International Journal of Juridical Studies & Research (IJJSR), Vol. 1, Issue 2, December 2021
Page 1-19

LEGAL FRAMEWORK FOR DRONE REGULATION IN INDIA: CHALLENGES, COMPLIANCE, AND THE WAY FORWARD

VIKAS YADAV

Abstract

The rapid proliferation of drone technology has created unprecedented opportunities in sectors such as agriculture, logistics, disaster management, surveillance, and urban planning, while simultaneously raising complex legal, ethical, and security concerns. In India, drone regulation has witnessed a marked shift from the restrictive Civil Aviation Requirements (CAR), 2018 to the more liberalized Drone Rules, 2021, reflecting an effort to balance innovation with public safety. This paper traces the evolution of India's drone regulatory framework, examining the roles of institutional actors such as the Directorate General of Civil Aviation (DGCA), Ministry of Civil Aviation (MoCA), and Ministry of Home Affairs (MHA), alongside relevant airspace laws. It further analyzes critical issues of privacy, data protection, liability, and national security, situating them within constitutional jurisprudence and comparative international practices. The study identifies persisting gaps, including weak enforcement, fragmented institutional control, and inadequate safeguards against misuse, while offering recommendations for a dynamic, technologyneutral regulatory model that is both innovation-friendly and rights-oriented. Ultimately, the research argues that India's drone governance must evolve into a holistic framework that harmonizes domestic priorities with global standards, ensuring that drones become enablers of economic growth and security without compromising constitutional values.

Keywords

Drone Regulation; Civil Aviation; DGCA; Drone Rules, 2021; Privacy; Data Protection; National Security; Liability; Comparative Law; Unmanned Aerial Systems (UAS); Airspace Management; Constitutional Law.

Introduction to Drone Technology and Legal Issues

Unmanned Aerial Vehicles (UAVs), commonly known as drones, are aircraft systems that operate without an onboard human pilot and can be controlled remotely or programmed to fly autonomously using software-controlled flight plans. The International Civil Aviation Organization (ICAO) categorizes drones as part of the broader domain of Remotely Piloted Aircraft Systems (RPAS), a subset of unmanned aircraft systems (UAS).12 Drones are Increasingly used for a wide range of applications including defense and surveillance, agriculture, medical supply delivery, aerial cinematography, infrastructure monitoring, and disaster management.

In India, drones first attracted attention in defense operations, but their civil and commercial use has rapidly expanded in recent years. E-commerce companies have experimented with drone deliveries, while state agencies have deployed drones for COVID-19 surveillance and disaster relief operations.3 Despite their advantages, drones present serious challenges, including airspace safety, privacy violations, national security risks, and liability concerns. The 2021 Jammu Air Force Station attack, allegedly carried out using drones, highlighted the potential of drones being misused for terrorism.4

Legally, drones intersect with multiple domains: aviation law, privacy law, information technology law, and criminal law. India's regulatory framework has evolved from the Civil Aviation Requirements (CAR), 2018 issued by the Directorate General of Civil Aviation (DGCA), to the more liberalized Drone Rules, 2021, notified under the Aircraft Act, 1934. These rules categorize drones based on weight, mandate unique identification numbers, and set out operational restrictions, no-fly zones, and licensing requirements.5 However, gaps remain with respect to data

[1] International Civil Aviation Organization (ICAO), *Manual on Remotely Piloted Aircraft Systems (RPAS)*, Doc [2], 2015.

[3] Press Information Bureau, Government of India, *Use of Drones for COVID-19 Surveillance and Deliveries*, Ministry of Civil Aviation, April 2020.

[4] Ministry of Defence, Government of India, *Drone Attack at Jammu Air Force Station*, Press Release, June 2021.

[5] Ministry of Civil Aviation, *Drone Rules, 2021*, Notification under the Aircraft Act, 1934 (Gazette of India, 25 August 2021)

protection, liability in case of accidents, insurance coverage, and harmonization with global standards.

From a constitutional perspective, drones also raise privacy concerns under Article 21 of the Constitution of India, as recognized in Justice K.S. Puttaswamy v. Union of India6, where the Supreme Court affirmed the right to privacy as a fundamental right. Unauthorized drone surveillance, facial recognition integration, or data collection could amount to infringement of this right. Moreover, issues of criminal misuse are addressed under provisions of the Indian Penal Code, 1860 (IPC), Unlawful Activities (Prevention) Act, 1967 (UAPA), and Information Technology Act, 2000 (IT Act), depending on the nature of misuse.

