

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

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

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

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

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

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

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

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

AUTONOMOUS DRONES IN INDIA: TOWARDS A RISK-BASED LIABILITY FRAMEWORK

AUTHORED BY - AKSHAT PANDEY

ABSTRACT

The increasing deployment of autonomous drones in India is creating new legal questions concerning responsibility for accidents and other forms of harm. India's existing drone regulatory framework has established important requirements governing the manufacture, registration, operation and safety of unmanned aircraft systems, while initiatives such as DigitalSky, UAS traffic management and incentives for domestic manufacturing have sought to facilitate the responsible growth of the sector. However, increasing autonomy challenges the traditional assumption that the operator should bear primary responsibility for every consequence arising from a drone's operation.

This article examines whether India's existing aviation-law framework adequately addresses liability arising from autonomous drone operations. It analyses the potential responsibility of operators, owners, manufacturers and software developers and considers the extent to which existing principles of negligence, product liability, insurance and causation can address technologically complex accidents. The article further examines risk-based regulatory approaches adopted in the European Union and the United States. It argues that India should adopt a proportionate and shared liability framework based on the degree of autonomy, operational risk, control and contribution to the harm. Such a framework should be supported by appropriate insurance requirements, preservation of flight and system data, and clear compliance standards. The proposed approach seeks to protect victims while providing regulatory certainty that encourages technological innovation, domestic manufacturing and the continued development of India's autonomous drone ecosystem.

Keywords: Autonomous Drones; Unmanned Aircraft Systems (UAS); Drone Regulation; Civil Liability; Product Liability; Risk-Based Liability; Artificial Intelligence; Aviation Law; India..

I. INTRODUCTION

Unmanned Aircraft Systems (UAS), commonly known as drones, have emerged as an important component of India's technological and economic development. Their applications now extend beyond recreational use to agriculture, infrastructure inspection, logistics, disaster management, surveying and public administration. Recognising this potential, India has progressively developed a regulatory environment intended not merely to control drone operations but also to facilitate their responsible growth. The Drone Rules 2021 represented an important step towards simplifying the regulatory framework, while subsequent initiatives have sought to encourage domestic manufacturing, research and technological development.¹

The government's approach has also linked the growth of the drone sector with technological self-reliance. The Production Linked Incentive (PLI) Scheme for Drones and Drone Components was introduced with the stated objective of making Indian drone manufacturing self-sustaining and globally competitive and developing India as a global hub for the research, development, testing, manufacturing and operation of drones.² This policy direction demonstrates that drone regulation in India must balance two legitimate objectives: ensuring public safety and accountability while creating sufficient regulatory certainty for innovation and investment.

The next challenge arises from the increasing autonomy of unmanned aircraft. A remotely piloted drone remains substantially dependent upon human instructions, whereas an automated or autonomous system can perform increasingly significant aspects of flight without continuous human intervention. As autonomous capabilities develop, the traditional assumption that the person operating the aircraft is necessarily the person responsible for every consequence of its operation becomes more difficult to sustain.

This creates a distinct legal question. If an autonomous drone causes injury or property damage because of a software error, defective design, sensor failure or an interaction between several technological components, responsibility may potentially extend beyond the operator to the manufacturer, software developer or maintenance provider. The issue is therefore not whether India should permit autonomous drone technology, but whether its liability framework can evolve alongside that technology.

The Bharatiya Vayuyan Adhiniyam 2024 provides the contemporary statutory foundation for

¹ Drone Rules 2021, GSR 589(E), Gazette of India, Extraordinary, pt II, sec 3(i) (25 August 2021).

² Ministry of Civil Aviation, Guidelines for the Operation of Production Linked Incentive Scheme (PLI) for Drones and Drone Components (29 November 2022) para 1.1 <<https://www.civilaviation.gov.in/node/3168>> accessed 14 September 2026.

the regulation and control of aircraft in India and came into force on 1 January 2025.³ Building upon this framework, India can address emerging autonomous-drone risks without abandoning its broader objective of technological development.

