Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 743-752

AI ENABLED DRONES AND THE RIGHT TO PRIVACY: A CONSTITUTIONAL ANALYSIS

[1]Chhaya Gupta, [2]Abhika Ojha, [3]Manjot Singh, [4]Sidharth Tulsyan
[1,2,3,4]Students of BA/BBALLB 10th Semester
[1,2,3,4]Kalinga University, Naya Raipur, C.G.
[1]guptac532@gmail.com, [2]abhikaojha@gmail.com, [3]manjots6908@gmail.com,
[4]tulsyansiddharth@gmail.com

Abstract
The concept of unmanned aerial vehicles (UAVs), known in ancient Indian scriptures as 'Vimanas', has evolved significantly with the advent of modern drone technology in the late 19th century. Although still in its nascent stages, the Indian drone industry holds immense potential, with projections estimating a revenue of US$28.7 million by 2025 and an expected annual growth rate of 5.58% between 2025 and 2029. Recognising the dual needs of promoting innovation and ensuring public safety, a robust regulatory framework is essential. Drones have revolutionised sectors such as agriculture, enabling field soil analysis, precision planting, agricultural spraying, and livestock monitoring, thereby offering promises of improved productivity and environmental adaptability. Beyond agriculture, the energy sector has witnessed significant advancements through drone technology, particularly in infrastructure inspection, hazard identification, and operational efficiency. With features like thermal imaging and LiDAR-based 3D modelling, drones are transforming traditional practices, enhancing safety, reducing costs, and driving the technological evolution of critical industries. This study underscores the importance of regulatory development alongside technological adoption to harness the full potential of drones across sectors.

Keywords: Drone technology, Indian drone market, Agriculture sector, Energy sector, Regulatory framework, Thermal imaging, LiDAR, Infrastructure inspection, Technological innovation, Safety and efficiency.

Introduction

Although the Indian scriptures have contained vivid references to Unmanned Aerial Vehicles in the form of 'Vimanas', which could be described as the ancient predecessors of the present day drones, it was not until the late 19th century that the use of modern day drones saw a rise in

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 743-752

India.[1] The drone industry in India is still at a stage of infancy and carries immense potential, provided that the industry and the legislators co-operate. The Drones market in India is projected to generate a revenue of US$28.7m in 2025.[2] This market segment is expected to witness 5.58% annual growth rate (CAGR 2025-2029).[3] Considering the impending popularity, it is essential to have a robust regulatory framework in place that takes into account the interests of safety and commerce and balances the freedom of movement with certain reasonable restrictions. In agriculture, technological advancements have been possible because of drones.[4] Currently, drones are being used, albeit at a very minimal scale, for field soil analysis, for planting, agricultural spraying of pesticides and insecticides, for tracking of livestock and a host of other uses.[5] The proliferation of the use of drones in agriculture has opened the doors for its widespread acceptance. The use of drones brings with convenience, a promise of improved production through comprehensive irrigation planning, adequate crop health monitoring and increased insights about the health of soil and adaptation to changes in the environment.

Apart from the agricultural sector, the energy sector has also undergone a significant transformation through the use of drones. It is estimated that out of the 41.3 Billion Dollar market valuation expected to be achieved by the drone industry in 2026, about 6 Billion Dollars would be contributed through the use of drones in the energy industry.[6] The most important contribution of drone technology to the energy sector is regarding the task of inspecting the hazardous infrastructure that threatens the lives of a vast number of workers. In terms of cost, efficiency and safety, drones have emerged as a one stop solution for the energy industry and the same can be evidenced by the increasing adoption of drones in the energy sector.[7] Drones are equipped with thermal cameras which enable them to identify overheating components, measure voltage levels and detect potential electrical issues. Through LiDAR technology, drones provide precise 3D Models of power lines, thus helping in pinpointing the structural problems, encroachment of vegetation and other hazards.[8]

---

[1]"Mrinmoy Roy, 'An Exploratory Study on Origin of AI: Journey through the Ancient Indian Texts & Other Technological Descriptions, Its Past, Present & Future' (2021) 12 Turkish Online Journal of Qualitative Inquiry."
[2]"MarketsandMarkets, *India Drone Market Size, Share, Trends & Growth Analysis* (2024)<https://www.marketsandmarkets.com/Market-Reports/india-drone-market-136782206.html> accessed 10 January 2025."
[3] Ibid
[4]"Ljungholm, D.P., 2019. Regulating government and private use of unmanned aerial vehicles: Drone policymaking, law enforcement deployment, and privacy concerns. *Analysis and Metaphysics*, (18), pp.16-22."
[5]"Cracknell, A.P., 2017. UAVs: regulations and law enforcement. *International Journal of Remote Sensing*, *38*(8-10), pp.3054-3067."
[6]Ibid
[7]Ibid
[8]Ibid

