INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ALGORITHMIC SURVEILLANCE AND THE RIGHT TO PRIVACY IN INDIA: A CONSTITUTIONAL ANALYSIS

AUTHORED BY - NIDA KHATOON
Student: LLM
Amity Law School, Lucknow
Amity University Lucknow

CO-AUTHOR - DR. RAJEEV KUMAR SINGH
Assistant Professor of Law
Amity Law School Lucknow,
Amity University Uttar Pradesh Lucknow Campus

Abstract

High rates of adoption of artificial intelligence and data-driven technologies in the State government have changed the surveillance practices in India, with significant constitutional implications. The algorithmic surveillance systems, including but not limited to biometric identification and facial recognition, predictive policing and data profiling, make it possible to provide extensive surveillance coverage of people in real-time and at almost all times, and remain hidden. The paper will provide a constitutional review of algorithmic surveillance in India, to explore how the practice has impacted the basic right to privacy in Article 21 of the Constitution. It follows the history of the development of privacy jurisprudence where in the early days of judicial reticence, privacy was fully acknowledged and recognized as a primary right in Justice K.S. Puttaswamy v. Union of India. The paper examines the modern surveillance in relation to the Aadhaar-based governance, facial recognition systems, and emergency surveillance and assesses it against the constitutional principles of legality, necessity, proportionality, and procedural protections. It also notes major hurdles of algorithmic opacities, data storage, discrimination, and the chilling effect on the basic liberties. The paper examines the best practices in the regulation of surveillance technologies by comparing the United States and the European Union. The paper concludes that the current legal framework in India is insufficient to mitigate the constitutional risks of algorithmic surveillance and suggests that a comprehensive surveillance law should be enacted and should be based on transparency, accountability, and rights-centric design to bring about balance between national security and individual liberties in the digital era.

ISSN: 2582-6433

Keywords

Algorithmic Surveillance; Right to Privacy; Article 21; Artificial Intelligence; Constitutional Law; Digital Governance; India

1. Introduction

1.1 Background and Context

The emergence of digital governance in India is so fast that it has altered the dynamics between the State and citizens and changed the concept of how they interact significantly. In recent years, the Indian government progressively has been using the technology-oriented systems in administration, law response, welfare service, and national security. Differing digital platforms like Aadhaar, face recognition systems, crime analytics systems, and data aggregation systems on a large scale have taken center stage in the social administration. As much as these technologies offer efficiency, accuracy and provision of better services, it has equally increased the ability of the State to track, gather and analyse personal information at a larger scale than was ever before.

The surveillance in India was traditionally very manual and focused where human intervention and physical supervision were necessary[1]. Nevertheless, as artificial intelligence (AI), machine learning, and automated decision-making are integrated, surveillance practices have developed into being automated, continuous, and predictive[2]. The technologies can allow the State to not only monitor the past behaviour but also predict future behaviour based on data profiling and pattern recognition. Consequently, surveillance has ceased to be reactive but proactive, and this posed enormous constitutional issues on the privacy, autonomy and individual freedom. The proliferation of the State power via algorithmic tools is therefore a major threat to constitutional restraints on the executive power in a democratic society.

1.2 Conceptualising Algorithmic Surveillance

The concept of algorithmic surveillance is the application of automated mechanisms and computational algorithms to gather, process, and analyse data and monitor individuals or groups. As opposed to traditional surveillance which requires human eyes on the target,

[1]Khamroi A, Shrivastava A. Analysing the practical implications of a right to privacy: State surveillance and constitution.

[2]Bala J, Arora A. An Analysis of Surveillance and Data Protection with Reference to the Right to Privacy. Part 2 Indian J. Integrated Rsch. L.2022;2:1.

ISSN: 2582-6433

algorithmic surveillance is based on huge data, forecasting systems and non-transparent decision-making. It does not only limit itself to data collection but also to profiling, behavioural prediction, and risk assessment without the awareness andapproval of the individuals involved.

The surveillance can be algorithmic and can be divided into "mass, targeted and predictive. Mass surveillance is the indiscriminate gathering of information about masses of people, usually by biometric data stores or communication logs or location tracking. Targeted surveillance, on the contrary, is devoted to particular persons or groups according to the determined criteria, typically supported by the reasons of national security or law enforcement[3]. The most invasive surveillance is predictive or profiling where algorithms use previous actions to predict future behaviour, categorise individuals as possible threats and affect administrative or policing actions. This type of surveillance entails causing real constitutional alarms because of the use of probabilistic judgment, possible favoritism and transparency.

