The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

POLICE DRONE SURVEILLANCE IN SMART CITIES: PRIVACY CONCERNS UNDER ARTICLE 21 OF THE INDIAN CONSTITUTION

~ Vidhi Bhatnagar

INTRODUCTION

The rapid growth of surveillance technologies has transformed modern governance and law enforcement across the world. In India, the development of "Smart Cities" under the Government's Smart Cities Mission has accelerated the use of digital infrastructure, artificial intelligence, facial recognition systems, and unmanned aerial vehicles (UAVs), commonly known as drones. Police authorities increasingly rely upon drone surveillance for crowd management, traffic regulation, crime prevention, disaster response, and public safety monitoring. While such technologies promise efficiency and enhanced security, they simultaneously raise significant constitutional concerns regarding privacy, dignity, and civil liberties under Article 21 of the Constitution of India.

Article 21 guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law. Over the years, the Supreme Court of India has interpreted this provision expansively to include the right to privacy, human dignity, autonomy, and informational self-determination. Drone surveillance, particularly when deployed extensively in smart cities, creates the possibility of continuous monitoring of citizens without adequate procedural safeguards. Such unchecked surveillance threatens to create a "surveillance state" inconsistent with constitutional democracy.

This article critically examines police drone surveillance in Indian smart cities and analyzes the constitutional concerns arising under Article 21. It discusses the evolution of the right to privacy in India, the legal framework governing drone operations, the risks associated with state surveillance technologies, and the need for regulatory safeguards balancing security and individual freedoms.

UNDERSTANDING DRONE SURVEILLANCE IN SMART CITIES

The Smart Cities Mission launched by the Government of India in 2015 seeks to integrate technology into urban governance to improve efficiency and public services. Surveillance infrastructure forms an essential component of this initiative. Many cities have established Integrated Command and Control Centers (ICCCs) where data from CCTV cameras, drones, and sensors are centrally monitored.

The increasing dependence upon drone-based policing became particularly visible during the COVID-19 pandemic, where drones were widely used for monitoring lockdown violations and public movement. Although such use was justified on grounds of public safety, it also

highlighted the absence of clear safeguards concerning data collection, storage, and citizen consent.

CONSTITUTIONAL BASIS OF PRIVACY UNDER ARTICLE 21

The Constitution of India does not expressly mention the "right to privacy." However, judicial interpretation has recognized privacy as an intrinsic component of Article 21. Initially, in M.P. Sharma v. Satish Chandra, the Supreme Court rejected the existence of a constitutional right to privacy.[1] Similarly, in Kharak Singh v. State of Uttar Pradesh, the majority held that surveillance regulations did not violate a constitutionally guaranteed right to privacy, although Justice Subba Rao's dissent recognized privacy as essential to personal liberty.[2]

Over time, the judiciary adopted a more liberal interpretation. In Gobind v. State of Madhya Pradesh, the Court acknowledged that privacy may be protected under Article 21, subject to reasonable restrictions.[3] Later, in People's Union for Civil Liberties v. Union of India (PUCL), the Supreme Court recognized telephone tapping as a serious invasion of privacy and laid down procedural safeguards against arbitrary state surveillance.[4]

The constitutional position was conclusively settled in Justice K.S. Puttaswamy v. Union of India, where a nine-judge bench unanimously declared privacy to be a fundamental right protected under Articles 14, 19, and 21.[5]The Court held that privacy includes bodily privacy, informational privacy, and decisional autonomy. It emphasized that any infringement upon privacy must satisfy the following tests:

1. Legality — existence of a valid law
2. Legitimate state aim
3. Proportionality between objective and means adopted
4. Procedural safeguards against abuse.

These principles are directly relevant in assessing the constitutionality of police drone surveillance.

DRONE SURVEILLANCE AND THREATS TO PRIVACY

CONTINUOUS MONITORING AND CHILLING EFFECT

Drone surveillance enables continuous observation of public and semi-public spaces. Unlike traditional policing methods, drones can silently monitor individuals from a distance without their knowledge. Such constant observation creates a chilling effect upon freedom of expression, association, and movement.

Citizens participating in protests, political meetings, or religious gatherings may fear being watched and profiled by authorities. This discourages democratic participation and weakens constitutional freedoms guaranteed under Articles 19 and 21.

---

[1] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (India).
[2] Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (India).
[3] Gobind v. State of Madhya Pradesh, (1975) 2 S.C.C. 148 (India).
[4] People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India).
[5] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

The Supreme Court in Puttaswamy warned against the dangers of mass surveillance and emphasized that privacy is necessary to preserve individual autonomy and democratic participation.[6] Excessive drone surveillance risks normalizing state intrusion into citizens' daily lives.