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 743-752

The Beginning of Drone Regulation in India

An event as ordinary as a pizza delivery rarely sparks discussions within legal circles. However, in May 2014, a popular pizzeria stirred up debate when it chose to bypass Mumbai's infamous traffic by using a drone to deliver a pizza.[9] This incident brought the legality of civilian drone use to the forefront. A police inquiry into the matter made little progress since, in the absence of relevant laws, there was no legal infraction, and therefore no basis for filing a complaint, making arrests, or seizing equipment.

Later that year, reports emerged about Amazon planning pilot drone delivery services in Bangalore and Mumbai. In response, the Directorate General of Civil Aviation (DGCA) issued a public notice in October 2014 stating that no private entity, organization, or individual could operate unmanned aircraft systems (UAS) in Indian airspace for any purpose until the DGCA established proper regulations for their certification and operation.[10] On April 21, 2016, the DGCA released draft guidelines outlining procedures for obtaining a Unique Identification Number (UIN) and operating civil UAS. Public feedback on the draft was invited within a month.

Even before the DGCA's notice and draft guidelines, drones had already entered the Indian market and were being utilized across various sectors. For instance, the Delhi Police employed drones for riot surveillance and street patrols.[11] The National Disaster Management Authority used them to survey flood-affected regions to enable timely action. A national tiger reserve expressed interest in deploying drones to combat poaching, and prototype air ambulances were being tested to improve rural healthcare and organ donation logistics. Additionally, drones became a valuable tool in the media and entertainment industries for aerial photography, with several companies emerging to offer such services.[12] These diverse applications demonstrate that drones are no longer merely luxury gadgets but have become integral to numerous civilian uses.

Presently, drone operations are carried out within the line of sight of the drone pilot. Foreseeing a time where the operation of drones would be beyond the visual line of sight, the DGCA has issued Regulations for Unmanned Aerial Systems. In 2014, the increased civilian use of drones and an absence of regulations to regulate the operation of drones led to the DGCA enforcing a blanket ban on the operation of drones. The Directorate General of Civil Aviation governs drone operation in India. In light of the significance of UAS, the DGCA has initiated a process of public consultation to gather stakeholder input and develop appropriate regulations. In April 2016, the

[9]"Royo, P., Asenjo, À., Trujillo, J., Çetin, E. and Barrado, C., 2022. Enhancing drones for law enforcement and capacity monitoring at open large events. *Drones*, *6*(11), p.359."
[10]"Smith, M.L., 2015. Regulating law enforcement's use of drones: The need for state legislation. *Harv. J. on Legis.*, *52*, p.423."
[11] Ibid
[12] Ibid

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 743-752

first formal rules for unmanned aerial system (UAS) usage in India were issued, laying the groundwork for the subsequent regulatory framework.

The Indian government finally unveiled CAR 1.0, the Civil Aviation Requirements for Remotely Piloted Aircraft Systems, on August 27, 2018, after much deliberation. The DGCA released its final regulations for civilian drone operating in 2018. "Remotely Piloted Aircrafts" is how the DGCA has classified drones.[13] Drones may now be lawfully used by citizens in India, according to the DGCA rules. Unmanned traffic management protocols and a contactless digital framework called Digitalsky Platform were both introduced in CAR 1.01. All types of unmanned aerial system (UAS) users, including owners and pilots, will be able to register on the Digitalsky platform. The authority's original plan was to monitor and approve all unmanned aircraft system flights above civilian airspace.

The program would remotely authorize all battles after the pilots applied for digital authorization in advance, eliminating the need for paperwork and bureaucratic approvals. Under some circumstances, the rules removed the need for nano drones to get permission before taking to the air. Drones are now categorized according to their weight and cargo capacity, a feature introduced in CAR 1.0. The unmanned aerial system (UAS) classifications were as follows:

1. Nano, for payload capacities of 250 grammes or less;
2. Micro, for payload capacities of 250 grammes to 2 kilograms;
3. Small, for payload capacities of 2 kg to 25 KG;
4. Medium, for payload capacities of 25 KG to 150 KG; and
5. Large, for payload capacities of 150 KG and above.