1.3 Research Problem

The growing use of algorithmic surveillance within India poses a basic constitutional challenge of whether the current legal and constitutional provisions are sufficient to secure the right to privacy in the face of scientifically advanced State surveillance. Even though the Supreme Court of India has acknowledged privacy as a basic right in the Art. 21, the usage of the right in algorithmic and AI-based surveillance has not been developed extensively. Lack of an overall law on surveillance and executive discretion and little checks and balances, leave a regulatory vacuum. The paper thus explores the argument of whether existing constitutional principles and legislative frameworks are adequate to meet the particular demands of algorithmic surveillance or need to be reassessed and reformulated substantively.

1.4 Research Questions

- Does Article 21(right to privacy) of the constitution of the country apply to algorithmic surveillance?
- Are the current legal systems constitutionally sufficiently covered?
- What should the constitutional doctrine play in an algorithmic form of governance?

[3]Dutt R. AI and the Right to Privacy-Balancing Innovation with Constitutional Protections. LawFoyer Int'l J. Doctrinal Legal Rsch..2025;3:920.

ISSN: 2582-6433

1.5 Objectives of the Study

- *In order to take into consideration constitutional standard.*
- *To investigate judicial responses.*
- *To suggest safeguards*

1.6 Research Methodology

The current research uses a doctrinal and analytical research design as the research topic is the constitutional provisions, court rulings, legislative acts, and research literature. An analysis of the case law is done in detail and it attempts to trace the history of the right to privacy and judicial review of surveillance activities in India. The study also utilizes a comparative constitutional method, relying on examples of other jurisdictions, including the United States and the European Union, to establish the optimal ways of regulating the use of algorithms in surveillance. This approach allows critically evaluating the constitutional system in India and makes it possible to develop well-informed suggestions on how to protect privacy in the digital era.

2. Understanding Algorithmic Surveillance: A Theoretical Framework

2.1 Meaning and Characteristics

For the purpose of governing, securing or administering people or groups, algorithmic surveillance, which involves automated computational systems to monitor, collect, process, and analyse data about individuals or groups, is used[4]. As compared to the old surveillance mechanisms which human eyes and discrete monitoring are used, algorithmic surveillance uses artificial intelligence, machine learning, and data analytics to produce insights, predictions and classifications. Such systems are infiltrating the decision-making in law enforcement, in the administration of the state, and in national security, but usually without human intervention.

Automation is a characteristic of algorithmic surveillance. The algorithms which are trained on the large datasets carry out surveillance decisionsincluding suspect identification, anomaly flagging, or risk profile determination. This lessens human discretion yet at the same time it does not leave human judgment, empathy and contextual reasoning to be applied to critical decisions that pertain to fundamental rights. Automation also facilitates continuous and continuous surveillance, as a result, monitoring is pervasive and not episodic.

[4]Mishra M. A Critical Analysis of the Right to Privacy. Issue 5 Indian JL & Legal Rsch..2022;4:1.

ISSN: 2582-6433

The other important feature is that of opacity which is often termed as black-box decision making. Algorithms used by many systems are either proprietary, complex or self-learning and even authorities find it challenging to explain the way results are generated comprehensively. People who are the subject of this kind of surveillance do not even have access to a way to know, question, or alter the algorithmic decision[5]. This lack of transparency weakens transparency, accountability and procedural fairness which are fundamental ideals of constitutional governance.

The breadth and rate of algorithmic surveillance also makes it unique as compared to conventional approaches. Such systems have the capacity to work with huge volumes of data at real time, tapping into various sources of information including biometrics, metadata of communications, location tracking and internet activity. The capability to monitor large groups of people at the same time is a qualitative change in State power that can be seriously worried about proportionality and excess in the context of constitutional democracy.

2.2 Types of Algorithmic Surveillance

There are different types of algorithmic surveillance, and each of them has a specific constitutional implication. Facial recognition technology (FRT) is one of the most well-known ones, because it identifies or authenticates people through the analysis of facial features based on the biometric data. FRT has been implemented in India by police departments to monitor crowds, identify crimes, and keep the population in order[6]. Although it is offered as a means to efficiency and security, facial recognition makes real-time recognition and tracking of people in a populated area possible, frequently without statutory permission or others informed consent.

Predictive policing algorithms are another important type and are based on historical crime data to predict the possible act of crime or people who are considered to be likely offenders. They are systems that are employed to distribute the police resources or increase surveillance in a specific location or community. Predictive policing is associated with anxieties about strengthening the existing biases because the algorithms trained on the historically skewed data are likely to focus more on the marginalised or over-policed populations, reinforcing the existing structural imbalance.