INFORMATIONAL PRIVACY AND DATA COLLECTION

Modern surveillance drones collect extensive personal data, including facial images, movement patterns, location tracking, and behavioral information. Such data may be stored indefinitely and integrated with facial recognition systems and artificial intelligence databases.

Informational privacy concerns become more serious when there is no comprehensive data protection legislation governing police surveillance practices. Citizens often remain unaware regarding:

1. What data is being collected;
2. How long such data is retained
3. Who has access to the information;
4. Whether data may be shared with third parties.

The absence of transparency and accountability increases the possibility of misuse, unauthorized profiling, and discriminatory targeting.

RISK OF ARBITRARY STATE POWER

Article 21 requires that any restriction upon liberty must follow "procedure established by law." However, large-scale drone surveillance in India often operates through executive notifications or administrative orders rather than comprehensive legislation.

The Supreme Court has repeatedly held that arbitrary state action violates Article 21.[7] Without statutory safeguards, police authorities may exercise excessive discretionary powers, leading to unlawful monitoring of political opponents, journalists, activists, or minority communities.

Such unchecked surveillance undermines constitutional governance and threatens the rule of law.

LEGAL FRAMEWORK GOVERNING DRONES IN INDIA

India regulates drone operations primarily through the Drone Rules, 2021 framed under the Aircraft Act, 1934.[8] The rules simplify licensing procedures and promote commercial and governmental use of drones. They classify drones according to weight categories and prescribe operational guidelines regarding registration, pilot certification, and no-fly zones.

However, the Drone Rules largely focus upon aviation safety and operational management rather than privacy protection. They do not comprehensively regulate:

---

[6] Justice K.S Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[7] The Drone Rules, 2021, Gazette of India, Extraordinary, Part II, § 3(ii), Ministry of Civil Aviation (Aug. 25, 2021).
[8] Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

1. Police use of surveillance drones
2. Data retention practices
3. Facial recognition integration
4. Judicial oversight mechanisms
5. Citizen remedies against unlawful surveillance

Additionally, Section 69 of the Information Technology Act, 2000 empowers the government to intercept, monitor, or decrypt information in the interest of sovereignty, security, or public order.[9] Nevertheless, these provisions were enacted before the rise of sophisticated drone surveillance technologies and fail to address contemporary privacy concerns adequately.

India presently lacks a dedicated surveillance reform law comparable to data protection frameworks existing in several democratic jurisdictions.

PROPORTIONALITY AND CONSTITUTIONAL VALIDITY

The doctrine of proportionality plays a crucial role in determining whether drone surveillance complies with Article 21. In Modern Dental College v. State of Madhya Pradesh, the Supreme Court clarified that restrictions upon fundamental rights must not be excessive and must maintain a proper balance between state objectives and individual freedoms.[10]

Applying the proportionality test to police drone surveillance requires examination of the following factors:

LEGITIMATE AIM

Public safety, crime prevention, disaster management, and national security constitute legitimate state aims. Therefore, the use of drones for narrowly tailored law enforcement purposes may be constitutionally permissible.

NECESSITY

Authorities must demonstrate that drone surveillance is necessary and that less intrusive alternatives are unavailable. Blanket or indiscriminate surveillance of entire populations cannot satisfy this requirement.

MINIMAL INTRUSION

Surveillance measures should be limited in duration, geographic scope, and intensity. Real-time monitoring during emergencies may be justified, whereas continuous mass surveillance may violate constitutional standards.

PROCEDURAL SAFEGUARDS

Independent oversight, judicial authorization, transparency mechanisms, and grievance redressal systems are necessary to prevent abuse. In the absence of safeguards, surveillance practices may become arbitrary and unconstitutional.

COMPARATIVE INTERNATIONAL PERSPECTIVES

[9] Information Technology Act, No. 21 of 2000, § 69 (India).
[10] Modern Dental Coll. & Research Ctr. V. State of Madhya Pradesh, (2016) 7 S.C.C. 353 (India).

Several democratic nations have recognized privacy risks associated with drone surveillance and introduced regulatory safeguards.

In the United States, courts have debated whether prolonged aerial surveillance violates the Fourth Amendment protection against unreasonable searches. The use of drones by law enforcement agencies often requires warrants in certain jurisdictions.

