© SEP 2022 | IRE Journals | Volume 6 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV6I3-1714600

AI Surveillance and the Right to Privacy: Balancing Public Safety and Civil Liberties in India

DR. RAMESH KUMAR
Institute of Law, Kurukshetra University, Kurukshetra

Abstract- ***The fast development of surveillance technologies that are based on artificial intelligence (AI) has made a huge change in policing and governance in India. Facial recognition, predictive policing systems, and big data analytics systems are the systems that are promised to lead to better safety of the population, efficiency of the administration, and crime prevention. Nevertheless, their implementation also brings up some severe constitutional and ethical issues of privacy, autonomy, and democratic liberties. In this paper, the author will explore the implication of AI-based surveillance on the Indian constitution especially on the fundamental right of privacy in Article 21. It examines the ways in which AI surveillance facilitates constant and mass surveillance by pooling CCTV network, biometric databases, social media and mobile devices data together. These practices pose threats to spatial privacy, informational privacy and decisional autonomy as well as having a chilling effect to freedom of speech, association and dissent. The paper also assesses the legality of the AI surveillance in terms of the proportionality test, noting that there is no elaborate law against these technologies in India. It also examines issues to do with the bias and discrimination of algorithms that are likely to have an unequal effect on discriminated groups, which brings about the question of equality in Article 14. Though the given paper does not deny that the issues of national security, crime control, and the overall public safety are the acceptable state objectives, it posits that blanket AI monitoring is not the least restrictive and the most proportionate tool to the purpose. Towards the end of the article, the author emphasizes the necessity of an all-inclusive surveillance legislation that entails judicial checks and balances, transparency, accountability, and anti-abuse provisions so that the effect of technological progress will not be a dent to the constitutional freedoms.***

Keywords: AI Surveillance; Right to Privacy; Constitutional Law; Proportionality Test; Digital Governance.

I. INTRODUCTION

The blistering development of artificial intelligence (AI)-related surveillance tools has profoundly altered the modern law enforcement and administration in India. Facial recognition systems, predictive policing algorithms, automated number plate recognition systems, and massive data analytics platforms are becoming more and more popular with State authorities as the tools that allow them to keep an eye on the masses, avert crimes, and improve their efficiency in the administration. Using these technologies, governments are able to handle large volumes of data, see people in real time and make patterns that can help in criminal investigations. Although these developments will be associated with enhanced security and better governance, they are also accompanied with some serious concerns regarding privacy, autonomy, and democratic freedoms. An AI-driven surveillance deployment, in its turn, requires a thorough review of its suitability with constitutional protections and civil liberties.

With the constitutional background of the Indians, the subject of surveillance should be evaluated with the necessary consideration of the primary right to life and individual liberty enshrined in Art. 21 of the Indian Constitution. The Supreme Court expanded the scope of this right and made de facto its significant expansion in K.S. Puttaswamy v. Union of India (2017) 10 SCC 1, in which the Court made unanimous collateral determination of the right to privacy as a fundamental right inherent in human dignity, autonomy and liberty (K.S. Puttaswamy v. Union of India, 2017). This ruling underscored the importance of privacy as encompassing informational privacy, bodily integrity and decision autonomy which are becoming increasingly threatened in the digital age due to the broad scope of gathering and processing of personal information. The Court also put a warning that the excessive accumulation of personal information by the State might lead to the development of a surveillance society against constitutional democracy (K.S. Puttaswamy v.). Union of India, 2017).

Traditionally, surveillance was a significant tool of State authority employed to ensure the order in the population and to enable criminal acts and guarantee the security of the nation. The advent of artificial intelligence has, however, made the scale, extent, and intrusiveness of surveillance practices far more intense. Many of the conventional surveillance systems introduced traditional surveillance systems that were based on manual observation and tends to be targeted unlike the AI-enabled systems that allow people to be observed continuously, in large scale and at a relatively large volume. Facial recognition systems (AFRS) which operate on AI, automatic number plate recognition (ANPR), and predictive policing tools can enable policymakers to monitor and trace the movements of people, assess their behavioural patterns, and observe their links across all types of platforms. Consequently, surveillance has not only become a specific investigation, but also a system that is capable of profiling populations in mass and in real time.