[5]Sonkar A. “Automated State Action in India: Administrative Justice, Privacy and Constitutional Accountability.
[6]Goel S. Right to Privacy: A Critical Analysis. Issue 3 Int'l JL Mgmt. &Human..2021;4:2117.

ISSN: 2582-6433

A less overt but much more invasive type of surveillance is metadata and behavioural profiling. Even without looking at the content, metadata, including call history, location data, surfing history, and payment history can tell a lot about the life of a particular person. Such data can be analysed algorithmically to give the State a detailed behavioural profile so that they can monitor habits, associations, and preferences. This type of surveillance is also especially problematic since it is invisible and constantly running.

Biometric surveillance, especially Aadhaar-based, is one of the biggest algorithmic surveillance systems globally[7]. Combining biometric identity with the welfare program, authentication and databases brings the possibility of wholesale monitoring of individuals within several spheres. It can be argued that despite the above justification Aadhaar was being used as an efficient instrument of governance, when it comes to its connection with other services, the aspect of function creep and the over-aggregating of data causes concern.

2.3 Risks Inherent in Algorithmic Surveillance

In a way, algorithmic surveillance is very dangerous to the constitutional rights and the value of democracy[8]. One of the main issues is the issue of lack of transparency since people can hardly be told how their data can be gathered, processed, or utilized. The lack of explanation in algorithmic systems does not allow the meaningful examination of them, and it does not comply with the principles of natural justice, which means the inability to appeal against unfavorable decisions.

Bias and discrimination is another significant threat. Algorithms are not unbiased; they mirror the preconceptions, value, and prejudice of the data, which the algorithms are trained on. Discriminatory results can be produced by accident, but can affect equality and non-discrimination under Article 14 on a very significant scale. As the State uses such biased systems, they gain the power of law without much protection.

Algorithms used to perform surveillance also have a chilling effect on the basic freedoms

[7]Vyas SN, Bhatt MN. The Algorithmic Panopticon: Artificial Intelligence, Mass Surveillance, and the Death of Privacy. InArtificial Intelligence for Global Counter-Terrorism: Utilizing Deep Learning and Innovative Strategies 2025 Oct 25 (pp. 153-175). Cham: Springer Nature Switzerland.

[8]Reddy J, Baradwaj A, Vijayakumar MN. Digital Privacy and State Surveillance: An Indian Legal and Technological Perspective. MN, Digital Privacy and State Surveillance: An Indian Legal and Technological Perspective (June 03, 2025). 2025 Jun 3.

ISSN: 2582-6433

especially the freedoms of speech, expression, association and movement. Depending on whether one is aware or conscious of the fact of always being observed, the fear may cause them not to engage in protests, dissenting, or do something that is lawful[9]. This kind of self censorship cannot be congruent with a democratic society that is based on constitutional freedoms.

Lastly, there is function creep, which is the structural risk, where the surveillance systems initially implemented with focused purposes slowly turn to become wider and unrelated. Without legal limits, data gathered in the context of welfare, health, or security can be reused in policing or intelligence, bit by bit, undoable privacy.

3. Evolution of the Right to Privacy in Indian Constitutional Law

3.1 Early Judicial Position

The Indian courts originally took a limited interpretation of right to privacy. In M.P. Sharma v. A 8-judge bench led by Satish Chandra (1954) ruled that the Indian Constitution made no express acknowledgement of a right to privacy, specifically in as far as search and seizure is concerned. The Court said that it did not interpret privacy into Article 20(3) or other basic rights and was a formalistic view of the constitutional text.

Similarly, in Kharak Singh v. In 1963, the case of State of Uttar Pradesh, the Supreme Court held that some of the police surveillance methods such as domiciliary visitation were constitutional, but denied that there was any homogeneity right to privacy. Though most people rejected constitutional protection, the dissenting opinion of Justice Subba Rao acknowledged privacy as inherent to the liberty of a person in Article 21. This opposition subsequently formed the basis of development of the privacy jurisprudence in India.

3.2 Emergence of Privacy Jurisprudence

The Court slowly changed to the perception of privacy being the implied constitutional right. In Gobind v. In the case State of Madhya Pradesh (1975) the Supreme Court recognized that it was possible to derive privacy based on Articles 19 and 21 but reasonable restrictions were allowed in the name of order in the society. It was the first time that the privacy was

[9]Kumar A, Kaur R. Right to Privacy in the Era of AI-Powered Surveillance Technologies. InInternational Conference on Emerging Research in Computing, Information, Communication, Artificial Intelligence and Machine Learning 2024 Feb 23 (pp. 245-252). Singapore: Springer Nature Singapore.