Therefore, the legal framework governing drones must carefully balance fostering innovation and economic prosperity with protecting privacy, national security, and public safety.

Evolution of Drone Regulation in India (CAR 2018 to Drone Rules, 2021)

The regulation of drones in India has evolved in a phased manner, responding to both technological developments and security imperatives. Initially, drones were unregulated, and their use was largely restricted to defense establishments. However, the increasing proliferation of drones for civil and commercial purposes compelled the Directorate General of Civil Aviation (DGCA) and the Ministry of Civil Aviation (MoCA) to issue specific regulatory frameworks.

-The "No Permission, No Takeoff" Era (Pre-2018): In October 2014, the DGCA issued a public notice prohibiting the use of drones for any civil purpose without prior approval, citing safety and security concerns.7 This effectively meant that private individuals and companies could not lawfully operate drones in India until a regulatory mechanism was put in place.

-Civil Aviation Requirements (CAR), 2018:After years of deliberation, the DGCA introduced the Civil Aviation Requirements (CAR) on Remotely Piloted Aircraft Systems (RPAS), effective from

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

[7] Directorate General of Civil Aviation (DGCA), Public Notice No. 05-13/2014-AED, "Use of Unmanned Aerial Vehicle (UAV)/Unmanned Aircraft Systems (UAS) for Civil Applications," 7 October 2014.

1 December 2018.8 This marked India's first attempt to comprehensively regulate drone operations.

Key features of CAR 2018 included:

- Drones were categorized into Nano (≤250g), Micro (250g–2kg), Small (2–25kg), Medium (25–150kg), and Large (>150kg).
- Digital Sky Platform through an online portal for granting permissions under the principle of "No Permission, No Takeoff" (NPNT).
- Operational Restrictions included Ban on flying in "No Drone Zones" such as airports, international borders, State Secretariat Complex in State Capitals, and military installations.
- Mandatory Licensing for all categories were required prior permission and operator permits,except for nano drones.
- RPAS were required to comply with air traffic regulations, with mandatory geo-fencing and flight logging.

While CAR 2018 was a progressive step, it was criticized for being restrictive and bureaucratic, limiting innovation in the commercial drone sector.9

-Draft Unmanned Aircraft System Rules, 2021: In March 2021, the MoCA released the Unmanned Aircraft System (UAS) Rules, 2021, notified under the Aircraft Act, 1934.10 These rules sought to replace CAR 2018 with a more detailed framework, covering manufacturing, import, testing, certification, and insurance of drones.

However, the UAS Rules, 2021, were heavily criticized by industry stakeholders for being overregulated and compliance-heavy. The Federation of Indian Chambers of Commerce and Industry (FICCI) noted that the rules imposed over 70 forms of permissions, creating barriers to entry for start-ups and innovators.11

---

[8] DGCA, *Civil Aviation Requirements, Section 3 – Air Transport, Series X, Part I: Requirements for Operation of Civil Remotely Piloted Aircraft Systems (RPAS)*, effective 1 December 2018.
[9] NITI Aayog, *Harnessing Drone Technology in India*, Discussion Paper, 2019.
[10] Ministry of Civil Aviation, *Unmanned Aircraft System Rules, 2021*, Gazette Notification, 12 March 2021.
[11] Federation of Indian Chambers of Commerce and Industry (FICCI), *Comments on UAS Rules, 2021*, Position Paper, April 2021.

-Drone Rules, 2021 – A Liberalized Regime: Responding to industry feedback, the Government repealed the UAS Rules within five months and introduced the Drone Rules, 2021 on 25 August 2021.12 These rules represented a paradigm shift toward liberalization and ease of doing business.

Salient features of the Drone Rules, 2021: ● Reduced Compliance Burden: The

number of forms reduced from 25 to 5.

- Registration & Certification: Unique Identification Number (UIN) and certification for drones made simpler.
- Weight Categories: Continuation of nano to large categorization but with relaxed operational requirements.
- Abolition of NPNT Mandate for Many Categories: Simplified "green zones" for drone operations without prior permission up to 400 ft.
- Promotion of Domestic Manufacturing: Encouragement of Indian-made drones through Production-Linked Incentive (PLI) schemes.
- Drone Corridors: Plans for dedicated corridors for drone deliveries and a future Unmanned Aircraft Traffic Management (UTM) system.