Such extensive surveillance has raised the question of the constitutionality of such surveillance in a number of court cases. People Union of Civil Liberties v. In the Supreme Court case (1997) of Union of India 1 SCC 301, it was found that the surveillance activities should be conducted in a legal framework where there should be procedural protection against random encroachment into personal life. Union of India, 1997). The Court highlighted the need to approve, control, and supervise the surveillance activities. In like manner in Anuradha Bhasin v. The Court repeated the emphasis of the case, Union of India (2020) 3 SCC 637, where the State actions that impact the basic rights have to pass the necessity and proportionality tests (Anuradha Bhasin v.). Union of India, 2020). These concepts are especially applicable when discussing the surveillance of the AI-based system that allows surveilling and monitoring individuals on a scale never heard of before.

Furthermore, AI-based surveillance systems are greatly dependent on the merging of information on numerous sources, such as CCTV networks, biometers, social media, and mobile communication logs. Such a wide range of data gathering enables the authorities to create detailed electronic inspections of individuals, disclosing their location, behaviors, as well as social relationship. These practices are a major threat to informational privacy, and they are subject to poor use, data security breaches, and accountability. Lack of a detailed legislative framework that specifically governs AI-based surveillance in India only adds to these dangers since most surveillance programs are executed by executive decree, not by law.

Hence, the most important constitutional issue which can be raised is whether the right to privacy and personal liberty which is guaranteed by Article 21 can be compatible with pervasive AI-enabled surveillance. The growing adoption of modern surveillance methods requires a prudent strike between the goals of ensuring safety in people and constitutional rights. Lack of proper legal protection, transparency, and supervisory systems will make AI-informed surveillance a threat to undermine democratic liberties and destroy the very basis of the right of citizens.

II. CONSTITUTIONAL FOUNDATION OF PRIVACY

The constitutional foundation of the right to privacy in India was firmly established by the Supreme Court in the landmark judgment of *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1. In this historic decision, a nine-judge constitutional bench unanimously held that the right to privacy is a fundamental right protected under Article 21 of the Constitution of India, which guarantees the right to life and personal liberty (K.S. Puttaswamy v. Union of India, 2017). The Court clarified that privacy is not an isolated right but an essential component of human dignity, autonomy, and liberty, forming an intrinsic part of the constitutional scheme. This judgment marked a significant turning point in Indian constitutional law, as it overruled earlier decisions that had denied privacy the status of a fundamental right.

The Supreme Court in *Puttaswamy* emphasized that the right to privacy is deeply rooted in the values of individual dignity and freedom. The Court observed that privacy enables individuals to make personal choices, control their personal information, and develop their personality without unnecessary interference from the State (K.S. Puttaswamy v. Union of India, 2017). It recognized that privacy has multiple

dimensions and cannot be confined to a single definition. In this context, the Court identified several facets of privacy, including informational privacy, bodily integrity, and decisional autonomy. Informational privacy refers to an individual's right to control the dissemination and use of personal data; bodily integrity relates to protection against physical intrusion; and decisional autonomy ensures that individuals can make personal and intimate choices free from external interference. These aspects are particularly relevant in the digital age, where technological advancements enable large-scale collection and processing of personal data.

Importantly, the Court recognized that privacy is essential for the meaningful exercise of other fundamental rights guaranteed under the Constitution. For instance, the right to privacy supports freedoms such as freedom of speech and expression, freedom of association, and freedom of movement under Article 19. Without privacy, individuals may feel constantly monitored and therefore reluctant to express their opinions or participate in democratic activities. In this sense, privacy acts as a safeguard that protects individuals from arbitrary State intrusion and preserves democratic values.

Justice D.Y. Chandrachud, who authored the majority opinion in the *Puttaswamy* judgment, highlighted the dangers associated with the State's ability to collect and aggregate large volumes of personal data. He cautioned that the accumulation of personal information by the government could lead to the emergence of a "surveillance society," which would be incompatible with constitutional democracy (K.S. Puttaswamy v. Union of India, 2017). According to the Court, when the State possesses extensive data about individuals' identities, movements, preferences, and behaviour, it gains unprecedented power that may threaten civil liberties and individual autonomy. This concern becomes even more significant in the context of artificial intelligence and digital technologies that allow real-time monitoring and analysis of personal information.