ISSN: 2582-6433

constitutionally acknowledged by the court.

More development was done in R. Rajagopal v. In State of Tamil Nadu (1994) the Court recognised the right to privacy as the right to be left alone, especially in the personal life and in the information[10]. The ruling insisted that the personal details published illegally contravened privacy except where the publication was done under the interest of the people. These rulings formed the basis of informational privacy acknowledgment within the Indian constitution.

3.3 The Puttaswamy Judgment and Its Significance

The case landmark in Justice K.S. Puttaswamy v. The constitutional status of privacy was finally determined by Union of India (2017). The unanimous decision of the nine-judge bench was to the effect that the right of privacy was a fundamental right guarded in Article 21 together with the other freedoms in Part III of the Constitution. The Court overturned previous precedents and reaffirmed the privacy as an inseparable part of human dignity and freedom.

The decision brought about the definition of the privacy at a significant scale where the informational privacy was acknowledged as a fundamental constitutional issue, where the individual control over personal data was regarded[11]. It also recognized decisional autonomy, which safeguards personal options of bodily integrity, family, sexuality and conviction. Most crucially, the Court did not want the uncontrolled State scrutiny and stressed the significance of the strong protective mechanisms in the digital world.

3.4 Privacy as a Facet of Article 21

Article 21 entrenches privacy in the post-Puttaswamy era as an aspect of dignity, autonomy, and liberty. Dignity demands that people should be treated as ends and not as data points. Autonomy safeguards the right to make individual decisions without unnecessary meddling of the State. Freedom means having no arbitrary encroachment on personal life.

These values in the scenario of algorithmic surveillance require greater attention to the State

[10]Bharal S, Sharma R, Pandey A, Ahmed S. Code, Constitution and AI: Rethinking Fundamental Rights in the Algorithmic Era. IJSAT-International Journal on Science and Technology. 2025 Sep 5;16(3).
[11]Haque IU, Jafri SM, Rehman TU. Right to Privacy in the Age of Mass Surveillance by the State. InInternational Conference on Law and Technology (ICLT 2025) 2025 Dec 26 (pp. 87-98). Atlantis Press.

ISSN: 2582-6433

action. Invisibility, disproportionate and unaccountable surveillance system endangers the very form of constitutional liberty and compromises the vision of transformation in Articles 21.

4. Constitutional Tests Governing State Surveillance

4.1 The Puttaswamy Three-Fold Test

The Puttaswamy ruling provided a three prong test to determine the constitutionality of State decisions that violate privacy: legality, legitimate State purpose and proportionableness. To start with, the surveillance measure should be legally established. Executive acts in the absence of legislative support are constitutionally questionable[12]. Second, the measure should seek a true State goal, which may be the national security or the civic law and order. Third, the end taken should be commensurate to the goal meant to be accomplished.

4.2 Doctrine of Proportionality

The proportionality principle dictates that the State action should be necessary, the least restrictive use of force be used, and a fair balance of interests should be achieved. Surveillance should not be too extreme and selective. The intrusiveness and scale of algorithmic surveillance require that a high level of proportionality is followed. Mass profiling or blanket data collection is hard to defend by this doctrine.

4.3 Procedural Safeguards as Constitutional Requirements

Procedural protection is a constitutional validity. To manage abuse, it should be supervised properly, authorised independently, and reviewed and held to account on a regular basis. In addition, the due process must be transparent, where practicable, and it must have redress. The absence of these types of security will introduce algorithmic surveillance as a weapon of arbitrary power that cannot be compatible with constitutional government.

5. Algorithmic Surveillance Practices in India

5.1 Aadhaar Ecosystem and Data-Driven Governance

Aadhaar system is the largest scale of algorithmic and biometric surveillance in India. As a distinct identification system to make the welfare delivery process more efficient, Aadhaar is designed with a central repository which is handled by Unique Identification Authority of India

[12]Basu T. Balancing Private Rights in India: Judicial Pronouncement and Contemporary Challenges. Available at SSRN 5977754. 2025 Nov 1.

ISSN: 2582-6433

(UIDAI). The system is based on the biometric identifiers like fingerprints, iris scan and facial images that are matched algorithmically to authenticate the individuals in a broad spectrum of services. Aadhaar forms the basis of digital governance infrastructure in India by ensuring that the quick verification and integration of multiple databases is possible through architecture.