The Drone Rules, 2021, were seen as industry-friendly, balancing safety with innovation. Yet, challenges remain, particularly regarding data protection, privacy safeguards, and national security risks, as highlighted by the Jammu drone attack in June 2021.1314

-Towards a Drone Ecosystem: Since 2021, India has further amended the rules to encourage drone adoption. The Drone (Amendment) Rules, 2022 abolished the requirement for remote pilot certificates for operating non-commercial drones up to 2 kg.15 Coupled with the "Drone Shakti" initiative announced in the Union Budget 2022–23, India aims to become a global drone hub by 2030.

---

[12] Ministry of Civil Aviation, *Drone Rules, 2021*, Notification under the Aircraft Act, 1934, Gazette of India, 25 August 2021.

[13] Ministry of Defence, Government of India, *Press Release on Drone Attack at Jammu Air Force Station*, June

[14] .

[15] Ministry of Civil Aviation, *Drone (Amendment) Rules, 2022*, Gazette Notification, 15 February 2022.

Institutional and Legal Framework

The regulation of drones in India operates within a multi-agency framework, involving civil aviation authorities, security agencies, and the central government. The complexity arises because drones intersect not only with aviation law but also with national security, privacy, and criminal law.

Directorate General of Civil Aviation (DGCA):The DGCA is the primary regulator of civil aviation in India, functioning under the Aircraft Act, 1934 and the Aircraft Rules, 1937. It is entrusted with safety oversight, airworthiness certification, licensing, and regulatory approvals.Civil Aviation Requirements (CAR), 2018 and later the Drone Rules, 2021 were both framed under DGCA's regulatory domain.16

DGCA administers the Digital Sky Platform, a technology-driven online system for drone registration, flight authorization, and operator licensing.It also implements the "No Permission, No Takeoff (NPNT)" mechanism, ensuring that drones cannot take off without digital clearance from the regulator.17Thus, the DGCA acts as the technical and operational regulator for drone safety, certification, and compliance.

Ministry of Civil Aviation (MoCA):The MoCA provides the overarching policy framework for civil aviation in India, including drones.It notified the Drone Rules, 2021 under Section 5 of the Aircraft Act, 1934.18MoCA is responsible for developing India's drone ecosystem, including policy initiatives like the Drone Shakti scheme (2022) and the PLI scheme for drone manufacturing. The Ministry also collaborates with state governments for airspace zoning, infrastructure creation (like drone corridors), and integration of drones with Unmanned Aircraft Traffic Management (UTM) systems.In short, MoCA functions as the policy-making authority, while DGCA acts as the regulator.

---

[16] DGCA, *Civil Aviation Requirements, Section 3 – Air Transport, Series X, Part I: RPAS Requirements*, effective 1 December 2018.

[17] Ministry of Civil Aviation, *NPNT Framework under Digital Sky Platform*, Policy Document, 2019.

[18] Ministry of Civil Aviation, *Drone Rules, 2021*, Gazette Notification, 25 August 2021

Ministry of Home Affairs (MHA):Given the security implications of drones, the MHA plays a crucial role.It is responsible for issuing security clearances for drone imports, operations near sensitive installations, and for foreign entities wishing to operate drones in India.19MHA also governs law enforcement usage of drones, including surveillance, anti-terror operations, and crowd monitoring.Following incidents like the Jammu Air Force Station drone attack (2021), MHA has strengthened coordination with DGCA for establishing No Drone Zones around defense and strategic assets.20State police authorities, functioning under MHA's framework, are empowered to enforce criminal liability in cases of drone misuse under the Indian Penal Code (IPC), Unlawful Activities (Prevention) Act, 1967 (UAPA), and other security laws. Thus, MHA acts as the security regulator, ensuring drones are not misused for terrorism or unlawful surveillance.

Airspace Laws and the Indian Air Force (IAF):The Indian airspace is a sovereign entity governed by the Aircraft Act, 1934 and managed jointly by the Airports Authority of India (AAI) and the Indian Air Force (IAF) under the Ministry of Defence. Drone operators must comply with airspace zoning classified into Green, Yellow, and Red zones as per the Drone Rules, 2021.

- ➢ Green Zone: Permission-free up to 400 feet.
- ➢ Yellow Zone: Controlled airspace requiring Air Traffic Control (ATC) permission.
- ➢ Red Zone: Strictly prohibited unless authorized by the central government.21

The IAF and National Air Traffic Services (NATS) oversee air traffic integration, preventing drones from interfering with manned aircraft operations.Unauthorized drone operations near airports, borders, or defense installations are punishable under the Aircraft Act, 1934 and criminal laws.