This article argues that India should adopt a proportionate, shared and risk-based liability framework, under which responsibility is determined by the degree of autonomy, control, fault and contribution to the risk. Such an approach can protect individuals and property while providing manufacturers and operators with predictable legal standards, thereby supporting safe innovation and the continued development of India's domestic drone ecosystem.

II. INDIA'S EXISTING DRONE REGULATORY FRAMEWORK AND THE EMERGENCE OF AUTONOMY

India has developed a relatively structured regulatory architecture for civil drone operations. The Drone Rules 2021 substantially simplified the regulatory framework by providing rules governing the manufacture, possession, operation, transfer and use of drones. The Rules also introduced a system of digital registration and certification through the DigitalSky platform, thereby moving significant aspects of drone regulation towards an online and technology-enabled model.⁴ The framework has subsequently been amended, including through the Drone (Amendment) Rules 2022, while the Drone (Amendment) Rules 2023 further demonstrate that the regulatory framework continues to evolve with the development of the sector.⁵

A. Classification and Operational Regulation

The Drone Rules classify drones according to their maximum all-up weight and establish corresponding regulatory requirements.⁶ The Rules recognise remotely piloted, model remotely piloted and autonomous UAS as subcategories, but do not separately define an 'automatic operation'. For analytical clarity, an automatic operation may be distinguished from an autonomous operation: in the former, the UAS follows pre-programmed instructions while the remote pilot remains able to intervene, whereas in the latter the remote pilot cannot intervene.⁷

³ *Bharatiya Vayuyan Adhiniyam 2024, ss 1(2), 2; Ministry of Civil Aviation, Notification SO 5646(E), Gazette of India, Extraordinary, pt II, sec 3(ii) (31 December 2024).*

⁴ Drone Rules 2021, rr 2, 3(1)(g), 6-19.

⁵ Drone (Amendment) Rules 2022, GSR 108(E), Gazette of India, Extraordinary, pt II, sec 3(i) (11 February 2022); Drone (Amendment) Rules 2023, GSR 715(E), Gazette of India, Extraordinary, pt II, sec 3(i) (27 September 2023).

⁶ *Drone Rules 2021, r 5.*

⁷ Drone Rules 2021, rr 3(1)(zb), 4(2); Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft OJ L152/45, art 2(17); European Union Aviation Safety Agency, Easy Access Rules for Unmanned Aircraft Systems (Revision from June 2026) GM1 art 2(17)

The increasing significance of autonomy therefore does not necessarily require India to abandon its existing regulatory architecture. Rather, it requires the existing framework to account for a technological development in which decision-making is increasingly distributed between human operators and automated systems.

B. DigitalSky and UAS Traffic Management

DigitalSky represents an important feature of India's approach because it integrates regulatory processes with a digital platform. The National Unmanned Aircraft System Traffic Management (UTM) Policy Framework further develops this approach by envisaging a software-based ecosystem connecting the DigitalSky platform with UTM service providers, UAS operators, remote pilots, manufacturers and other stakeholders.⁸ The framework also recognises the importance of automated information exchange and coordination in managing unmanned aircraft traffic.

This technology-enabled regulatory model is particularly significant as drone operations expand beyond conventional visual-line-of-sight activities. By creating a common digital architecture for stakeholders, India has sought to make the integration of unmanned aircraft into the wider aviation system more systematic while preserving the regulatory authority of the DGCA and other relevant authorities.⁹

C. Autonomy and the Next Stage of Regulation

The emergence of autonomous drones nevertheless introduces a new dimension. Existing regulatory requirements can establish who is authorised to operate a drone, the conditions under which it may operate and the safety standards that must be observed. They do not, by themselves, completely answer the question of who should bear responsibility when an autonomous decision causes harm.

This issue is particularly relevant because autonomy can shift decision-making away from the person operating the aircraft. A drone may alter its route, avoid an obstacle or respond to changing conditions through software without receiving a specific instruction from the operator. The potential causes of an accident may consequently extend to the aircraft's design,

<<https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems>> accessed 14 September 2026.