Even the Supreme Court in the Justice K.S. Puttaswamy v. Union of India did not reject the constitutional validity of Aadhaar but with restrictions, there are grave concerns with profiling and tracking[13]. The connection of Aadhaar to the welfare programmes, financial services, telecommunications services and digital platforms opens a prospect of total monitoring of the activity of the individuals. The behavioural patterns can be inferred using the algorithmic authentication logs, metadata, and transaction logs, causing concerns about the function creep beyond the scope of the system. This concentration of sensitive biometric information increases the chance of abuse, unauthorized access and long term surveillance without sufficient consent or control as well.

5.2 Facial Recognition Technology (FRT)

Facial recognition technology has become one of the most popular devices of algorithmic surveillance in India, especially within the sphere of law enforcement. FRT has been applied by police authorities in various States to detect suspects, countercheck on people assembly and detect crime. These systems are based on AI algorithms that compare the face features that are recorded with CCTV cameras and compared with databases with the images of the suspects or missing persons. With the help of FRT, it is possible to monitor the public space in real-time, which greatly increases the monitoring capacities of the State.

The first constitutional issue with FRT of significance is the lack of a detailed statutory framework of its deployment[14]. In comparison to the conventional surveillance techniques, facial recognition is not supported by the explicit authorisation of the legislature, but, instead, by the executive order or administrative regulations. The national crime records bureau (NCRB) has led the way in initiatives like Automated Facial Recognition System (AFRS) which is projected to be a national database that can be accessed by law enforcers. Such

[13]Singh S, Mittal K. The Constitution and Artificial Intelligence: The Future of Rights and Governance in India. Available at SSRN 5394092. 2025 Mar 15.
[14]Joshi P, Wamankar Y. ALGORITHMIC POLICING AND DUE PROCESS IN CYBERCRIME INVESTIGATIONS: A CONSTITUTIONAL ANALYSIS UNDER ARTICLES 14, 19 AND 21 OF THE INDIAN CONSTITUTION. ShodhSamajik: Journal of Social Studies. 2025 Dec 19;2(2):153-67.

ISSN: 2582-6433

initiatives, however, are constitutionally susceptible because there is no distinct legal framework in terms of data collection, accuracy, consent, retention, and accountability. The unthoughtful utilisation of FRT poses a threat to make mass surveillance normal and disregard the privacy and anonymity that were once related to the space.

5.3 Predictive Policing and Crime Analytics

Predictive policing is a less obvious but more effective kind of algorithmic surveillance, where police resources and criminal behaviour are predicted with help of data-driven tools. These systems are the systems that examine past crime data, social indicators and patterns of behaviour in order to determine high-risk areas or people[15]. Various police departments in India have deployed crime analytics platforms and websites to enhance efficiency and decision-making in many cases, usually under the guise of smart policing or e-governance.

Nevertheless, predictive policing has some grave constitutional issues because of the possibility of bias and excessive policing. Algorithms that are trained based on past crime data can be recreating the existing biases that exist in the criminal justice system and may unfairly focus on the marginalised communities or localities. The usage of probabilistic evaluation, as opposed to tangible evidence, dilutes the distinction between suspicion and guilt, which might end up in random monitoring and preemptive measures. These practices extend the presumption of innocence and cast doubt on issues of fairness, proportionality, and due process in Articles 14 and 21 of the Constitution.

5.4 Surveillance During Public Health and Security Emergencies

The COVID-19 pandemic was a major growth of algorithmic surveillance in India as it was stated to be based on public health and emergency management[16]. Contact-tracing applications, location tracking and digital health monitoring technologies were quickly implemented to prevent the virus. Although these steps were organized as emergency and obligatory steps against an unprecedented crisis, they showed the ability of the State to quickly amplify surveillance facilities.

[15]Sreekumar TT, Balakrishnan S. Digital Governmentality and the Algorithmic State:: AI Surveillance in Comparative Perspective. Sanglap: Journal of Literary and Cultural Inquiry (ISSN: 2349-8064). 2025 Dec 29;12(1):17-31.
[16]Balarabe K. Algorithmic authoritarianism: Artificial intelligence's threat to privacy and freedom in the global south. Information & Communications Technology Law. 2025 Aug 1:1-33.

ISSN: 2582-6433

The surveillance consequences of the emergency are highly worrying in the long term. The short-term solutions may turn into long-term aspects of the government, particularly without the sunset provisions or effective control systems. Emergency data can be stored or put to further use that is not within its initial purposes, which diminishes privacy gradually. The process of becoming used to surveillance in crises, therefore, creates a dangerous precedent, undermining the constitutional protection and blurring the line between the emergency authorities and the normal services.