Other Supporting Legislations:Information Technology Act, 2000 (IT Act) governs liability for data breaches or cyber misuse of drones. Indian Penal Code, 1860 (IPC) is applicable for trespass, nuisance, or endangerment caused by drones.Cinematograph Act, 1952 & Indian Telegraph Act,

[19] Ministry of Home Affairs, *Standard Operating Procedures on Drone Operations for Security Clearance*, Circular, 2020.
[20] Ministry of Defence, *Press Release on Jammu Drone Attack*, June 2021.
[21] Drone Rules, 2021, Rule 22 – *Classification of Airspace Zones*.

1885 is Applicable for filming/telecommunications involving drones.Personal Data Protection Bill (pending) is expected to have implications for drone-based data collection and privacy.

Institutional Interplay and Challenges: While DGCA and MoCA regulate drones for civil use, MHA and MoD are responsible for security and defense oversight. This creates overlapping jurisdictions and, at times, regulatory ambiguities. For instance, while DGCA may permit a drone for commercial use, MHA may restrict its operations near sensitive borders or government installations.Thus, India's institutional framework reflects a multi-agency balancing act, where aviation safety, national security, and innovation must be harmonized.

Privacy, Security, and Liability Concerns

The rapid integration of drones into civil and commercial domains has raised significant concerns in three interrelated areas: privacy, security, and liability. These issues highlight the challenges of balancing innovation with constitutional rights, national security, and accountability.

Privacy Concerns: Drones equipped with high-resolution cameras, thermal sensors, and facial recognition technology pose risks of mass surveillance and data intrusion.

In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Supreme Court recognized the right to privacy as intrinsic to Article 21 of the Constitution.22 Drone surveillance without consent could infringe upon informational and spatial privacy.India lacks a comprehensive data protection statute (the Personal Data Protection Bill has been pending). As a result, drone-collected personal data lacks specific statutory safeguards. Police use drones for crowd control and monitoring protests, raising concerns of chilling effects on free speech and assembly under Articles 19(1)(a) and 19(1)(b).23The European Union's General Data Protection Regulation (GDPR) mandates purpose limitation and data minimization, but India's framework does not impose similar

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

[23] Human Rights Law Network (HRLN), *Report on the Use of Drones for Crowd Control in India*, 2020.

obligations on drone operators.Thus, the privacy dimension remains one of the weakest aspects of India's current drone regulation.

Security Concerns: Drones present serious national security and public safety challenges, particularly due to their potential for weaponization and unlawful use.The 2021 Jammu Air Force Station attack using explosive-laden drones underscored drones as tools of cross-border terrorism.24Drones are increasingly used for smuggling arms, drugs, and contraband across borders. Security agencies like the Border Security Force (BSF) have intercepted multiple instances of cross-border drone incursions in Punjab and Jammu.25Unauthorized drones pose collision risks to commercial aircraft. The DGCA prohibits flying near airports and in red zones, but enforcement remains difficult.Many commercial drones are GPS-enabled and Wi-Fi controlled, making them susceptible to hacking and manipulation. Lack of mandatory cybersecurity standards creates vulnerabilities.

The Ministry of Home Affairs (MHA) and Ministry of Defence (MoD) have therefore emphasized the need for counter-drone technologies and coordination between law enforcement and aviation regulators.

Liability Concerns:The issue of liability arises when drones cause harm to persons, property, or air traffic.

- Civil Liability: Under the Aircraft Act, 1934 and Aircraft Rules, 1937, drones are classified as "aircraft." This implies that general principles of aviation liability apply.
  However, no separate liability regime exists specifically for drones. Tort Law: Victims of drone accidents may seek remedies under negligence and nuisance. For instance, unauthorized drone flights over private property may amount to trespass or invasion of privacy.
- Insurance: The Unmanned Aircraft System (UAS) Rules, 2021 initially mandated thirdparty insurance, but the Drone Rules, 2021 liberalized this requirement, leaving a regulatory vacuum.26

[24] Ministry of Defence, *Press Release on Drone Attack at Jammu Air Force Station*, June 2021.
[25] Border Security Force (BSF), *Annual Report 2021-22: Interceptions of Drone-based Smuggling at Borders*.
[26] Ministry of Civil Aviation, *Drone Rules, 2021*, Gazette Notification, 25 August 2021

- Criminal Liability: Operators flying drones in restricted zones or for unlawful purposes may face prosecution under the IPC, UAPA, 1967, and IT Act, 2000.
- Product Liability: In cases of malfunction, liability may extend to manufacturers and software developers, especially as drones rely heavily on autonomous navigation.

