tools, automated facial recognition systems, algorithmic analysis of communications metadata, predictive policing software, and commercially procured spyware capable of infiltrating a personal device without any action by its owner, allow the State to monitor populations at a scale and granularity that was not technically conceivable when India's surveillance statutes were first enacted. The Indian Telegraph Act, 1885 and the Information Technology Act, 2000 were drafted for a world of discrete, targeted interception; they were not designed to regulate a world in which a single facial recognition deployment can process the biometric data of an entire crowd, or in which spyware can extract the complete digital life of a target without a physical search.



This mismatch between technological capability and statutory design assumes constitutional significance because the Supreme Court of India, in Justice K.S. Puttaswamy (Retd.) v. Union of India, unanimously held that the right to privacy is intrinsic to the right to life and personal liberty under Article 21, and that any State action infringing this right must satisfy a threefold, later elaborated as a four-pronged, test of legality, legitimate aim, necessity and proportionality. The judgment was widely read as a foundational check on unregulated State surveillance. Yet the practical experience of the years since Puttaswamy, including the Pegasus spyware controversy, the expansion of facial recognition deployment by police forces, and the wide national-security exemptions carved into the Digital Personal Data Protection Act, 2023, suggests that the constitutional promise of Puttaswamy has not been matched by a corresponding statutory or institutional architecture capable of disciplining AI-enabled surveillance.

This article examines that gap. Part II sets out the constitutional foundation of the right to privacy and the proportionality standard that governs its restriction. Part III surveys the statutory and regulatory framework presently governing surveillance in India. Part IV describes the principal forms of AI-enabled surveillance now in use or contemplated by Indian authorities. Part V examines the judicial response to date, including the Pegasus proceedings. Part VI critically interrogates the invocation of national security as a justification for AI surveillance. Part VII offers a brief comparative perspective. Part VIII identifies implementation challenges, and Part IX offers recommendations, before Part X concludes.

II. Constitutional Foundations: Article 21 and the Right to Privacy

The constitutional status of privacy in India has evolved considerably since independence. Early decisions such as *M.P. Sharma v. Satish Chandra* and *Kharak Singh v. State of Uttar Pradesh* had either declined to recognise a fundamental right to privacy or recognised it only partially, reflecting a more restrained, positivist reading of the Constitution. This position was decisively overturned by a nine-judge Bench in Justice K.S. Puttaswamy (Retd.) v. Union of India, which held unanimously that privacy is a constitutionally protected right, an intrinsic part of the right to life and personal liberty guaranteed under Article 21, and of the freedoms guaranteed under Part III of the Constitution more generally. The Court described privacy as encompassing bodily autonomy, informational self-determination, and decisional autonomy, and held that the right, while not absolute, could only be restricted by a law that satisfies the requirements of legality, a legitimate State aim, and proportionality between the means adopted and the object sought to be achieved.

The proportionality standard articulated in Puttaswamy, and refined in subsequent decisions such as the Aadhaar judgment and *Anuradha Bhasin v. Union of India*, requires, at minimum, that any privacy-restricting measure pursue a legitimate goal, that it be a suitable means of achieving that goal, that no less restrictive but equally effective alternative be available, and that the measure not have a disproportionate impact on the right holder relative to the benefit secured. Indian courts have, in principle, accepted that this standard applies with equal force to surveillance measures undertaken in the name of national security, since the Court in Puttaswamy itself, and again in the Pegasus proceedings, cautioned that the State cannot claim automatic immunity from constitutional scrutiny merely by invoking national security. The difficulty, examined further below, lies not in the articulation of the standard but in its application to surveillance systems whose existence, scope and technical operation the State is frequently unwilling to disclose even to a reviewing court.

III. Statutory and Regulatory Framework Governing Surveillance

A. *The Indian Telegraph Act, 1885*

Interception of communications in India traces its statutory origin to Section 5(2) of the Indian Telegraph Act, 1885, which permits the Central or State Government to intercept messages in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, or the prevention of incitement to an offence, and only in the occurrence of a public emergency or in the interest of public safety. In *People's Union for Civil Liberties v. Union of India*, the Supreme Court, while upholding the constitutional validity of Section 5(2), held that the provision did not confer unguided or unbridled power and read into it a set of procedural safeguards, including that interception be authorised only by an order of the Union or State Home Secretary, that such orders be time-bound and subject to periodic review, and that a review committee examine the legality of interceptions. These safeguards were subsequently codified in Rule 419A of the Indian Telegraph Rules, 1951.