6. Constitutional Challenges Posed by Algorithmic Surveillance

6.1 Violation of Informational Privacy

The breach of informational privacy, which can be defined as the right of an individual to control the gathering, use, and distribution of personal information, is one of the most important constitutional issues of algorithmic surveillance. Most surveillance systems are run without any informed consent, based on either compelled participation or indirect data mining. People usually lack much knowledge about the volume of collecting their data, as well as the processing of this data by algorithm systems.

Also, privacy issues are aggravated by unlimited storage of data. Once the data of surveillance is collected, it is often kept over long periods of time without defined deletion policies or restrictions on the purpose[17]. This poses a danger of constant surveillance and retrospective inspection that would mean the State can rebuild lives of people over period of time. These activities go against the principles of data minimisation and purpose limitation that have been identified in the privacy jurisprudence.

6.2 Lack of Transparency and Explainability

There is a system of profound lack of transparency with algorithmic surveillance systems. Algorithms are too complex and proprietary, so it is challenging to know how decisions are made or what data is taken as inputs. This is a weakness of constitutional accountability because it protects the actions of the States against any serious scrutiny. When the people are being surveilled the unpleasant decisions made are hardly communicated to them and they do not get chances to defend or rectify error.

[17]Sethi A, Ullah HH, Naseem RM. Surveillance, National Security and the Right to Privacy in the Digital Era. The Critical Review of Social Sciences Studies. 2025 Oct 12;3(4):431-43.

ISSN: 2582-6433

The procedural fairness and due process are at the core of the impossibility to challenge the algorithmic decisions[18]. In cases where monitoring leads to policing, access to welfare, or administrative response, lack of explainability may lead to the deprivation of rights at random. The constitutional governance requires that the power of the State should be exercised in a transparent and reviewable manner which the algorithmic surveillance does not satisfy.

6.3 Discrimination and Equality Concerns (Article 14)

The issue of article 14 of the Constitution of equality is an alarming concern of algorithmic surveillance. Algorithms can be discriminatory either because of biased training data, improper design or insensitivity to context. Surveillance systems that are particularly focused on some communities or geographic areas would threaten to institutionalize discrimination in the name of technological neutrality.

The use of predictive tools and facial recognition to profile marginalised communities will increase the extent of social exclusion and strengthen power imbalances[19]. The discriminatory impacts of algorithmic systems become constitutional when applied by the State. The absence of bias protection mechanisms compromises the Indian constitutional system, which ensures equality in the eyes of the law and equal protection of the law which are fundamental principles of the Indian constitution.

6.4 Chilling Effect on Fundamental Freedoms

The all-encompassing quality of algorithmic surveillance sends a chilling effect to major freedoms, such as the right to speech, the right to assemble, and the right to move, as enshrined in Articles 19 and 21. The fear of being constantly watched can keep people silent about their dissent, stop them going out in the streets, or even having a legitimate form of collective action. This self-censorship undermines democracy and discourages the populace.

Chilling effects of surveillance can be very detrimental especially in a constitutional democracy where freedom of expression and association constitutes accountability and governance. The fact that algorithmic surveillance is an invisible and continues to operate, increases these effects

[18]Tripathi D, Sharma AK. The Evolution of Right to Privacy in India: A Socio-Legal Approach. Legal Lock J..2024;4:25.
[19]Patil A, Borikar E, Venkatraman M. The Illusion of Legal Rights: Regulating AI-Powered Satellite Surveillance to Protect Privacy, Sovereignty and Security. ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences. 2025 Dec 19;10:497-502.

ISSN: 2582-6433

in a way that it makes the environment an atmosphere of fear and conformity that is not conducive to the values of the constitution.

7. Judicial and Legislative Responses in India

The conservative but evolving judicial role of the Indian judiciary has been in reviewing the State surveillance practices. This is in the Hindu LiterumbarRada case, or litigation as it is also named, Justice K.S. Puttaswamy Vs. The Court of the Supreme Court in Union of India (2018) said that the restriction of the use of data, retention of data and mandatory connection of data were constitutionally sound in the scheme. The Court mentioned the importance of proportionality, purpose limitation, and legislation support, which signifies the greater emphasis on data-driven regulation. However, critics allege that the decision was not broad and deep enough on the extended threats of algorithmic profiling and enduring surveillance, however.