The absence of a clear statutory liability and insurance framework in India poses risks both for victims and for the drone industry, which faces uncertainty in case of accidents.

Balancing Innovation and Regulation:The challenge for India lies in achieving a balanced framework of encouraging innovation and adoption of drones in agriculture, healthcare, and logistics. Protecting individuals from privacy violations. Safeguarding national security through counter-drone measures. Ensuring compensation and accountability in case of accidents or misuse.Without addressing these concerns, the legal regime risks being either too restrictive (stifling growth) or too liberal (endangering security and rights).

A Global Look at Drone Regulations

United States (FAA): Their system centers on small drone operations under 14 CFR Part 107, with the option to get waivers for more advanced flights, like at night or over people. A major focus is Remote ID, which is now required for most registered drones to ensure they can be identified remotely. The FAA is continuing to expand operations through waivers as it works on broader integration and standardized Remote ID27

European Union (EASA): The EU uses a risk-based model, sorting operations into Open, Specific, and Certified categories under Reg. (EU) 2019/947 and 2019/945. This approach makes the pilot's skills, the drone's class, and where it's flying central to the rules. The EU has also enabled “Uspace” airspace to support more automated and higher-density flights.28

[27] "Drone Laws by Country: The Ultimate Guide," Flying Glass, accessed August 29, 2025, https://www.flyingglass.com.au/guide-to-drone-laws-by-country/#:~:text=Drone%20regulations%20vary%20widely%20from,There%20is%20no%20universal%20standard

[28] "Regulation of unmanned aerial vehicles," Wikipedia, last modified August 25, 2025,https://en.wikipedia.org/wiki/Regulation_of_unmanned_aerial_vehicles.

United Kingdom (CAA): After Brexit, the UK's rules are quite similar to the EU's risk framework, implemented through its master policy, CAP 722. They also have specific registration and competency requirements. The CAA issues special "operational authorizations" for certain missions29

China (CAAC): China's system is very focused on oversight and requires "real-name" registration for all civil drones over 250 grams. Manufacturers and owners must register their drones and attach a label to them. The government issues broader operational standards, and permissions get stricter around cities and borders.30

Australia (CASA): Australia has a practical, category-based approach with "excluded" pathways. Under CASR Part 101, low-risk commercial operations with drones under 2 kg can fly without a license if the pilot is accredited and follows standard conditions. Heavier drones or flights beyond visual line of sight require specific authorizations.

Singapore (CAAS): Singapore's system is permit-led, with a strong emphasis on urban safety. Many activities, especially those near people, require both an Operator and an Activity Permit. The country also has detailed rules on drone registration, remote identification, pilot licensing, and nofly zones.

India: India has undergone a significant liberalized pivot. The country moved from the restrictive CAR 2018 to the more flexible Drone Rules, 2021, which simplified forms and enabled permission-free flights in "green zones" within limits. Everything is anchored on the Digital Sky platform, and future policies aim to scale up the drone ecosystem.

Judicial Interpretations

Right to Privacy and Aerial Surveillance:Indian courts have not yet delivered a landmark judgment specifically on drones. However, privacy jurisprudence lays the foundation in Justice K.S.

---

[29] "Guide to Drone Laws by Country," Flying Glass, accessed August 29, 2025,https://www.flyingglass.com.au/guide-to-drone-laws-by-country/.

[30] UAV Coach. (n.d.). *Drone Laws in China*. UAV Coach.https://uavcoach.com/drone-laws-in-china/

Puttaswamy (Retd.) v. Union of India (2017)where The Supreme Court recognized privacy as a fundamental right under Article 21.31 This extends to informational privacy and spatial privacy, directly relevant to drone-based surveillance by state or private actors. Any unauthorized aerial surveillance using drones could thus be challenged as unconstitutional.

In People's Union for Civil Liberties v. Union of India (1997) Though concerning telephone tapping, the Court emphasized that surveillance without statutory safeguards violates privacy rights.32 By analogy, warrantless drone surveillance would require judicial scrutiny.Thus, while no drone-specific privacy case exists, constitutional principles make unauthorized aerial surveillance vulnerable to challenge.

Property Rights and Airspace Ownership: In the seminal case of United States v. Causby (1946, US Supreme Court) the Court held that while airspace is a public highway, property owners have rights to "immediate reaches of the enveloping atmosphere" necessary for the use and enjoyment of land.33 This principle has influenced global drone liability debates and may be persuasive for Indian courts when balancing low-altitude drone flights against private property rights.