⁸ Ministry of Civil Aviation, National Unmanned Aircraft System (UAS) Traffic Management Policy Framework (24 October 2021) 4–5 <https://www.civilaviation.gov.in/sites/default/files/migration/National-UTM-Policy-Framework-2021_24_Oct_2021.pdf> accessed 14 September 2026.

⁹ Ministry of Civil Aviation, National UTM Policy Framework (n 8) 4–5.

sensors, software and maintenance.

India's policy objective should therefore be to build upon the existing regulatory foundation rather than replace it. A proportionate framework that distinguishes between levels of autonomy can preserve the benefits of digital regulation while ensuring that responsibility remains identifiable as technological decision-making becomes more sophisticated. Such an approach would also provide greater certainty to India's emerging drone industry and support the broader objective of developing domestic capabilities in drone manufacturing and technology.

III. THE LIABILITY GAP: FROM OPERATOR RESPONSIBILITY TO SHARED RESPONSIBILITY

The existing Indian framework places substantial responsibility upon the person responsible for operating a drone. This approach is logical for remotely piloted aircraft because the operator exercises meaningful control over the flight and is therefore best placed to prevent many operational risks. The difficulty arises when autonomous systems begin to make decisions that are not directly controlled by the operator. In such cases, the person operating the drone may not necessarily be the person who created or could have prevented the particular risk that caused the accident.

A. Limits of Operator-Centred Responsibility

Operator responsibility should remain an important component of India's liability framework. An operator who disregards airspace restrictions, fails to maintain the drone, uses it outside authorised conditions or ignores known safety warnings should not be able to rely upon the drone's autonomy to avoid liability. Autonomy cannot become a means of escaping responsibility for risks that remain within the operator's control.

The difficulty is with automatic attribution of liability. Consider an autonomous delivery drone whose operator has complied with all applicable requirements but whose navigation system unexpectedly directs it into the path of another aircraft. If the accident resulted from an undiscoverable software defect, imposing the entire loss upon the operator would disconnect liability from the source of the risk. The law should therefore distinguish between negligence in operating the drone and failures arising from the autonomous system itself.

B. Manufacturer Liability

Manufacturers are likely to occupy an increasingly important position in the liability chain

because many risks associated with autonomous drones originate before the aircraft reaches the operator. A defective sensor, inadequate fail-safe mechanism or flawed system design may create risks that cannot reasonably be controlled during the flight.

The Consumer Protection Act 2019 provides a useful existing legal foundation. Its product-liability provisions recognise circumstances in which a manufacturer may be liable for harm caused by a defective product, including manufacturing defects, defective design and inadequate warnings or instructions.¹⁰ These principles can provide an avenue for addressing physical and design-related failures in autonomous drones.

However, autonomous systems create more difficult cases. A drone may conform perfectly to its physical specifications while its software produces an unsafe response in circumstances that should reasonably have been anticipated. Whether this amounts to a design defect, inadequate warning or another form of actionable failure would require examination of the manufacturer's knowledge, testing procedures, safety standards and intended operating environment.

C. Software and Algorithmic Responsibility

Autonomous drones also introduce a significant actor that traditional aviation liability frameworks did not have to consider to the same extent: the developer or supplier of the software responsible for autonomous decision-making. Navigation, obstacle avoidance, route optimisation and responses to environmental conditions may all depend upon software.

Where an accident is directly attributable to defective programming or inadequate safety testing, it would be difficult to justify placing the entire burden upon an operator who had no reasonable opportunity to identify or correct the defect. At the same time, software developers should not be treated as insurers against every unpredictable outcome. Liability should depend upon whether the relevant risk was reasonably foreseeable and whether reasonable testing, safeguards, updates and warnings were provided.

This creates an additional causation and evidence problem. Determining why an autonomous drone took a particular decision may require examination of software versions, sensor information, flight paths, system alerts and intervention records. The person suffering harm may have little or no access to such technical evidence. A future regulatory framework should therefore ensure that relevant autonomous-system data is preserved following significant incidents.

