Law Conflicts in Aviation: Governing Drone Offenses under Indian and International Jurisprudence

Prashant Kumar
Uttar Pradesh State Institute of Forensic Science, Lucknow, India

Abstract—**Drones, also referred to as Unmanned Aerial Vehicles (UAVs), have revolutionized aviation and changed how technology, law, and security interact. Drones, which were first created for military use, are now used for a variety of commercial and civilian tasks, such as farming, logistics, surveillance, disaster relief, and infrastructure inspection. But because of their dual-use nature, they pose serious hazards, including as terrorism, cybercrime, espionage, and smuggling, which puts conventional regulatory and enforcement systems to the test.**

The Drone Rules, 2021, which set licensing, operating, and safety guidelines, serve as the cornerstone of India's drone laws. In order to handle illegal, dangerous, or malevolent drone operations, these regulations are complemented by laws included in the Bharatiya Nyaya Sanhita (BNS), 2023, the Information Technology Act, 2000, and the Unlawful Activities (Prevention) Act, 1967. The Indian framework is conceptually extensive, but it has real-world restrictions in terms of interagency collaboration, technology integration, and enforcement.

Different countries have different regulatory strategies. Airspace safety, operational standards, and the incorporation of UAVs into traditional aviation are priorities for the International Civil Aviation Organization (ICAO). While the US Federal Aviation Administration (FAA) uses its Part 107 framework to strike a balance between innovation and national security concerns, the European Union (EU) has enacted standardized drone regulations with strict certification and operational criteria.This comparative study emphasizes that, despite its seeming strength, India's drone governance needs improved cross-sector cooperation, technology monitoring, and enforcement measures. It comes to the conclusion that in order to reduce risks and promote the safe, effective, and profitable use of drones in both the commercial and civilian sectors, it is imperative to implement a single anti drone law, integrate cutting-edge surveillance technology, and encourage interagency cooperation.

I. INTRODUCTION

The limits of the law are always being tested by technological innovation, necessitating ongoing adaptation to new threats. One of the most revolutionary of these inventions is the Unmanned Aerial Vehicle (UAV)[1], or drone. Drones, which were first created for military use, have quickly developed into useful instruments that assist both commercial and civilian endeavors, such as infrastructure inspection, environmental management, agricultural monitoring, and humanitarian logistics. However, because of their operational flexibility and accessibility, they can also be abused for terrorism, cybercrime, espionage, and smuggling.

Drones are increasingly becoming entangled with criminal or national security issues in India, as seen by incidents like the 2021 drone attack on the Jammu Air Force Station[2] and the frequent dropping of contraband along the Punjab border[3]. These instances highlight a crucial gap: legal and regulatory frameworks frequently fall behind the swift advancements in drone technology. Although the Chicago Convention of 1944[4] established fundamental principles, such as state sovereignty over airspace, it was unable to foresee the development of autonomous, lightweight UAVs that

[1] See *Unmanned Aircraft System (UAS) Operations in Civil Aviation*, International Civil Aviation Organization (ICAO) Circular 328, 2011.
[2] "Jammu Air Force Station Drone Attack: A New Dimension to Security Threats," *The Hindu*, June 28, 2021.
[3] "Pak Drones Dropping Arms and Narcotics in Punjab," *Times of India*, July 20, 2022.
[4] Convention on International Civil Aviation (Chicago *Convention*), Dec. 7, 1944, 15 U.N.T.S. 295, Art. 1 (recognizing complete and exclusive sovereignty over national airspace).

might operate with little suspicion and covertly traverse boundaries.

This study looks at how India and top international jurisdictions deal with the new issues brought on by drone abuse. It assesses whether existing legal frameworks, such as the Drone Rules 2021 [5]; Bharatiya Nyaya Sanhita (BNS) 2023[6] and pertinent security and cyber laws, effectively reduce risks and compares them to global norms established by the Federal Aviation Administration (FAA) [7], the European Union (EU)[8], and the International Civil Aviation Organization (ICAO)[9]. In the conclusion, this study will offer suggestions for more effective and coordinated drone governance by evaluating how legal regimes may strike a balance between technological innovation, public safety, national security, and sovereign sovereignty through the analysis of comparative regulatory approaches.

II. THE DUAL-USE DILEMMA OF DRONE TECHNOLOGY

Drones are a prime example of dual-use technology; although they promote efficiency and creativity, they also pose serious security risks. Drones in India are categorized by weight and function using the Drone Rules 2021 [10], which were published under the Aircraft Act, 1934. The drones range from Nano (250 g) to Large (150 kg). These regulations specify the conditions for licensing, registration, operating boundaries, and no fly zones. Although these regulations encourage responsible drone use, they provide no protection against malevolent or wilful misuse.