B. The Information Technology Act, 2000

The Information Technology Act, 2000 extends a broadly similar interception and monitoring power to electronic communications and computer resources through Section 69, which allows the Central or State Government to direct the interception, monitoring or decryption of information on comparable grounds to those in the Telegraph Act, and through Section 69A and 69B, which separately empower the blocking of public access to information and the monitoring of traffic data. The safeguards attached to these powers are executive rather than judicial in character: authorisation rests with a designated competent authority within the executive, and review is conducted by a review committee that is itself constituted by the executive, rather than by an independent judicial or quasi-judicial body. Neither Section 69 of the Information Technology Act nor the Rules framed under it were drafted with AI-enabled analytics in mind, and neither provision distinguishes between the targeted interception of a single individual's communications and the algorithmic analysis of bulk communications metadata, a distinction of considerable constitutional significance once AI tools make bulk analysis technically trivial.

C. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 is the first comprehensive data protection statute enacted in India, and its Section 17 is directly relevant to AI-enabled State surveillance. Section 17(1)(a) exempts the processing of personal data by any person notified by the Central Government where such processing is necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, the maintenance of public order, or the prevention of incitement to a cognizable offence connected with any of these. Section 17(2)(a) goes further, empowering the Central Government to exempt any instrumentality of the State from the application of the entire Act, rather than merely from specified obligations, through executive notification, on the same broad grounds. Because the Act's core protections, including the requirement of consent, purpose limitation, and data minimisation, are precisely the protections most relevant to constraining AI-driven profiling and predictive analytics, an exemption of this breadth substantially narrows the statute's relevance to the AI surveillance systems that most urgently require regulation.

IV. AI-Enabled Surveillance Technologies in Practice

A. Automated Facial Recognition

The National Crime Records Bureau has pursued the development of a nationwide Automated Facial Recognition System intended to allow police stations across the country to compare images, drawn from sources such as closed-circuit television footage, against a centralised database for the stated purposes of identifying criminals, missing persons and unidentified bodies. Facial recognition technology has also been deployed by State and city police forces for specific operational purposes, including the identification of missing children and the securing of large public gatherings. Commentators have observed that facial recognition technology presently operates in India without any dedicated legislative framework specifically authorising or regulating its use, its deployment instead resting on general policing powers and executive approval, a gap that leaves the purpose limitation, accuracy standards, retention periods and grievance-redressal mechanisms that would ordinarily accompany a biometric identification system largely undefined.

B. Predictive Policing and Communications Analytics

Several Indian State police forces have piloted or adopted predictive policing tools that use historical crime data to forecast the likelihood of offences in particular localities, and law enforcement and intelligence agencies increasingly rely on communications-metadata analytics that use algorithmic pattern recognition rather than the interception of the content of any single communication. These tools raise distinct constitutional concerns from those addressed by the Telegraph Act and the Information Technology Act, since their output is a probabilistic inference about a place or a person rather than the interception of a specific communication, and the existing authorisation framework, built around discrete interception orders, is not well suited to authorising or reviewing an ongoing algorithmic process applied to bulk data.



C. Commercial Spyware

The most consequential recent controversy concerning AI-adjacent surveillance in India has concerned the alleged use of Pegasus, a spyware product developed by the Israeli firm NSO Group and capable of infiltrating a target's mobile device without any action on the part of the user, granting access to stored data, live communications, camera and microphone. International reporting in 2021 indicated that a substantial number of Indian mobile numbers, including those of journalists, politicians, and civil society figures, appeared on a list of possible surveillance targets. The Union Government neither confirmed nor denied the use of the software, instead invoking national security in response to petitions before the Supreme Court, a response examined further in Part V.

V. The Judicial Response: Proportionality and Pegasus

The petitions concerning the alleged use of Pegasus spyware, consolidated in *Manohar Lal Sharma v. Union of India*, gave the Supreme Court its most direct opportunity to date to test the boundary between national security and the right to privacy against an AI-adjacent surveillance technology. The Union Government's response before the Court was, notably, to file a limited affidavit that neither confirmed nor denied the deployment of the software, citing national security concerns. The Supreme Court, by order dated 27 October 2021, declined to accept that a bare invocation of national security could foreclose judicial scrutiny, holding that the State cannot, by merely raising the spectre of national security, obtain a free pass from judicial review whenever citizens complain of a violation of their fundamental rights. The Court instead constituted an independent Technical Committee, supervised by a former judge of the Supreme Court, to examine the allegations. The Committee, upon examining a sample of devices, found malware on some of them but was unable to conclusively confirm the presence of Pegasus specifically, and separately noted an absence of cooperation from the Union Government with its inquiry.