The judgment also laid down a constitutional framework to determine the validity of State actions that infringe upon privacy. The Court held that any restriction on the right to privacy must satisfy the test of legality, necessity, and proportionality (K.S. Puttaswamy v. Union of India, 2017). First, the action must have a valid legal basis supported by law. Second, it must pursue a legitimate State aim. Third, the measure adopted must be proportionate, meaning it should not be excessive or arbitrary in relation to the objective sought to be achieved. Additionally, the Court emphasized the importance of procedural safeguards to prevent misuse of power and to protect citizens from arbitrary surveillance.

Thus, the recognition of privacy as a fundamental right represents a cornerstone of India's constitutional jurisprudence. The *Puttaswamy* judgment not only affirmed the importance of protecting individual autonomy and dignity but also established clear principles that guide the regulation of emerging technologies and State surveillance practices. In an era increasingly shaped by artificial intelligence, digital governance, and data-driven decision-making, the constitutional foundation of privacy serves as a critical safeguard against excessive State intrusion and ensures that technological progress remains consistent with democratic values and fundamental rights.

III. AI SURVEILLANCE AS A PRIVACY INVASION

Artificial intelligence (AI)–driven surveillance represents a significant shift from traditional monitoring practices to highly intrusive and technologically advanced systems capable of continuous and large-scale observation. Unlike conventional surveillance, which generally relied on human oversight and targeted monitoring, AI surveillance involves automated processes that collect, analyze, and interpret vast quantities of data in real time. With the integration of facial recognition technologies, predictive policing tools, and advanced data analytics, the State is now able to monitor individuals and populations in ways that were previously impossible. While these technologies are often justified on grounds of public safety and crime prevention, they raise serious concerns regarding privacy and constitutional rights.

AI surveillance goes far beyond passive observation. It involves the systematic aggregation and processing of data from multiple sources, including CCTV networks, social media platforms, biometric databases, and mobile communication devices. This extensive data collection enables authorities to create detailed digital profiles of individuals, tracking their movements, interactions, and behavioural patterns over time. The ability to combine these data sources significantly enhances the State's capacity to monitor citizens continuously and invisibly. In the digital era, where individuals leave electronic footprints through everyday activities, AI systems can analyze this information to generate insights about personal habits, preferences, and associations. Such pervasive monitoring transforms surveillance from a limited law enforcement tool into a mechanism capable of mass observation and control.

Another important aspect of AI surveillance is automated profiling. Through advanced algorithms and machine learning techniques, surveillance systems can analyze patterns in individuals' behaviour, movement, and associations. These systems may categorize individuals based on perceived risk levels or suspicious activities, often without human intervention. This form of algorithmic profiling raises concerns about fairness, accountability, and transparency, as individuals may be subject to surveillance or scrutiny based on opaque computational processes. Moreover, predictive analytics tools are increasingly being used to anticipate what authorities describe as "criminal propensity." By analyzing historical crime data and behavioural indicators, these systems attempt to forecast potential criminal activity before it occurs. However, such predictive models risk reinforcing existing biases in data and may lead to unwarranted surveillance of certain communities or individuals.

The deployment of AI surveillance technologies directly affects multiple dimensions of privacy recognized under constitutional jurisprudence. First, it threatens spatial privacy, which refers to the right of individuals to move freely without constant monitoring. Continuous tracking through facial recognition cameras, automated number plate recognition systems, and location-based data collection can reveal detailed information about an individual's movements and daily routines. Second, AI surveillance undermines informational privacy, as it involves the large-scale collection, storage, and analysis of personal data. When personal information is aggregated across various platforms, it creates a comprehensive digital record that may be vulnerable to misuse or unauthorized access. Third, it affects decisional autonomy, as the knowledge or fear of being constantly monitored can influence individuals' choices and behaviour. People may refrain from expressing opinions, participating in protests, or associating with certain groups if they believe they are under surveillance.