Indian jurisprudence has not explicitly defined property rights in low airspace, but principles of trespass and nuisance under tort law as in the case of Shiv Kumar v. State of Haryana, 199434 could apply if drones interfere with property use.

National Security and Public Safety: Indian courts have recognized that individual rights can be reasonably restricted in the interest of national security. InA.K. Gopalan v. State of Madras (1950) and later ADM Jabalpur v. Shivkant Shukla (1976), the judiciary acknowledged wide state powers in security contexts.35Applied to drones, courts may be inclined to uphold restrictions in red zones, border areas, and near strategic installations, even if challenged on grounds of commercial hardship.

---

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

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

[33] *United States v. Causby*, 328 U.S. 256 (1946).

[34] *Shiv Kumar v. State of Haryana*, AIR 1994 SC 1794.

[35] *A.K. Gopalan v. State of Madras*, AIR 1950 SC 27; *ADM Jabalpur v. Shivkant Shukla*, AIR 1976 SC 1207.

Civil and Criminal Liability: While no Indian precedent specifically addresses drone accidents, courts have consistently applied strict liability principles in hazardous activities (M.C. Mehta v. Union of India, Oleum Gas Leak case, 1987).36

If drones are classified as "dangerous activities", courts may impose absolute liability for harm caused, regardless of negligence. This could shape judicial reasoning in future drone accident cases. riminally, unauthorized drone use in sensitive areas could be interpreted under IPC Section 287, 336-338 (negligent conduct endangering life), and courts would likely rely on established negligence standards.

Comparative Judicial Perspectives: InSinger v. City of Newton,(2017, US District Court, Massachusetts)the Court struck down parts of a municipal drone ordinance for conflicting with FAA regulations.37These highlights judicial deference to central aviation regulators, a principle likely to apply in India (DGCA vs. state restrictions).

The court in Huerta v. Pirker,recognized drones as "aircraft," subject to FAA jurisdiction.38 Indian courts could adopt a similar interpretation under the Aircraft Act, 1934. European Court of Human Rights (ECHR) jurisprudence on surveillance (e.g., Roman Zakharov v. Russia, 2015)39 may guide Indian courts in balancing drone-enabled state surveillance against human rights.

Judicial interpretations of drone-related issues in India are still nascent and indirect, derived mostly from constitutional privacy law, tort liability, and aviation statutes. However, comparative jurisprudence especially from the US, EU, and ECHR is likely to influence Indian courts as drone litigation expands. Courts in India are expected to apply a balancing test: safeguarding fundamental rights (privacy, property, safety) while allowing the state broad powers to regulate drones for national security and airspace safety.

---

[36] *M.C. Mehta v. Union of India* (Oleum Gas Leak Case), (1987) 1 SCC 395
[37] *Singer v. City of Newton*, 284 F. Supp. 3d 125 (D. Mass. 2017).
[38] *Huerta v. Pirker*, NTSB Order EA-5730 (2014).
[39] *Roman Zakharov v. Russia*, European Court of Human Rights, App. No. 47143/06, Judgment of 4 Dec 2015.

Challenges and Gaps in Indian Drone Regulation

Enforcement & Compliance Gaps: Although the Drone Rules, 2021 and the Digital Sky ecosystem create a regulatory architecture, on-ground enforcement is inconsistent. State police and local authorities often lack statutory clarity and technical capacity to detect and act on illegal flights; this has led to arrests in localized incidents but uneven deterrence nationwide.40Privacy and Data-Protection Vacuum: India still lacks a comprehensive, operational data-protection statute that directly addresses drone-collected personal data. While regulators claim the Drone Rules contain privacy safeguards, commentators and privacy experts argue the rules leave significant gaps on purpose limitation, retention, third-party sharing, and redress for individuals whose data are captured by drones. This regulatory lacuna complicates oversight of police and commercial surveillance use41.