The Pegasus proceedings illustrate both the strength and the limitation of the proportionality doctrine as a check on AI-enabled surveillance. On one hand, the Court firmly rejected the proposition that national security operates as a talismanic exemption from constitutional scrutiny, reaffirming the legality and necessity limbs of the *Puttaswamy* standard. On the other hand, the proceedings also demonstrate the practical difficulty of applying that standard where the State declines to disclose whether a surveillance technology has been procured or deployed at all: a proportionality inquiry cannot meaningfully assess the necessity or the least-restrictive-alternative character of a measure whose very existence is not admitted. This evidentiary asymmetry is a structural feature of AI and spyware-based surveillance that traditional interception law, built around a discrete, admitted order to intercept a specific line, did not have to confront.

VI. National Security Claims and Their Limits

National security is unquestionably a legitimate aim capable of justifying restrictions on the right to privacy; the difficulty lies not in the legitimacy of the aim but in the tendency of the concept to expand, in practice, well beyond matters that would ordinarily be understood as touching the sovereignty, integrity or external security of the State. The Supreme Court in *Anuradha Bhasin v. Union of India* cautioned against the reflexive invocation of national security to justify sweeping restrictions on fundamental rights, insisting that the State provide the reviewing court with a factual basis for the restriction rather than a bare assertion of necessity. Applied to AI surveillance, this caution has particular force, because AI systems are frequently justified by reference to diffuse and anticipatory goals, the prevention of unspecified future offences, the general maintenance of public order, the identification of unnamed persons of interest, rather than the investigation of a specific, already-suspected offence. A surveillance measure justified by reference to a diffuse and perpetually renewable goal is structurally difficult to subject to the necessity and least-restrictive-alternative limbs of the proportionality standard, since there is no discrete objective against which the measure's necessity can be tested.

A related concern is the breadth of Section 17(2)(a) of the Digital Personal Data Protection Act, 2023, which permits the Central Government to exempt an entire instrumentality of the State from the Act through executive notification, without requiring a demonstrable, case-specific nexus between the exempted processing and the stated security objective, and without the kind of independent, judicially supervised authorisation mechanism that the Supreme Court read into the Telegraph Act in the *PUCL* case. Where a facial recognition system, a predictive policing tool, or a



communications-analytics platform operates within an exempted instrumentality, the statutory protections of consent, purpose limitation and data minimisation, precisely the safeguards most relevant to AI-driven profiling, cease to apply, and the individual is left to rely solely on the constitutional proportionality standard, enforceable only through the comparatively slow and resource-intensive mechanism of writ litigation.

VII. Comparative Perspective

The European Union has adopted a risk-based regulatory approach to artificial intelligence through the Artificial Intelligence Act, which classifies real-time remote biometric identification systems used by law enforcement in publicly accessible spaces as a high-risk, and in most circumstances prohibited, use of AI, permitting narrow exceptions, such as the search for specific victims of crime or the prevention of a specific and imminent terrorist threat, only subject to prior judicial or independent administrative authorisation. This *ex ante*, case-specific authorisation requirement stands in contrast to the Indian position, where facial recognition deployment presently rests on general executive and policing authority rather than on any dedicated statutory permission tied to a specific, judicially reviewed purpose.

In the United States, the regulation of AI-enabled surveillance has developed unevenly, primarily through State and municipal legislation restricting or banning the use of facial recognition by local police departments, and through constitutional litigation under the Fourth Amendment addressing the circumstances in which the warrantless collection of location and communications data constitutes an unreasonable search. The United States Supreme Court's recognition, in cases addressing the compelled disclosure of cell-site location data, that the sheer comprehensiveness and retrospective reach of digitally generated records can itself trigger constitutional protection, offers an instructive parallel to the Indian proportionality inquiry, since it demonstrates a comparable judicial concern with the aggregate, rather than merely the individual, privacy impact of a surveillance capability enabled by automation.

What both jurisdictions share, and what the Indian framework presently lacks, is a mechanism that treats the scale and automation of a surveillance technology as itself a factor relevant to the intensity of the safeguards required, rather than treating AI-enabled surveillance as simply an incremental extension of traditional, individually targeted interception.

VIII. Implementation Challenges

A. Absence of Independent Authorisation

Authorisation for interception under both the Telegraph Act and the Information Technology Act rests with the executive branch, and review is likewise conducted by an executive review committee rather than an independent judicial or quasi-judicial authority. No comparable authorisation mechanism presently exists for facial recognition deployment or predictive policing analytics, which are typically approved through internal police or executive procurement processes rather than any statute specifically directed to their use.