The Supreme Court of India has acknowledged the constitutional significance of protecting freedoms that may be indirectly affected by State actions. In *Anuradha Bhasin v. Union of India* (2020) 3 SCC 637, the Court held that measures taken by the State that have a chilling effect on fundamental freedoms must satisfy the tests of necessity and proportionality (Anuradha Bhasin v. Union of India, 2020). The Court emphasized that restrictions affecting rights such as freedom of speech and expression must be reasonable, lawful, and proportionate to the objective sought to be achieved. This principle becomes particularly relevant in the context of AI-driven mass surveillance, which has the potential to suppress not only freedom of movement but also free speech, dissent, and association.

Furthermore, the chilling effect created by pervasive surveillance can undermine democratic participation and civil liberties. When individuals know that their actions, communications, and movements are being constantly monitored by sophisticated AI systems, they may self-censor or avoid engaging in lawful activities that are essential to democratic society. This indirect suppression of fundamental rights raises serious constitutional concerns, particularly under Articles 19 and 21 of the Constitution of India. Therefore, while AI surveillance may serve legitimate State interests such as crime prevention and national security, its deployment must be carefully scrutinized to ensure that it does not disproportionately infringe upon the privacy and freedoms of citizens.

© SEP 2022 | IRE Journals | Volume 6 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV6I3-1714600

IV. THE PROPORTIONALITY TEST

The constitutional validity of any State action that interferes with the right to privacy must be evaluated through the proportionality test laid down by the Supreme Court in *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1. In this landmark judgment, the Court held that although the right to privacy is a fundamental right under Article 21 of the Constitution of India, it is not absolute and may be restricted under certain conditions. However, such restrictions must satisfy a strict constitutional standard to prevent arbitrary or excessive State intrusion into individual liberties. The Court formulated a four-fold test to determine the legitimacy of any measure that limits privacy: legality, legitimate State aim, proportionality, and procedural safeguards (K.S. Puttaswamy v. Union of India, 2017). These principles are particularly relevant in assessing the constitutionality of AI-driven surveillance practices in India.

The first requirement of the proportionality test is legality, which mandates that any restriction on privacy must have a clear basis in law. In other words, surveillance measures must be authorized by a valid statutory framework enacted by the legislature rather than by executive discretion alone. The presence of a law ensures transparency, accountability, and democratic oversight over the exercise of State power. However, a significant concern in the Indian context is the absence of a comprehensive surveillance law regulating the use of artificial intelligence–based monitoring technologies. For instance, facial recognition technologies are increasingly deployed by law enforcement agencies without a dedicated legislative framework governing their use. The proposed National Automated Facial Recognition System (NAFRS), which aims to integrate facial recognition databases across the country, has largely been implemented through executive guidelines and administrative directions rather than through parliamentary legislation. Surveillance carried out without a clear statutory basis fails to meet the legality requirement established in *Puttaswamy*, as it lacks the procedural legitimacy necessary in a constitutional democracy (K.S. Puttaswamy v. Union of India, 2017).

The second requirement is the existence of a legitimate State aim. The State may justify surveillance on grounds such as crime prevention, national security, public order, or identification of missing persons. These objectives are recognized as valid governmental interests in constitutional jurisprudence. However, the mere existence of a legitimate aim is not sufficient to justify intrusive surveillance measures. The third requirement proportionality demands that the means adopted by the State must be rationally connected to the objective and must not be excessive or disproportionate. In other words, the measure should be the least restrictive option available to achieve the intended purpose.

In the context of AI surveillance, concerns arise because such systems often operate on a mass scale rather than being limited to specific suspects or targeted investigations. AI-driven monitoring technologies, including facial recognition systems and predictive policing tools, are capable of scanning and analyzing the data of entire populations in real time. This raises serious proportionality concerns because surveillance that indiscriminately monitors large numbers of people goes beyond what is necessary to achieve law enforcement objectives. Less intrusive alternatives—such as warrant-based targeted surveillance—are available and are more consistent with constitutional principles. When the State opts for blanket surveillance instead of targeted measures, it risks violating the proportionality requirement under the constitutional framework.