A variety of statutes are used to address criminal activity utilizing drones, resulting in a complicated and overlapping legal environment. The Bharatiya Nyaya Sanhita (BNS) 2023[11], governs offenses such property destruction (Section 108), negligence (Section 106), and homicide (Section 101–109). While terrorist acts are the focus of the Unlawful acts (Prevention) Act (UAPA) 1967 [12], cyber related offenses such as hacking and data theft are covered by the Information Technology Act, 2000[13] (Section 43, Section 66). Particularly when drones cross both the physical and digital realms, this patchwork of regulations creates procedural ambiguities and makes defining jurisdiction difficult.

Since traditional aviation regulations might not adequately address cyber-attacks or remote operational dangers, drones' dual status as "aircraft" and "data devices" exacerbates these regulatory issues. As a result, hybrid regulatory strategies that include cyber security, aviation, and counterterrorism frameworks are required. Clear legal definitions and enforcement procedures are necessary to address the dual-use conundrum, but so are technological monitoring systems that can identify, track, and stop illegal UAV operations, protecting national security and public safety without limiting innovation.

III. DRONE CRIMES: NATURE AND LEGAL RESPONSE

Drone-related offenses in India are diverse and represent both the advantages and disadvantages of UAV technology. These offenses fall into the following categories:

1. Smuggling and Contraband: Especially along the Indo-Pakistan border, UAVs are being used more and more to convey weapons, drugs, and other illegal goods. The Narcotic Drugs and Psychotropic

[5] *Drone Rules, 2021*, notified under Section 5A of the *Aircraft Act, 1934* (Act XXII of 1934).

[6] *Bharatiya Nyaya Sanhita, 2023* (Act No. 45 of 2023), replacing the *Indian Penal Code, 1860*.

[7] Federal Aviation Administration (FAA), *Part 107 – Small* Unmanned *Aircraft Systems*, Code of Federal Regulations (14 CFR Part 107), United States, 2016.

[8] *Commission Implementing Regulation (EU) 2019/947* on the rules and procedures for the operation of unmanned aircraft, and *Delegated Regulation (EU) 2019/945* on unmanned aircraft systems and third-country operators, European Union, 2019.

[9] ICAO, Annex 2 to the Convention on International Civil Aviation – Rules of the Air, 11th Edition, 2005.

[10] *Drone Rules, 2021*, notified under Section 5A of the *Aircraft Act, 1934* (Act XXII of 1934), Ministry of Civil Aviation, Government of India.

[11] *Bharatiya Nyaya Sanhita, 2023* (Act No. 45 of 2023), Section 101–109, 106, 108

[12] *Unlawful Activities (Prevention) Act, 1967* (Act No. 37 of 1967).

[13] *Information Technology Act, 2000* (Act No. 21 of 2000), Section 43, 66.

Substances (NDPS) Act[14] of 1985 and the Customs Act of 1962[15] both regulate such activities and give authorities the ability to pursue illegal cross-border transportation.

2. Terrorism: The possibility of drones for remote terrorist activities was brought to light by the 2021 drone attack on the Jammu Air Force Station. The Unlawful Activities (Prevention) Act (UAPA) 1967[16], was first used in response to this occurrence, focusing on terrorist acts made possible by drones.
3. Espionage and Unauthorized Surveillance: The Drones used to spy on sensitive installations or restricted areas are a violation of the Official Secrets Act of 1923[17] and relevant laws of the Information Technology Act of 2000[18], particularly those dealing to illegal access to digital information.
4. Privacy Violations: Unauthorized aerial recording may be against the BNS's voyeurism[19] regulations and the constitutional right to privacy guaranteed by Article 21[20], creating complex problems at the intersection of technological control and individual freedoms.
5. Cyber security Risks: Drones can be taken over using techniques like GPS spoofing and Wi-Fi. The connection between cybercrime and aviation highlights the need for combined technological and legal protections.
6. Negligence and Accidents: Under section 106 of the BNS[21] and the applicable safety rules in the Aircraft Act, 1934, incidents involving improper drone operation that result in harm or property damage are actionable. Manufacturers, operators, and other accountable parties may be held liable.

In order to successfully address concerns and encourage lawful UAV use, the hybrid nature of drone offenses which span aviation, cyber law, criminal statutes, and national security legislation requires coordinated legal tactics, technology surveillance, and extensive regulatory frameworks.