B. Algorithmic Opacity

AI surveillance systems, particularly facial recognition and predictive policing tools, are frequently procured from private vendors under commercial arrangements that treat the underlying model, training data, and accuracy metrics as proprietary. This opacity makes it difficult for an affected individual, or even a reviewing court, to assess the reliability of a system's output, including its documented tendency, observed in comparable systems internationally, to exhibit higher error rates for certain demographic groups, a concern with direct implications for the equality guarantee under Article 14 as well as for Article 21.

C. Absence of Notification and Redress

Persons subjected to interception, facial recognition matching, or algorithmic profiling are, as a rule, never notified that they have been monitored, whether or not the monitoring results in any adverse action. Without notification, the practical ability of an individual to invoke judicial review, whether under the proportionality standard or otherwise, is severely constrained, since a right of challenge is of limited value if the affected person has no means of learning that the right has been engaged.



D. Fragmented Legal Basis

AI surveillance in India presently operates under a patchwork of general statutory powers, the Telegraph Act, the Information Technology Act, ordinary policing statutes, and executive procurement decisions, none of which was drafted with automated, continuous, or predictive surveillance in mind. This fragmentation makes it difficult to identify a single, coherent statutory standard against which the legality limb of the proportionality test can be applied to any given AI surveillance deployment.

IX. Recommendations

The following measures would help align India's surveillance framework with the constitutional standard articulated in Puttaswamy and its progeny.

- Enactment of a dedicated surveillance reform statute, replacing the executive-authorisation model of the Telegraph Act and the Information Technology Act with a requirement of prior authorisation by an independent judicial or quasi-judicial authority for any surveillance measure, including AI-enabled measures, that is more than momentary or narrowly targeted.
- A specific statutory framework for facial recognition and biometric surveillance, modelled on the case-specific, ex ante authorisation requirement found in comparable jurisdictions, restricting real-time biometric surveillance in public spaces to narrowly defined and independently authorised purposes.
- Narrowing of Section 17(2)(a) of the Digital Personal Data Protection Act, 2023 to require a demonstrable, purpose-specific nexus between any exemption granted to a State instrumentality and the security objective relied upon, rather than a blanket, Act-wide exemption.
- Mandatory algorithmic audit and accuracy-reporting requirements for any AI system procured for surveillance or predictive policing purposes, with independent verification of demographic error rates before deployment.
- A statutory notification mechanism allowing individuals to learn, after a reasonable delay where operationally necessary, that they were subject to interception or algorithmic surveillance, so as to make the right of judicial challenge practically meaningful.
- Regular, published reporting on the volume and categories of AI surveillance measures undertaken, analogous to transparency reporting practices in other democracies, to enable meaningful parliamentary and public oversight.

X. Conclusion

The recognition of privacy as intrinsic to Article 21 in Puttaswamy stands as one of the most significant developments in modern Indian constitutional law, and the proportionality standard it articulated remains, in principle, well suited to disciplining State surveillance, including surveillance conducted through artificial intelligence. The difficulty is that the statutory and institutional architecture surrounding that standard, an executive-authorised interception regime under the Telegraph Act and the Information Technology Act, and a data protection statute whose broadest exemptions apply precisely to the State surveillance activities most in need of oversight, was not designed with automated, continuous and predictive surveillance in mind, and has not been substantially reformed to meet it. The Pegasus proceedings demonstrated both the judiciary's willingness to reject a bare invocation of national security and its practical difficulty in enforcing the proportionality standard against a State unwilling to admit the existence of a surveillance capability. Bridging this gap will require legislative, not merely judicial, action: an independent authorisation mechanism, algorithmic transparency requirements, and a narrower conception of the national-security exemption are all necessary if the constitutional guarantee recognised in Puttaswamy is to retain practical force in an era in which surveillance is increasingly automated, continuous and difficult to detect.



References

- The Constitution of India, 1950, arts. 14, 19, 21.
- The Indian Telegraph Act, 1885, s. 5(2).
- The Indian Telegraph Rules, 1951, r. 419A.
- The Information Technology Act, 2000, ss. 69, 69A, 69B.
- The Digital Personal Data Protection Act, 2023, s. 17.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar), (2019) 1 SCC 1.
- People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
- Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
- Manohar Lal Sharma v. Union of India, 2021 SCC OnLine SC 985.
- Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
- Modern Dental College and Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council (Artificial Intelligence Act).
- National Crime Records Bureau, Ministry of Home Affairs, Government of India, Request for Proposal for the Automated Facial Recognition System.
- PRS Legislative Research, “FAQs on Telephone Tapping.”