The fourth element of the proportionality test involves procedural safeguards designed to prevent abuse of power. Safeguards such as judicial oversight, authorization mechanisms, transparency, and accountability are essential to ensure that surveillance powers are not misused. The importance of such safeguards was emphasized by the Supreme Court in *People's Union for Civil Liberties v. Union of India* (1997) 1 SCC 301, where the Court held that surveillance measures must be authorized, targeted, and time-bound (People's Union for Civil Liberties v. Union of India, 1997). This decision established that unchecked surveillance without clear limitations and oversight mechanisms could violate fundamental rights.

People Union for Civil Liberties v highlighted the significance of these safeguards by the Supreme Court. The Court stated that it is the duty of the surveillance to be authorized, targeted, and time-bound as in Union of India (1997) 1 SCC 301. Union of India, 1997). This ruling determined that unlimited surveillance without an explicit limit and control measures would infringe on the basic rights.

Mass AI surveillance seems to be incompatible with these principles since, in many cases, it does not imply individualized suspicion, is working 24/7, and does not have proper supervision. Surveillance, done on a mass and unrestricted basis, has the effect of contravening the constitutional provision that the power of the State must be exercised in a restraint and responsive way. The lack of legal permission, together with the broadness of monitoring on the basis of AI, thus brings gravitational concerns to the question of whether it is in line with the proportionality test that was established in Puttaswamy.

This means that any use of AI surveillance technologies by the constitutional framework will need to be critically analyzed to make sure it does not violate the four part proportionality criterion. In the absence of a clear legal framework, sound justification, small-scope application, and a sound procedure, AI-assisted surveillance may turn into an illegal violating of the privacy and freedom of citizens.

V. DISCRIMINATION AND ALGORITHMIC BIAS

The increased application of artificial intelligence (AI) to surveillance systems has caused great concern over the issue of discrimination and algorithmic bias. Artificial intelligence technologies are based on the fact that big data is needed to develop algorithms using which it is possible to identify patterns, categorize people, and forecast behavior. But these datasets usually represent historical disparities and social prejudices that are found in society. When these biased records are utilized to train AI systems, they will lead to discriminatory results that impact some communities disproportionately. This, when applied in the framework of surveillance, entails that minorities and marginalized populations can be scrutinized, tracked, and wrongly identified. This is of special concern to India where social stratifications like caste, class, and regional inequalities may affect the data that is to be used in surveillance technologies.

Surveillance AI is often trained over past data obtained in law enforcement databases, crime data, and records. Such data sets might already have an implicit internal bias, like the prejudices of caste, racial profiling, or against a particular class. Consequently, the algorithms can duplicate and even enhance such biases during prediction or identification of individuals. Some instances include predictive policing systems that might have declared some neighborhoods or communities as high risk based on the historical crime information itself, which can be discriminatory policing. As a result, additional surveillance of these communities is possible, which only strengthens the cycles of inequality and suspicion (Barocas & Selbst, 2016).

This type of algorithmic bias is very troubling because Article 14 of the Constitution of India is a guarantee of equality before the law and the forbidding of arbitrary action of the State. The Supreme Court has always believed that actions of State should be reasonable, not arbitrary, and founded on fair classification. In cases where AI surveillance systems discriminate against some groups based on biased data sets or mistaken algorithms, it can mean that it breached the principle of equality and non-discrimination stipulated in Article 14. In E.P. Royappa v. State of Tamil Nadu (1974) 4 SCC 3, the Supreme Court pointed at the fact that arbitrariness is contrary to equality and that any arbitrary action of the State would breach Article 14 (E.P. Royappa v.). State of Tamil Nadu, 1974). In the same way, the algorithmic profiling, which discriminates certain communities, may be treated as a kind of arbitrary and discriminatory State action.

The issue of accuracy of facial recognition technologies is the other significant issue linked to AI surveillance. A number of foreign researches have shown that facial recognition system usually have high rate of error when it comes to identifying dark-skinned people and women. According to a study by the National Institute of Standards and Technology (NIST), it was discovered that there are demographic groups such as people with darker skin tones, where

many facial recognition algorithms exhibit far greater rates of false positives (NIST Face Recognition Vendor Test, 2019). Equally, according to a study widely cited by Joy Buolamwini and Timnit Gebru, commercial facial recognition systems were significantly more vulnerable to errors in recognizing darker-skinned women than it was with lighter-skinned men (Buolamwini and Gebru, 2018). These differences demonstrate the danger of the AI surveillance systems resulting in false identification, false imprisonment, or unwarranted police suspicion.