IV. CONSTITUTIONAL AND HUMAN RIGHTS CONCERNS

Significant constitutional and human rights issues are brought up by drone activities' intersection with fundamental rights. In K.S. Puttaswamy v. Union of India (2017)[22], the Supreme Court of India upheld the fundamental nature of Article 21 of the Constitution, which guarantees the right to privacy. This right is directly threatened by unauthorized drone monitoring, especially when it is carried out without supervision or legal authorization.

At the same time, journalists, business owners, and other professionals who use drones for lawful purposes are protected by Articles 19(1)(a) and 19(1)(g), which also protect freedom of speech, expression, and the right to engage in commerce or business. As a result, any drone usage restrictions must adhere to the proportionality standard set down in Modern Dental College v. State of Madhya Pradesh (2016)[23], guaranteeing that restrictions are appropriate, required, and specifically designed.

In order to address privacy and human rights concerns associated with drone technology, several legal frameworks have been developed internationally. While creating strict restrictions for data collection, processing, and surveillance, the European Union's General Data Protection Regulation (GDPR)[24] places a heavy focus on transparency and individual consent. The United States' Fourth Amendment[25] theory limits

[14] *Narcotic Drugs and Psychotropic Substances Act, 1985* (Act No. 61 of 1985), Section 8–23.
[15] *Customs Act, 1962* (Act No. 52 of 1962), Section111–113.
[16] *Unlawful Activities (Prevention) Act, 1967* (Act No. 37 of 1967), Section 15–16.
[17] *Official Secrets Act, 1923* (Act No. 19 of 1923), Section 3–5.
[18] *Information Technology Act, 2000* (Act No. 21 of 2000), Section 43, 66.
[19] *Bharatiya Nyaya Sanhita, 2023* (Act No. 45 of 2023), Section 77 (Voyeurism and related offences).
[20] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[21] *Bharatiya Nyaya Sanhita, 2023*, Section 106; *Aircraft Act, 1934* (Act XXII of 1934), Section 5A.
[22] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[23] *Modern Dental College and Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353.
[24] European Union, *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679, 2016.
[25] United States Constitution, Fourth Amendment, 1791.

unwarranted government interference and provides protections against unauthorized aerial observation.

The requirements of individual liberty and national security must also be balanced in India's regulatory approach. Strong safeguards, open authorization processes, and accountability guidelines can all be used to permit drone use legally while avoiding undue interference. There must be a single framework that respects privacy and practical utility in order to ensure that technological advancements do not compromise human rights or constitutional protections.

V. INTERNATIONAL LEGAL FRAMEWORKS

A. ICAO Guidelines[26]:- Through its Annexes and Circulars, the International Civil Aviation Organization (ICAO) offers guidance on Unmanned Aircraft Systems (UAS), defining consistent safety standards, requirements for pilot certification, and procedures for cross-border coordination. Although these principles help standardize operations and integrate airspace, there is presently no worldwide treaty that tackles the criminal abuse of drones, therefore domestic authorities are largely responsible for enforcing them.

B. European Union [27] :- Using a risk-based categorization system, the European Union regulates drone operations under Regulation (EU) 2019/947, which is enhanced by Regulation 2019/945. These operations are classified as Open (low risk), Specific (medium risk), and Certified (high risk). Operational authorizations, insurance regulations[28], and strict data protection measures are all integrated into this framework. Its primary strength is the uniformity of drone laws among its member states, which successfully strikes a balance between technology advancement and security and safety goals.

C. United States: - Drones are subject to Part 107 regulations set forth by the Federal Aviation Administration (FAA)[29] of the United States, which mandate registration, certification of remote pilots, and specified operating restrictions. Complementary laws, such the Preventing Emerging Threats Act of 2018[30], give federal agencies the authority to identify, monitor, and destroy unapproved drones. This strategy tackles security and compliance issues by fusing proactive counter-drone capabilities with regulatory supervision.

D. China: - China's nationwide public security network incorporates geofencing[31], GPS tracking, and real-name registration to impose strict control. To provide centralized management, accountability, and improved monitoring of both commercial and recreational UAVs, drones that surpass certain thresholds must be approved by the government.

E. Comparative Observations: - A comparative study of drone laws around the world reveals three major overlapping ideas. First, risk-based classification matches operational authority to the degree of danger that various UAV types pose. Second, strong cybersecurity and privacy integration guarantees that changes in technology won't jeopardize data security or individual rights. Third, using tech-enforcement tools like GPS tracking, geofencing, and AI-powered monitoring improves compliance and makes surveillance easier in real time. Although these concepts are conceptually included in India's regulatory framework, it is not fully implemented in practice due to deficiencies in technology infrastructure, enforcement capabilities, and international standardization [32] . To ensure safe innovation, achieve effective drone governance, and

[26] ICAO, *Annex 2 to the Convention on International Civil Aviation – Rules of the Air*, 11th Edition, 2005; ICAO Circular 328, *Unmanned Aircraft System (UAS) Operations in Civil Aviation*, 2011.