The European Union adopts a rights-based approach emphasizing data protection, transparency, and accountability under the General Data Protection Regulation (GDPR). Drone operators processing personal data must comply with strict privacy obligations.

Canada and the United Kingdom also impose limitations upon police surveillance through independent oversight bodies and privacy commissioners.

India can learn from these comparative models while developing its own constitutional framework balancing security and civil liberties.

CHALLENGES IN SMART CITIES

INTEGRATION WITH FACIAL RECOGNITION TECHNOLOGY

Drone surveillance becomes particularly intrusive when integrated with facial recognition systems. Such technology allows automatic identification and tracking of individuals in real time.

The use of facial recognition raises concerns regarding:

Misidentification

Algorithmic bias

Mass profiling

Discriminatory policing

Studies globally indicate that facial recognition systems may disproportionately misidentify women and minority communities. In India’s diverse social context, such risks become even more significant.

ABSENCE OF TRANSPARENCY

Citizens are rarely informed regarding the scope and extent of surveillance infrastructure in smart cities. Lack of transparency prevents meaningful public debate concerning privacy implications.

Democratic governance requires that surveillance programs operate subject to public accountability rather than secrecy.

POTENTIAL MISUSE AGAINST DISSENT

History demonstrates that surveillance powers are vulnerable to political misuse. Journalists, activists, opposition leaders, and protestors may become targets of unlawful monitoring.

The Pegasus spyware controversy illustrated growing concerns regarding state surveillance and civil liberties in India.[11] Drone surveillance without independent oversight could intensify similar constitutional challenges.

NEED FOR A COMPREHENSIVE REGULATORY FRAMEWORK

To ensure constitutional compliance, India requires a robust legal framework governing police drone surveillance. The following reforms are essential:

ENACTMENT OF SURVEILLANCE LEGISLATION

Parliament should enact a comprehensive surveillance regulation law clearly defining:

Permissible uses of drones;

Conditions for deployment;

Data collection limitations;

Retention and deletion policies;

Penalties for misuse.

JUDICIAL AUTHORIZATION

Intrusive surveillance measures should require prior judicial approval except in genuine emergencies. Independent authorization reduces the risk of arbitrary executive action.

DATA PROTECTION SAFEGUARDS

Strong data protection mechanisms must regulate storage, sharing, and processing of surveillance data. Citizens should possess rights regarding access, correction, and deletion of personal information.

TRANSPARENCY AND ACCOUNTABILITY

Authorities should publish transparency reports disclosing the extent of drone deployment and surveillance activities. Independent oversight bodies should monitor compliance with constitutional standards.

PUBLIC PARTICIPATION

Smart city governance should involve public consultation regarding surveillance technologies. Citizens must participate in decisions affecting their privacy and liberties.

BALANCING SECURITY AND LIBERTY

The debate surrounding drone surveillance ultimately reflects the broader constitutional challenge of balancing collective security with individual freedom. Technological advancements undoubtedly enhance policing efficiency and public safety. Drones can assist in locating missing persons, managing disasters, controlling riots, and monitoring dangerous zones without risking human lives.

[11] Manohar Lal Sharma v. Union of India, (2021) 10 S.C.C. 1 (India).

However, constitutional democracy cannot sacrifice civil liberties in the name of technological progress. The Supreme Court in Puttaswamy emphasized that privacy is not an elitist concern but an essential aspect of human dignity and liberty. Smart cities must therefore remain "constitutional cities" where technology serves citizens rather than controlling them.

The legitimacy of surveillance depends not merely upon technological capability but upon adherence to constitutional morality, accountability, and rule of law.

CONCLUSION

Police drone surveillance in Indian smart cities represents both an opportunity and a constitutional challenge. While drones offer valuable tools for modern policing and urban governance, their unchecked deployment threatens privacy, dignity, and personal liberty protected under Article 21 of the Constitution.

The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India imposes constitutional limitations upon state surveillance powers. Any intrusion into privacy must satisfy the tests of legality, necessity, proportionality, and procedural safeguards. Presently, India's regulatory framework remains inadequate to address the complex constitutional implications of drone-based surveillance systems.

As India advances toward technologically integrated smart cities, it must simultaneously strengthen constitutional protections against arbitrary surveillance. Democratic governance requires that security measures remain accountable, transparent, and proportionate. Surveillance technologies should enhance public welfare without transforming citizens into subjects of continuous monitoring.

Ultimately, the future of smart cities in India must be guided not only by technological innovation but also by constitutional values ensuring that liberty, privacy, and dignity remain protected in the digital age.