The courts have been more forceful as far as internet censorship is concerned. In Anuradha Bhasin v. On the restrictions imposed on the access to the internet, the Supreme Court declared that it should withstand the scrutiny of the necessity and proportionality test, because it recognized the internet as a vital element of the exercise of fundamental rights (Union of India (2020). The jurisprudence demonstrates that the judicial awareness of the digital dimension of the constitutional liberties exists, although the application of algorithmic surveillance is yet of an indirect character[20]. On the other hand, the example of the Pegasus spyware revealed institutional limitations. The problem of the grave claims of unauthorized surveillance, even though it was raised, the Court ruled that it would deal with the issue just in the form of procedural inquiry and not the substantive constitutional decision, which serves as a pointer of the challenges of judicial review in national security.

The enactment of the Digital Personal Data Protection Act, 2023 is a significant step in the Indian legislative sphere on the topic of privacy. One of the Puttaswamy principles is the principles of consent, data minimisation and accountability, which are found in the Act. However, it is not very efficient in addressing State surveillance[21]. Broadly accepted

[20]Kumar V. The The Intersection of Technology, Privacy, and Human Rights: Judicial Perspectives in India. Motherhood International Journal of Research & Innovation". 2024;1(02):92-9.
[21]Ramaswamy S. The Evidence Machine: Rethinking Admissibility and Privacy in India's AI Surveillance State. Indian Journal of Law and Technology. 2024;20(2):4.

ISSN: 2582-6433

exemptions that are usually accorded to government agencies on the basis of national security and preserving the order undermine privacy and proper supervision. In addition to that, the Act does not directly regulate algorithmic decision-making; moreover, it does not send surveillance technologies to be open and accessible to auditing.

India has no particular and elaborate legislative framework of surveillance. The already existing practices are more or less governed by the executive order, colonial era laws and administrative directives. Such reliance in executive will prevent any constitutional advantage and power without checks. Supervisory procedures remain highly centred and internalised posing question of accountability, transparency and power abuse.

8. Comparative Constitutional Perspectives

In United States, the Fourth Amendment of the protection against unreasonable searches and seizures forms the major part of the regulation of surveillance. It has become widely accepted within the courts that new digital surveillance technologies need to be scrutinized more closely, and that such scrutiny is necessary when matters of privacy are involved. The judicial insistence of warrants and standards of reasonableness are the signs of conservative attitude towards technological surveillance.

The European Union is a proponent of rights-based approach by incorporating the General Data Protection Regulation (GDPR) which stressed proportionality, data minimisation, limit of purpose, and accountability. The GDPR creates an imperative on both the State and the private actors, transparency and redress mechanisms, providing a better protection against the surveillance of the algorithm.The experience of the comparisons creates an imperative of independent oversight, algorithmic responsibility, and privacy-by-design principles. A valuable lesson open to be learnt by India is to entrench rights-based protections and place such safeguards by ensuring that surveillance technologies are deployed within well-stipulated constitutional parameters.

9. Towards a Constitutional Framework for Regulating Algorithmic Surveillance

The ever-growing dependence on algorithmic surveillance requires the creation of the consistent constitutional system based on the rule of law, responsibility, and safeguards of

ISSN: 2582-6433

rights. It is important to have a specific statutory-based surveillance law in place that will be used to substitute the existing use of executive discretion. The scope, the purpose and the boundaries of the surveillance powers should be spelt out through such legislation to avoid arbitrariness and excesses. The protection provided by the constitution has to be enshrined at both design and operational levels such as transparency in the algorithms, ability to audit systems and that fundamental rights be subjected to human intervention in decision-making. It is also significant the institutional role of constitutional actors. The courts should develop norms on the evaluation of algorithmic systems so that technological non-transparency does not protect the State action. Specialised committees have to be used by parliament as the main democratic body to maintain constant control over surveillance practices in way that they are in line with the constitutional values.

10. Conclusion and Recommendations

The paper concludes that legal and constitutional protection mechanisms currently in place in India cannot respond suitably to the problem of algorithmic surveillance, because these phenomena are due to the unique characteristics of the country. The lack of a rigorous regulatory framework, the existence of anonymous technologies, and extensive executive authority are a huge threat to privacy, equality, and individual freedom. To address the research questions, it is clear that algorithmic surveillance should be exposed to an increased level of constitutional scrutiny in relation to Articles 14, 19, and 21. The research suggests that it would be appropriate to establish the global legislation implementing complete surveillance, reinforcing data protection standards, and making algorithmic responsibility institutional. Finally, a constitutional democracy should take into account the security needs of individuals at the expense of a reasonable balance of personal freedoms, where the development of technologies should be used to support the principles of the Constitution instead of being against them.