[27] European Union, *Regulation (EU) 2019/947 on the rules and procedures for the operation of unmanned aircraft*, Official Journal of the European Union, 2019; European Union, *Regulation (EU) 2019/945 on unmanned aircraft systems and third-country operators*, Official Journal of the European Union, 2019.

[28] European Union Aviation Safety Agency (EASA), *Introduction to the EU Drone Regulations*, 2020, https://www.easa.europa.eu/domains/civil-drones-rpas

[29] Federal Aviation Administration (FAA), *Part 107 – Small Unmanned Aircraft Systems*, Code of Federal Regulations (14 CFR Part 107), 2016.

[30] *Preventing Emerging Threats Act, 2018*, Pub. L. No. 115-141, United States Congress, 2018.

[31] Civil Aviation Administration of China (CAAC), *Measures for the Administration of Civil Unmanned Aircraft*, 2017.

[32] European Union Aviation Safety Agency (EASA), ICAO, FAA, and CAAC reports on UAV regulation and risk management, 2018–2022.

protect national security, these areas must be strengthened.

VI. ENFORCEMENT AND POLICY CHALLENGES

India still faces major enforcement and policy issues in drone governance, despite remarkable progress in creating a regulatory framework. Since nano and micro-UAVs frequently avoid radar and visual identification systems, identifying and attributing unlicensed drones continues to be a challenge. In order to maintain accountability, cross-border drone activities necessitate international cooperation and dependence on Mutual Legal Assistance Treaties (MLATs)[33]. Due to their vulnerability to hacking, data theft, and GPS spoofing, autonomous and networked drones significantly increase cybersecurit[34]y hazards, combining worries about aviation safety with online dangers. Rapid reaction and policy coherence are also frequently delayed by the disjointed coordination of regulatory, law enforcement, and defense organizations, including the armed forces, state police, and the Directorate General of Civil Aviation (DGCA)[35]. Another significant issue is finding the right balance between regulation and innovation; too much control could stifle research and entrepreneurship in India's developing drone ecosystem. A paradigm change from reactive enforcement to proactive governance based on interagency collaboration, technology integration, and conformity to international legal norms is required to address these issues. Building a robust, safe, and innovative drone ecosystem in India would require improving data-sharing procedures, fortifying detection systems, and cultivating global collaborations.

[33] Ministry of External Affairs, Government of India, *Mutual Legal Assistance Treaties (MLATs) – Status and Guidelines*, 2020

[34] Cyber Security and Aviation Safety Joint Task Force, *Report on Emerging Threats from Autonomous Drones in India*, 2021.

[35] Directorate General of Civil Aviation (DGCA), *National Unmanned Aircraft System (UAS) Traffic Management Policy*, 2021.

VII. STRENGTHS AND WEAKNESSES OF THE INDIAN LEGAL FRAMEWORK

By combining several legislative tools, such as the Drone Rules 2021[36]; the Bharatiya Nyaya Sanhita (BNS) 2023[37]; the Bharatiya Nagarik Suraksha Sanhita (BNSS) 2023[38]; the Bharatiya Sakshya Adhiniyam (BSA) 2023[39]; the Information Technology Act 2000[40]; and the Unlawful Activities (Prevention) Act, 1967, India's drone regulations show significant structural strength. These come together to create a multi-layered ecosystem that tackles national security, cybersecurity, criminal liability, and safety concerns. But even with this strong legislative base, enforcement is nevertheless hampered by a lack of technology capability, uneven application, and poor coordination between the regulatory and enforcement agencies. The lack of a specific anti-drone law has also led to jurisdictional overlaps and accountability gaps, especially when cross-sectoral offenses are involved.

Another serious flaw is still data protection. India currently lacks a complete legislative framework requiring consent-based data processing and guaranteeing openness in drone surveillance or picture gathering, in contrast to the General Data Protection Regulation (GDPR) of the European Union[41]. As a result, even though India's legal system is flexible and conceptually solid, its technology enforcement powers and operational procedures nevertheless lag behind those of other countries. To achieve an efficient and future-ready drone regulatory environment, these aspects must be strengthened through specific legislation, institutional coordination, and data governance reform.