¹⁰ Consumer Protection Act 2019, ss 83–84.

D. Multiple Causes of an Accident

The most difficult cases will involve more than one contributing cause. Suppose an autonomous drone contains a software defect, but its operator has also failed to maintain its sensors. The software failure may have initiated the accident, while inadequate maintenance may have increased its likelihood or severity. Treating either actor as automatically responsible for the entire loss may produce an unfair result.

Indian law already recognises the importance of examining causation and the conduct of different parties rather than treating every accident as attributable to a single source. In *Municipal Corporation of Delhi v Subhagwanti*, the Supreme Court's discussion of *res ipsa loquitur* demonstrates the relevance of control in determining responsibility for an accident.¹¹ Autonomous drones make the question of control more complex because it may be distributed among several participants.

E. Towards Shared Responsibility

The appropriate response is therefore not to eliminate operator responsibility but to distribute responsibility according to the source of the risk. The operator should ordinarily remain responsible for negligent operation and maintenance; the manufacturer should bear responsibility for defective design or manufacture; and the software provider should bear responsibility where defective autonomous functionality materially contributes to the harm.

Where several actors contribute to the accident, liability should be apportioned according to their respective contribution to the risk. The degree of autonomy should also be relevant. The greater the autonomous control exercised by the system and the less meaningful the operator's ability to intervene, the stronger the justification for examining the responsibility of manufacturers and technology providers.

This approach would preserve accountability without imposing disproportionate burdens upon India's developing drone industry. It would also create appropriate incentives: operators would have reason to operate and maintain drones responsibly, while manufacturers and software developers would have stronger incentives to design, test and continuously improve autonomous systems. The objective should therefore be a liability regime based not merely on who operated the drone, but on who controlled, created or contributed to the risk that materialised.

¹¹ *Municipal Corporation of Delhi v Subhagwanti* 3 SCR 649, 652–53.

IV. COMPARATIVE LESSONS AND A MODEL FOR INDIA

The development of autonomous drones requires India to look beyond traditional operator-centred aviation liability and examine regulatory models that allocate obligations according to the level of risk involved. The European Union and the United States provide two useful, although different, approaches. Their experience demonstrates that autonomy does not necessarily require abandoning human accountability; rather, responsibility can be distributed according to the nature of the operation, the technology involved and the degree of control exercised by different actors.

A. European Union: Risk-Based Regulation

The European Union has adopted one of the most structured risk-based approaches to unmanned aircraft regulation. Regulation (EU) 2019/947 divides UAS operations into three categories - 'open', 'specific' and 'certified', according to the level of operational risk.¹² The open category covers comparatively low-risk operations and is subject to predefined operational limitations. The specific category applies where those limitations are exceeded and generally requires an operational risk assessment and authorisation by the competent authority. The certified category applies to the highest-risk operations and can require certification of both the aircraft and the operator, together with licensing of the remote pilot where applicable.¹³ This model is significant for India because it demonstrates that the legal consequences of operating a drone need not be identical across every type of operation. The European framework also regulates the design and manufacture of UAS, particularly where the consequences of an accident may be serious. Regulation (EU) 2019/945 establishes requirements concerning the design, manufacture and marketing of unmanned aircraft and links certain requirements to the operational risks associated with particular classes of UAS.¹⁴

The EU approach therefore provides an important conceptual lesson: liability and regulatory responsibility should correspond to risk rather than merely to the physical identity of the person controlling the aircraft. A low-risk autonomous drone operating within tightly prescribed conditions presents a different legal problem from a highly autonomous aircraft conducting BVLOS delivery operations over populated areas.

Insurance provides a further layer of protection. Regulation (EC) No 785/2004 establishes

¹² Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft OJ L152/45, arts 3–6

¹³ Commission Implementing Regulation (EU) 2019/947 OJ L152/45, arts 4–6.