Facial recognition systems, when applied in law enforcement, can be disastrous to people even when there is the slightest of errors. Misidentification can result in wrong arrests, harassment or observation of innocent individuals especially those of vulnerable groups. These mistakes in greater proportions in marginalized groups contribute to the escalation of social inequalities and diminish trust in law enforcement agencies. Furthermore, when algorithmic systems wrongly identify anyone, they might not have any option to appeal against the decisions made especially when the algorithm applied by the authorities is not transparent or accountable.

The problem of algorithmic bias also implies more general concerns of fairness, accountability, and transparency when it comes to the implementation of AI technologies by the State. In contrast to the conventional decision-making processes, algorithmic systems can be viewed as black boxes, and it is hard to grasp how the decisions are formed and why some people are considered to be suspicious. This non-transparency makes it difficult to identify and remedy the discriminatory outcomes. Researchers have claimed that in the absence of appropriate controls and auditory controls, AI surveillance systems can actually strengthen systemic discrimination as opposed to eradicating it (O'Neil, 2016).

Hence, although AI surveillance technologies can potentially be used to enhance efficiency and detect crime, their usage should be thoroughly considered to avoid breaching constitutional principles of equality and fairness. The independent audits, the openness of the algorithmic decision-making, and accountability mechanisms are the necessary safeguards that would prevent the discrimination and safeguard the basic rights. In the absence of these practices, AI in surveillance can be used to enhance the continuation of social prejudices and infringe the principle of equality before the law written in Article 14 of the Constitution of India.

VI. CHILLING EFFECT ON DEMOCRATIC FREEDOMS

Among the most important effects of the widespread surveillance is the chilling effect on the free exercise of democracy. Surveillance does not simply gather information but it also shapes the way people will act in both the public and the privacy. When people realize that any of their actions, communications, and movements can be tracked by the State, they can change their behavior due to fear of being analyzed or even punished. This is popularly known as the chilling effect and it is a phenomenon that compromises the free exercise of fundamental rights that are paramount in a democratic society.

The Supreme Court of India has realized the effects of fear and possible punishment on freedom of expression. In S. Khushboo v. The Court noted that fear of litigation or punishment may lead to the muting of free speech and the dishearten of people when they want to say what they think freely (Kanniammal, 2010) 5 SCC 600. Kanniammal, 2010). The ruling put a strong stress on the idea that the democratic society should safeguard the power of individuals to voice their opinions, even when they are not popular or even controversial. People who have a fear of being monitored or facing some consequences of what they are saying will avoid engaging in the general discussion thus undermining democracy.

This chilling effect can be exacerbated with AI-driven surveillance since it will facilitate the constant and mass surveillance of citizens. Unlike the conventional surveillance systems that were only sporadic, AI can enable the authorities to monitor online activities, the social media behavior and track the actual physical movements in real-time. Consequently, people can be more reserved in their political views, in taking part in demonstrations, and in identifying with a certain group. The sense of being surveilled all the time may prompt self-censorship, which is when people on their

own, limit their own speech and actions in case of being noticed by the authorities.

This chilling effect goes directly against some of the basic rights that are guaranteed by the Article 19 of the Constitution of India. To start with, it impacts on the Article 19(1)(a) that guarantees the freedom of speech and expression by the subject that is prone to be subjected to surveillance or repercussions. Second, it affects the liberty of assembly stipulated in Article 19(1)(b) as individuals can evade attending a mass meeting, demonstrations or protests in case they feel that their identities and actions are being profiled and examined. Thirdly, it limits the freedom of association in Article 19(1) (c) since people might not want to join associations and social movements because they fear surveillance or profiling.

What is more, the chilling effect of AI surveillance is not only an impact on the individual rights but also the operations of democracy. A healthy democracy will be based on open debate, action, and a capacity of the citizen to challenge the authority without fear. When surveillance technologies build a sense of constant being monitored to, they may deter civic engagement and undermine the confidence of people to the institutions.