[36] *Drone Rules, 2021*, notified under Section 5A of the *Aircraft Act, 1934* (Act XXII of 1934), Ministry of Civil Aviation, Government of India.

[37] *Bharatiya Nyaya Sanhita, 2023* (Act No. 45 of 2023), Section 101–109, 106, 108

[38] *Bharatiya Nagarik Suraksha Sanhita, 2023* (Act No. 48 of 2023).

[39] *Bharatiya Sakshya Adhiniyam, 2023* (Act No. 46 of 2023)

[40] *Information Technology Act, 2000* (Act No. 21 of 2000), Section 43, 66.

[41] European Union, *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679, 2016.

VIII. COMPARATIVE PERSPECTIVES AND THE FUTURE

India's drone governance framework can learn numerous important lessons from a comparative analysis of overseas regulatory approaches[42]. First and foremost, a comprehensive anti-drone law that unifies cybersecurity, privacy, criminal responsibility, and aviation safety issues into a single, cohesive statute is required. Currently[43], the overlap between many legal instruments makes accountability and enforcement difficult. A unified structure would facilitate efficient collaboration between law enforcement, defense, and civil aviation organizations, simplify institutional duties, and lessen jurisdictional ambiguity.

The use of cutting-edge technologies in the enforcement and regulatory framework is equally important. Rogue UAVs could be tracked and neutralized in real time with the use of automated counter drone [44] systems, drone forensics, and artificial intelligence-based detection techniques. A strong legal framework that guarantees accountability and transparency in its application should be in place to support this technological breakthrough. Furthermore, a specific legal framework that complies with international norms like the EU's [45] GDPR is required to address data protection and privacy. While preserving operational effectiveness, a statutory emphasis on consent-based data gathering and surveillance limitations would protect individual rights.

In addition to implementing changes at home, India must actively engage in regional security frameworks and ICAO-led projects to improve its international cooperation. Transnational drone dangers can be addressed and worldwide interoperability improved through cooperative systems for cross-border data sharing, research, and enforcement. Furthermore, public awareness efforts encouraging responsible drone use and enforcement agency capacity-building initiatives are critical to long-term sustainability. When combined, these changes would bring India's regulatory strategy into line with global best practices while balancing innovation, safety, and national security.[46]

IX. CONCLUSION

Drone technology has completely changed the legal landscape of today, blurring the lines between civilian and military uses, cyberspace and airspace, and the frequently conflicting demands of national security and privacy. The Bharatiya Nyaya Sanhita (BNS), Information Technology Act, and Unlawful Activities (Prevention) Act (UAPA) all support India's legal response, which is based on the Drone Rules, 2021 and represents a positive start toward organized regulation. To achieve a truly flexible and safe drone governance system, however, there are still major obstacles in the areas of institutional coordination, technology integration, and enforcement.

Three key pillars must support sustainable drone regulation, according to a comparative analysis of worldwide models, especially those of the ICAO, EU, US, and China: risk-based classification, technology enforcement, and rights-based accountability. These frameworks ensure that the advantages of UAV technology are not eclipsed by the possibility of its misuse by striking a balance between innovation and control. To address the complex issues of drone misuse and cross-border threats, India's future route calls for passing a comprehensive anti-drone law, putting strong data protection measures in place, and strengthening interagency and international cooperation.

---

[42] ICAO, *Annex 2 to the Convention on International Civil Aviation – Rules of the Air*, 11th Edition, 2005; ICAO Circular 328, *Unmanned Aircraft System (UAS) Operations in Civil Aviation*, 2011.

[43] *Drone Rules, 2021*, notified under Section 5A of the *Aircraft Act, 1934* (Act XXII of 1934), Ministry of Civil Aviation, Government of India.

[44] European Union Aviation Safety Agency (EASA), *Introduction to EU Drone Regulations*, 2020; FAA, *Part 107 – Small Unmanned Aircraft Systems*, 14 CFR Part 107, 2016.

[45] European Union, *General Data Protection Regulation (GDPR)*, Regulation (EU) 2016/679, 2016

[46] Department of Electronics and Information Technology (DeitY), Government of India, *Draft Data Protection and Privacy Guidelines for Emerging Technologies*, 2020; Ministry of Home Affairs, Government of India, *UAV Awareness and Capacity Building Initiatives*, 2021.

The future of drone regulation in India ultimately needs to shift from a reactive to a proactive legal paradigm, where justice and innovation coexist peacefully. By integrating technological innovation into a rights-aware legal framework, India can guarantee that the new "legal battles in the sky" are settled by law that is driven by responsibility, creativity, and the timeless values of justice rather than by conflict or force.