¹⁴ Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems OJ L152/1, arts 4–6 and annex pts 1–5.

insurance requirements for air carriers and aircraft operators in respect of liability for passengers, baggage, cargo and third parties, subject to its scope and exclusions.¹⁵ The broader European approach consequently demonstrates how compulsory insurance can complement regulatory requirements by ensuring that the financial consequences of aviation risks do not fall entirely upon individual victims.

B. United States: Continuing Importance of the Remote Pilot

The United States provides a somewhat different model. Under the Federal Aviation Administration's framework, the remote pilot in command remains responsible for the operation of the unmanned aircraft and retains final authority over the flight.¹⁶ This preserves a clear point of accountability and reflects the continuing importance of human supervision even where automated systems are extensively used.

However, the American approach also recognises that increasingly complex UAS operations may involve several participants. Part 107 permits the participation of other persons, including a person manipulating the flight controls under supervision and a visual observer, but the remote pilot in command remains directly responsible for the operation, retains final authority and must ensure compliance with applicable regulations.¹⁷ This distinction is relevant to autonomous drones because it demonstrates that operational responsibility can be distributed within a broader organisational structure.

The FAA's Beyond Visual Line-of-Sight Aviation Rulemaking Committee has further examined the regulatory difficulties created by more advanced UAS operations. Its final report recognised that expanding BVLOS operations would require reconsideration of existing roles and responsibilities within the UAS ecosystem.¹⁸ The American experience therefore illustrates that increasing autonomy and operational complexity can make a purely pilot-centric conception of responsibility increasingly difficult to sustain.

C. A Model Adapted for India

India should therefore adopt the principle of risk-based allocation while retaining the simplicity and administrative advantages of its existing regulatory structure. A separate liability regime

¹⁵ Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for air carriers and aircraft operators OJ L138/1, arts 2(2)(b), 4, 6 and 7.

¹⁶ 14 CFR § 107.19(b)–(e) (2026).

¹⁷ 14 CFR §§ 107.12(a), 107.19(b)–(e), 107.33 (2026).

¹⁸ Unmanned Aircraft Systems Beyond Visual Line of Sight Aviation Rulemaking Committee, Final Report (10 March 2022) 110–31, especially 120–29 <https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS_BVLOS_ARC_FINAL_REPORT_03102022.pdf> accessed 14 September 2026.

for every technological variation would unnecessarily increase compliance costs and undermine ease of doing business. Instead, liability should be linked to three principal factors: degree of autonomy, operational risk and control over the source of harm.

First, where a drone remains substantially under human control and operates in a low-risk environment, the operator should remain primarily responsible for negligent operation, maintenance and compliance with airspace restrictions. Secondly, where the drone possesses significant automated decision-making capabilities, responsibility should be shared where the accident results from both operator conduct and technological failure. Thirdly, highly autonomous or high-risk operations, particularly BVLOS operations carrying significant payloads or operating over populated areas, should attract enhanced manufacturer, software-provider and operator responsibilities.

Such a framework would allow India to retain a clear regulatory hierarchy while avoiding the unfairness of automatically imposing every loss upon the person who happened to operate the drone. It would also encourage manufacturers and software developers to invest in safer autonomous systems because responsibility would follow the source of the risk.

The objective should consequently not be to import a foreign liability model wholesale. India can instead build upon its existing Drone Rules, DigitalSky architecture and UAS traffic-management framework to create an indigenous model suited to its technological and economic conditions. A risk-based system would protect the public while preserving regulatory certainty for India's growing drone industry and supporting its ambition to become a globally competitive centre for drone technology.

V. TOWARDS A PRO-INNOVATION LIABILITY REGIME FOR INDIA

India does not need to replace its existing drone regulatory architecture to address the liability challenges created by autonomy. The more appropriate approach is to build upon the framework already established through the Drone Rules 2021, DigitalSky and the developing UAS traffic-management ecosystem. The objective should be to provide greater legal certainty without creating regulatory burdens that discourage investment, research and domestic manufacturing.