Thus, even though surveillance can be reasonable in some situations to ensure that people live in peace or the state of the nation is safe, its uncontrolled and extensive implementation with the help of AI technologies can affect a variety of constitutional rights indirectly. Surveillance should be well-controlled and practically protected by strong constitutional laws in order to safeguard democratic freedoms.

VII. PUBLIC SAFETY JUSTIFICATIONS

The State tends to rationalize the use of artificial intelligence (AI)-powered surveillance technologies in terms of national security and general safety of people. According to governments, high-tech surveillance devices like facial recognition systems, predictive policing technologies, and massive data analytics are necessary to tackle the security issues of the present day. Specifically, the State insists that AI surveillance can be used to prevent crime, help in counter-terrorism activities, and locate missing individuals. These are certainly lawful goals and they are within the mandate of the State to uphold law and order as well as safeguard citizens. Nonetheless, the constitutionality of these actions is determined not only by the authenticity of the purpose but also by the adequacy of the means taken and their compliance with the basic rights.

The Supreme Court of India has underscored the fact that even where the State is seeking legitimate ends, it should not make sure that the ends embraced by it do not needlessly violate the individual rights. Modern Dental College and Research Centre v. The Court in State of Madhya Pradesh (2016) 7 SCC 353 discussed the doctrine of proportionality and concluded that the State action has to pursue the minimum means to reach its goals (Modern Dental College and Research Centre v. State of Madhya Pradesh, 2016). This principle dictates that in the event that a less invasive measure exists and can be effectively used to achieve the same goal, the State has to use it instead of the more invasive means. The doctrine is especially applicable to the consideration of the application of AI surveillance technologies.

Although AI surveillance can make law enforcement agencies more efficient, mass or random surveillance of whole population can attract significant constitutional issues. The mass surveillance technologies are based on the idea that they are able to gather and analyze information of massive numbers of people, many of whom have no relation to a crime that occurred. These practices extend to targeted law enforcement and may lead to violations of privacy and liberty of the common citizens. Surveillance on a broad basis and without individualized suspicion turns out to be hard to warrant as least restrictive means of attaining the goals of ensuring people are safe.

Other solutions like judicial warrant-based targeted surveillance, better means of investigation and better coordination of law enforcement agencies can provide the same objectives without invading the privacy of the whole population. In this respect, the unselective use of AI-based surveillance systems seems to be unproportional and not at all aligned with the principles of the constitution. The principle of least restrictive means demands that the State considers

security demands and protection of the basic rights, in a balanced manner.

Thus, despite crime prevention, control of terrorism and finding missing persons being legitimate State interests, the application of blanket AI surveillance cannot be justified by such means only. Constitutional jurisprudence demands that such actions be very specific, proportional and backed by sufficient safeguards. In the absence of such measures, AI-based surveillance is likely to destabilize the equilibrium between the security interests of the population and personal freedom that is the center of Indian constitution.

VIII. NEED FOR A SURVEILLANCE LAW

The fast proliferation of artificial intelligence (AI)-driven surveillance technologies in India is a demonstration of the necessity of an advanced legal framework that will govern the utilization of this approach. Currently, numerous surveillance activities are conducted under executive notifications, bureaucratic instructions, or in bits of statutory legislation instead of an exclusive and comprehensive law of surveillance. Such regulatory loophole is a serious issue in terms of accountability, transparency, and protection of fundamental rights. With the rise of intelligent use of AI surveillance systems, there is a growing necessity to ensure that the systems are implemented within the legal framework that is transparent in legal standards and aligned with the principles of constitutionality and democracy.

The enactment of a comprehensive surveillance law that clearly stipulates the extent, boundaries, and modalities of using the surveillance technologies is one of the most important requirements. These laws would indicate the conditions on which surveillance is allowed, the kind of technologies that can be applied and what protection is required to ensure that surveillance is not abused. A legal framework would also make sure that any surveillance being carried out is in a clear legal framework as opposed to the discretionary executive powers.

The other significant protection is that the surveillance measures should be done under judicial warrants. Court sanctioning serves as a necessary limitation to the use of State power as it makes sure that surveillance is only carried out in cases where there is adequate justification. It would be better to make such monitoring of individuals prioritized by an independent judicial authority to avoid arbitrary or excessive monitoring of individuals and make surveillance target, as well as necessary.