Reference

1. [1]Khamroi A, Shrivastava A. Analysing the practical implications of a right to privacy: State surveillance and constitution.
2. [1]Bala J, Arora A. An Analysis of Surveillance and Data Protection with Reference to the Right to Privacy. Part 2 Indian J. Integrated Rsch. L..2022;2:1.

ISSN: 2582-6433

3. [1]Dutt R. AI and the Right to Privacy-Balancing Innovation with Constitutional Protections. LawFoyer Int'l J. Doctrinal Legal Rsch..2025;3:920.
4. [1] Mishra M. A Critical Analysis of the Right to Privacy. Issue 5 Indian JL & Legal Rsch..2022;4:1.
5. [1]Sonkar A. Automated State Action in India: Administrative Justice, Privacy and Constitutional Accountability.
6. [1]Goel S. Right to Privacy: A Critical Analysis. Issue 3 Int'l JL Mgmt. &Human..2021;4:2117.
7. [1]Vyas SN, Bhatt MN. The Algorithmic Panopticon: Artificial Intelligence, Mass Surveillance, and the Death of Privacy. InArtificial Intelligence for Global Counter-Terrorism: Utilizing Deep Learning and Innovative Strategies 2025 Oct 25 (pp. 153-175). Cham: Springer Nature Switzerland.
8. [1] Reddy J, Baradwaj A, Vijayakumar MN. Digital Privacy and State Surveillance: An Indian Legal and Technological Perspective. MN, Digital Privacy and State Surveillance: An Indian Legal and Technological Perspective (June 03, 2025). 2025 Jun 3.
9. [1]Kumar A, Kaur R. Right to Privacy in the Era of AI-Powered Surveillance Technologies. InInternational Conference on Emerging Research in Computing, Information, Communication, Artificial Intelligence and Machine Learning 2024 Feb 23 (pp. 245-252). Singapore: Springer Nature Singapore.
10. [1]Bharal S, Sharma R, Pandey A, Ahmed S. Code, Constitution and AI: Rethinking Fundamental Rights in the Algorithmic Era. IJSAT-International Journal on Science and Technology. 2025 Sep 5;16(3).
11. [1]Haque IU, Jafri SM, Rehman TU. Right to Privacy in the Age of Mass Surveillance by the State. InInternational Conference on Law and Technology (ICLT 2025) 2025 Dec 26 (pp. 87-98). Atlantis Press.
12. [1]Basu T. Balancing Private Rights in India: Judicial Pronouncement and Contemporary Challenges. Available at SSRN 5977754. 2025 Nov 1.
13. [1]Singh S, Mittal K. The Constitution and Artificial Intelligence": The Future of Rights and Governance in India. Available at SSRN 5394092. 2025 Mar 15.
14. [1]Joshi P, Wamankar Y. ALGORITHMIC POLICING AND DUE PROCESS IN CYBERCRIME INVESTIGATIONS: A CONSTITUTIONAL ANALYSIS UNDER ARTICLES 14, 19 AND 21 OF THE INDIAN CONSTITUTION. ShodhSamajik: Journal of Social Studies. 2025 Dec 19;2(2):153-67.

ISSN: 2582-6433

15. [1]Sreekumar TT, Balakrishnan S. Digital Governmentality and the Algorithmic State:: AI Surveillance in Comparative Perspective. Sanglap: Journal of Literary and Cultural Inquiry (ISSN: 2349-8064). 2025 Dec 29;12(1):17-31.
16. [1]Balarabe K. Algorithmic authoritarianism: Artificial intelligence's threat to privacy and freedom in the global south. Information & Communications Technology Law. 2025 Aug 1:1-33.
17. [1]Sethi A, Ullah HH, Naseem RM. Surveillance, National Security and the Right to Privacy in the Digital Era. The Critical Review of Social Sciences Studies. 2025 Oct 12;3(4):431-43.
18. [1]Tripathi D, Sharma AK. The Evolution of Right to Privacy in India: A Socio-Legal Approach. Legal Lock J..2024;4:25.
19. [1]Patil A, Borikar E, Venkatraman M. The Illusion of Legal Rights: Regulating AI-Powered Satellite Surveillance to Protect Privacy, Sovereignty and Security. ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences. 2025 Dec 19;10:497-502.
20. [1]Kumar V. The The Intersection of Technology, Privacy, and Human Rights: Judicial Perspectives in India. Motherhood International Journal of Research & Innovation. 2024;1(02):92-9.
21. [1]Ramaswamy S. The Evidence Machine: Rethinking Admissibility and Privacy in India's AI Surveillance State. Indian Journal of Law and Technology. 2024;20(2):4.