National Security & Counter-Drone Capability Shortfalls: Drones can be weaponized, used for smuggling, or for covert surveillance. High-profile incidents (e.g., attacks and cross-border incursions) have exposed weaknesses in detection and response; several states and agencies are procuring counter-drone systems, but a coherent national counter-drone doctrine and interoperable detection network remain works in progress.42

Airspace Management & UTM Integration: India's color-zoned approach (green/yellow/red) is a useful start, but scaling to high-density operations (BVLOS, delivery corridors, urban air mobility) requires a mature Unmanned Traffic Management (UTM) system, robust Remote ID, and real-time data sharing with ATC. Timelines and technical standards for nationwide UTM and Remote ID adoption are still evolving.43

---

[40] Mishra, P. (2025, August 29). *Empowering State Police to Enforce Drone Regulations: A Legislative Need in India's Evolving Space*. The Times of India.https://timesofindia.indiatimes.com/city/lucknow/empowering-statepolice-to-enforce-drone-regulations-a-legislative-need-in-indias-evolving-space/articleshow/122189423.cms

[41] Mishra, P. (2022, December 2). *Drone Rules, 2021: Privacy Concerns Raised in Parliament*. MediaNama.https://www.medianama.com/2022/12/223-drone-rules-2021-privacy-concerns-parliament-4/

[42] Sharma, S., & Kaur, R. (2025). *Counter-Drone Technologies: A Comprehensive Review*. International Journal of Research and Publications, *6*(5), 1-15.

[43] Singh, S., &Gunjal, S. (2025, July 24). *Fast-Tracking the Flight of India's Drone Industry*. Observer Research Foundation.https://www.orfonline.org/research/fast-tracking-the-flight-of-india-s-drone-industry

Fragmentation between Central and State Roles: A recurring governance problem is jurisdictional fragmentation. DGCA/MoCA frame aviation rules while MHA/MoD and state police manage security and local enforcement. This multi-agency structure produces overlaps, delays in approvals (especially near sensitive installations), and uncertainty for commercial operators. Calls to better define state police powers and streamline coordination have grown louder.44

Technology Standards, Type-Certification & Illegal Imports: Industry and enforcement agencies report a rising problem of uncertified/black-market drones, often bypassing typecertification and safety checks. This raises safety and security risks and undermines domestic manufacturers. Import controls, enforcement at ports, and stricter type-certification processes are needed but unevenly implemented.

Liability, Insurance & Redress Mechanisms:The rules liberalized several compliance burdens but left third-party liability and mandatory insurance frameworks under-specified. In the event of collisions, privacy breaches, or property damage, victims may face procedural hurdles in claiming timely compensation; insurers and courts will need clearer statutory guidance on standards of care and strict/absolute liability for certain hazardous drone uses.4546

Awareness, Training & Institutional Capacity: A significant portion of unsafe or illegal drone activity stems from operator ignorance unregistered drones, flights in no-fly zones, and noncompliance with Digital Sky protocols. Scaling training (remote pilot competency), public awareness campaigns, and capacity-building in regulatory and enforcement agencies is essential.47 Rapid Tech Evolution Outpacing Rules:Drones are converging with AI, computer vision, encrypted comms, and autonomy. Regulatory instruments are often reactive; by the time

---

[44] iSPIRT. (2021, August 29). *iSPIRT Response to the Drone Rules, 2021*. iSPIRT.https://pn.ispirt.in/ispirt-response-drone-rules-2021/

[45] Gupta, R. (2025). *Drone Regulation in India: A Critical Analysis*. Research Journal of Policy & News, *1*(1), 1-

[46] .https://rjpn.org/jetnr/papers/JETNR2410008.pdf

[47] LexStart Partners. (2021, August 26). *Drones and Drone Rules, 2021*. LexStart Partners.https://www.lexstartpartners.com/post/drones-and-drone-rules-2021

rules are updated, capabilities (autonomous swarm behavior, spoof-resistant comms) may have moved ahead. A mechanism for adaptive, tech-neutral rulemaking is therefore necessary.48

Recommendations and Way Forward

The regulation of drones in India is still in its formative stages, and while the Drone Rules, 2021 have marked a decisive shift towards liberalization, several areas require urgent attention to create a holistic and future-ready framework. A key recommendation is the adoption of a robust data protection and privacy regime aligned with global standards. The recently enacted Digital Personal Data Protection Act, 2023 provides an opportunity to integrate drone-specific safeguards, such as strict purpose limitation, obligations for secure storage, and explicit consent mechanisms before data collection in civilian applications. Embedding such protections within drone regulation would address growing anxieties around surveillance and ensure proportional use of drone technology.

Equally critical is the strengthening of airspace management and counter-drone infrastructure. The gradual rollout of an indigenous Unmanned Traffic Management (UTM) system, interoperable with manned aviation and compliant with International Civil Aviation Organization (ICAO) standards, should be accelerated. Remote ID protocols and geofencing must be made mandatory to ensure accountability and prevent rogue operations. In parallel, India needs a unified national counter-drone strategy that integrates the capacities of the Ministry of Defence (MoD), Ministry of Home Affairs (MHA), and state enforcement agencies, supported by indigenous R&D in detection and neutralization systems.