Besides that, it is also important to introduce a separate oversight authority to control and supervise the application of AI surveillance technologies. This authority may check the surveillance practices, examine complaints, and make sure that they are in line with the legal and constitutional practices. Independent surveillance control would also help make the system more responsible and minimize the chances of the misuse or misappropriation of surveillance authority by the governmental bodies.

The other important aspects of a good surveillance law are the transparency and auditability of AI systems. The use of AI-based surveillance tools can be based on intricate algorithms, which can be black boxes. In the absence of good transparency arrangements, it is hard to determine whether these systems are operating fairly, accurately and without any bias. Strict auditing, reporting, and disclosure of the information that is of interest to the society can contribute to the responsible use of surveillance technologies and their use in accordance with the law.

Lastly, people should be entitled to a right to know and redress in cases where they are being monitored or where the actions of the AI machines were taken against them. This encompasses the right to counter unlawful surveillance, remedy against breach of privacy and information regarding collection and utilization of their data. It is crucial to provide effective solutions that would ensure the protection of the rights of citizens and the confidence of the people in the government.

Devoid of these legal protections, AI-based surveillance will turn into a system of unrestrained State authority. When these technologies are not regulated, there might be a lot of monitoring and control which may cause digital authoritarianism. Thus, there is a need to pass a comprehensive law on surveillance to strike a balance between the

technological progress and safeguarding constitutional rights and democratic accountability.

IX. CONCLUSION

One of the most critical issues in the digital era has become artificial intelligence-powered surveillance, which has become the subject of a constitutional issue. Although the application of technological resources has contributed to the improvement of the capacity of the State to keep peace with the population and prevent criminal activities and reinforce the security systems, it has also created significant issues regarding the preservation of the basic rights. The growing use of AI-powered surveillance systems, including facial recognition technology, predictive policing systems, and extensive data analytics, has changed the character of State surveillance to be observed instead of possibly omnipresent and omnipresent control of the populace. This transformation brings a direct challenge to the constitutional principles of dignity, autonomy, and individual liberty which is the core of the democratic society.

Articles 14, 19, and 21 of the Indian Constitution provide a system through which citizens cannot be arbitrarily illegally dealt with by the State and through which the individual freedom of a person is preserved. Court decisions and rulings, particularly, in K.S. Puttaswamy v. Union of India (2017), have confirmed that right to privacy is inalienable to life and individual liberty. According to these principles, the intrusion by the State required, such as surveillance, shall be lawful, proportionate, and be accompanied by sufficient protection. But the unregulated growth of AI surveillance threatens to take away these constitutional safeguards because it will allow the gathering of a vast amount of data, profiling without human intervention, and uninterrupted monitoring with little regulation.

Even though the safety of the population and the national security are just causes of the State, the system where all citizens are under the surveillance and control of algorithmic technologies cannot be combined with the provisions of the constitutional democracy. Surveillance practices rooted in convenience or efficiency rather than core values pose a danger to the question of the balance between the power of the State and the freedom of the individual. The democratic society should make sure that technological innovation does not violate constitutional freedoms.

Thus, privacy protection in the age of artificial intelligence should be seen not as an option but a democratic possibility. Protecting privacy and responsible application of surveillance technologies are important to the preservation of the rule of law, safeguarding civil liberties, and integrity of the constitutional system in India.

REFERENCES

[1] Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671–732. https://doi.org/10.15779/Z38BG31

[2] Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 1–15.

[3] National Institute of Standards and Technology. (2019). *Face recognition vendor test (FRVT) part 3: Demographic effects*. U.S. Department of Commerce.

[4] O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing Group.

[5] Supreme Court of India. (1997). *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.

[6] Supreme Court of India. (2010). *S. Khushboo v. Kanniammal*, (2010) 5 SCC 600.

[7] Supreme Court of India. (2016). *Modern Dental College and Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353.

[8] Supreme Court of India. (2017). *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

[9] Supreme Court of India. (2017). *Justice K. S. Puttaswamy (Retd.) v. Union of India* (Chandrachud, J., concurring opinion), (2017) 10 SCC 1.

[10] Supreme Court of India. (2020). *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.