First, India should introduce a graduated classification of autonomous drone operations for liability purposes. The existing distinction between different categories of UAS can be supplemented by considering the degree of autonomous decision-making and the consequences of a potential failure. Low-risk operations involving meaningful human control should continue to place primary responsibility upon the operator. For more autonomous operations,

responsibility should progressively extend to manufacturers and software providers where their products or systems materially contribute to the harm.

Secondly, India should strengthen its existing insurance framework. Rule 44 of the Drone Rules 2021 already provides for third-party insurance and compensation in respect of damage to life or property caused by a UAS, with certain exemptions for nano drones.¹⁹ This provides a foundation upon which a more differentiated insurance regime can be developed. Higher-risk autonomous and BVLOS operations should be required to maintain adequate third-party liability coverage proportionate to the potential consequences of an accident. Such a requirement would protect victims while ensuring that liability does not become an unpredictable financial burden on individual operators.

Thirdly, mandatory preservation of flight and system data should form part of the framework for higher-risk autonomous operations. Autonomous drones can generate information concerning flight paths, sensor inputs, system alerts, software versions and attempted human interventions. Requiring operators and manufacturers to preserve relevant data following a serious incident would make it easier to establish causation and determine which participant contributed to the accident. Where critical evidence is exclusively controlled by a manufacturer or technology provider, appropriate evidentiary rules should prevent victims from being disadvantaged by the technological complexity of the system.

Fourthly, the regulatory framework should provide a compliance-based defence for responsible operators and manufacturers. A party that has complied with approved technical standards, certification requirements, maintenance obligations and prescribed safety procedures should not automatically be treated as liable merely because an autonomous system produced an unexpected result. Such protection would encourage innovation while ensuring that the defence is unavailable where there has been negligence, concealment of a known defect or failure to comply with mandatory safety requirements.

Finally, India should encourage controlled testing of advanced autonomous systems through regulatory sandboxes and certification pathways. This would permit manufacturers and technology developers to test increasingly sophisticated systems under regulatory supervision before large-scale deployment. A predictable approval and liability framework would complement India's objective of developing a globally competitive domestic drone ecosystem.²⁰

¹⁹ Drone Rules 2021, r 44.

²⁰ Ministry of Civil Aviation, Guidelines for the Operation of Production Linked Incentive Scheme (PLI) for Drones and Drone Components (n 2) para 1.1.

The proposed model therefore seeks to balance two interests that should not be viewed as contradictory: technological innovation and public accountability. Clear allocation of responsibility, compulsory insurance for higher-risk operations, reliable technical records and proportionate liability can reduce uncertainty for industry while improving protection for the public. Rather than treating autonomy as a reason for restrictive regulation, India can treat it as the next stage in the development of a technologically sophisticated and innovation-oriented aviation framework.

VI. CONCLUSION

The rapid development of autonomous drone technology presents India with an important regulatory challenge. The existing framework has established a strong foundation for the growth of the drone sector by regulating operations, introducing digital regulatory mechanisms and encouraging domestic manufacturing. However, increasing autonomy complicates the traditional assumption that the person operating an aircraft should bear primary responsibility for every consequence arising from its operation.

As autonomous systems increasingly make decisions relating to navigation, obstacle avoidance and flight management, liability must correspond more closely to the source of the risk. An operator should remain accountable for negligent operation and maintenance, while manufacturers and software developers should bear responsibility where defective design, manufacturing or autonomous functionality materially contributes to harm. Where multiple factors cause an accident, responsibility should be apportioned according to each participant's contribution to the risk.

India should therefore adopt a proportionate, shared and risk-based liability framework, supported by mandatory insurance for higher-risk autonomous operations, preservation of relevant flight and system data, and clear compliance standards. Such reforms need not impede innovation. On the contrary, predictable liability rules can reduce uncertainty for businesses, encourage safer technological development and strengthen investor confidence.

The objective should be to build upon India's existing regulatory achievements and create a framework capable of supporting the next generation of autonomous aviation. A balanced approach can protect the public while advancing India's ambition to become a leading global hub for drone technology and domestic innovation.