Another pressing reform is the clarification of liability and insurance frameworks. The current absence of mandatory third-party liability insurance exposes both victims and operators to uncertainties in the aftermath of accidents. Borrowing from EU and U.S. practices, India should mandate baseline insurance coverage proportionate to drone weight and risk profile. Establishing fast-track claims mechanisms under aviation insurance law would also strengthen confidence among commercial operators and consumers.

---

[48] Sharma, S., & Kaur, R. (2025). *Counter-Drone Technologies: A Comprehensive Review*. International Journal of Research and Publications, *6*(5), 1-15.

Institutional reform is equally important. At present, drone governance is fragmented across the DGCA, MoCA, MHA, and state agencies. A single-window inter-agency coordination mechanism, possibly through a National Drone Authority, could minimize bureaucratic overlap and streamline licensing, security clearances, and enforcement. Decentralization of certain responsibilities to state governments, while maintaining national security oversight, would allow context-specific regulation without diluting central control.

Further, promoting domestic manufacturing and innovation is vital to reducing dependence on imports and curbing black-market drones. Incentives under Atmanirbhar Bharat and the Production Linked Incentive (PLI) schemes should be extended to drone components, sensors, and counter-drone systems, coupled with stricter enforcement against uncertified imports. This dual strategy would strengthen supply-chain security while boosting India's position in the global drone economy.

Capacity-building remains a foundational requirement. Expanding certified remote pilot training organizations, standardizing curricula, and introducing tiered licensing for different drone categories would enhance operator professionalism. Parallelly, large-scale awareness campaigns on the Digital Sky platform, flight restrictions, and penalties for non-compliance would minimize inadvertent violations. Special focus should be placed on equipping law enforcement agencies with technical know-how to detect and regulate drones at the ground level.

Finally, the legal framework must remain dynamic and adaptive. Instead of static, technologyspecific rules, India should adopt a principles-based, technology-neutral approach that can flexibly accommodate emerging innovations such as autonomous swarms, AI-driven analytics, and urban air mobility. Periodic regulatory sandboxes where operators, regulators, and researchers can experiment within controlled environments would allow law to evolve alongside technology, minimizing regulatory lag while safeguarding public interest.

In sum, the way forward for drone regulation in India lies in striking a careful balance: encouraging innovation and commercial growth while embedding safeguards for privacy, security, and accountability. A coordinated, forward-looking regulatory framework will not only mitigate risks

but also enable India to harness drones as engines of technological progress and economic opportunity.

Conclusion

The regulation of drones in India has evolved significantly within a short span of time, reflecting the tension between technological innovation and the imperatives of law and security. From the restrictive Civil Aviation Requirements (CAR), 2018 to the more liberal and facilitative Drone Rules, 2021, India has sought to foster a regulatory environment that supports innovation while addressing the risks posed by unmanned aerial systems. Yet, as the analysis demonstrates, the existing framework continues to grapple with complex challenges relating to privacy, national security, liability, and institutional coordination.

Judicial interpretations, particularly in the domain of privacy rights post-K.S. Puttaswamy v. Union of India, remind us that drone regulation cannot be confined to aviation safety alone but must align with constitutional protections. At the same time, incidents such as the Jammu Air Force Station attack underscore the pressing national security concerns that demand robust counter-drone policies and technological preparedness. The comparative analysis with international jurisdictions further highlights the need for India to harmonize its standards with global best practices while tailoring them to domestic realities.

Moving forward, the recommendations outlined strengthening privacy safeguards, mandating liability insurance, establishing a unified governance mechanism, promoting indigenous manufacturing, and adopting adaptive, technology-neutral rules are crucial to bridging the regulatory gaps. A forward-looking framework that balances security with innovation, central oversight with decentralized implementation, and commercial growth with fundamental rights will enable India to fully realize the transformative potential of drone technology.

In conclusion, drones represent both an opportunity and a challenge. If governed through a dynamic, inclusive, and rights-oriented legal framework, they can emerge as vital tools in sectors ranging from agriculture and logistics to national security and disaster management. However, without adequate safeguards, they risk becoming vectors of insecurity, surveillance, and liability disputes. The path ahead, therefore, lies in building a regulatory ecosystem that is not only

compliant with international aviation norms but also responsive to India's constitutional values and developmental priorities.