UIN registration became available to Indian citizens, Indian-owned or controlled companies, and government-controlled businesses with the 1.0 CAR. This regulation effectively outlawed the ownership of unmanned aerial systems (UAS) in India by foreign individuals and companies. For organizations providing UAS service as operators, the CAR 1.0 additionally included a distinct Unmanned Aircraft Operator Permit (UAOP). A DGCA-approved flight training organization was granted the authority to implement CAR 1.0's training requirements. Attendance and certification as a UAS operator are contingent upon the operator's having reached the legal age of eighteen.[14]

To earn the title of UAS pilot, students were required to demonstrate mastery of both theoretical and practical components of the program. In order to prepare the UAS pilot to handle unexpected

[13]"Bharanitharan, K., Kaur, G. and Shukla, V.K., 2024, October. Drones and Surveillance Challenges and Legal Regulation Against Drone Crimes in India. In *2024 International Conference on Artificial Intelligence, Metaverse and Cybersecurity (ICAMAC)* (pp. 1-6). IEEE."

[14]"Nugraha, R.A., Jeyakodi, D. and Mahem, T., 2016. Urgency for legal framework on drones: Lessons for Indonesia, India, and Thailand. *Indon. L. Rev.*, *6*, p.137."

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 743-752

circumstances, some training requirements were put in place. The three parts of CAR 1.0 that deal with flying limits for UAS operations are as follows.

1. In the first area, unmanned aerial system (UAS) activities were severely limited. Permission to fly was required in the second zone, which was a regulated airspace. Unauthorized aerial vehicle (UAS) activities were not required in the remaining uncontrolled airspace zone. Regular contact with drone air traffic controllers was required before, during, and after launch authorization due to restricted airspace activities. Prior to each UAS operation, the operator was responsible for ensuring compliance with local regulations and conducting risk assessments.
2. The authority to suspend or revoke UIN and UAOP for infractions was conferred to the DGCA under the CAR 1.0. Local law enforcement agencies have the authority to bring charges against the owner or operator of a UAS for any infractions of the Indian Penal Code, 1860.
3. Additionally, on 3 June 2019, the DGCA RPAS Guidance Manual was released, and the Airports Authority of India published AIP Supplement 164 of 2018 (Airports Authority of India, 2018). Both documents were provided by the Government of India. The Indian government has published proposed regulations for UAS (unmanned aerial systems) as part of its consultation process. The UAS Rules, 2021 were announced by the government after the receipt of stakeholder opinions and suggestions from the industry.

Constitutional Provisions Relevant to UAS and Privacy in India

Ever since the Hon'ble Supreme Court of India recognised the Right to Privacy in the case of **Justice K.S.Puttaswamy vs Union of India**[15], discussions regarding the Right to Privacy have spread like wildfire within academic circles. The Right, being a part of Article 21 is essential for the dignity of human beings and thus, impacts virtually every aspect of the expansive Article 21. The preceding sections of the study have clearly highlighted how drones, if not regulated properly, can pose a threat to privacy of individuals, ultimately endangering their dignity. The Puttaswamy case concretized the legal position regarding privacy and established that the same was a Fundamental Right and could not be abridged by the state.

The case revolved around the collection of sensitive personal information of individuals by the Central Government for the purpose of Aadhar enrollment. When it comes to drones, the Puttaswamy case is significant as various aspects regarding privacy may be impacted by the use of drones. Since there exists no specific legislation pertaining to the Right to Privacy in India, the text of the Puttaswamy judgment becomes particularly significant. The court held, among other things that Privacy was a concomitant of an individual's right to exercise control over

[15]AIR 2018 SC (SUPP) 1841

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 743-752

his/her personality. Unmanned Aerial Vehicles, if unregulated, pose a threat to the right of an individual to exercise control over his personality as it would leave individuals prone to unwarranted surveillance and trespass.

Unwarranted surveillance directly dilutes the control of a person over his personality due to the 'fear of being continuously watched'. The famous novel by George Orwell titled 1986 is a brilliant example in this context. The constant surveillance by state in almost all areas of human life led to the commoditization of individual personalities in the hands of the government. The Indian Constitution seeks to prevent an Orwellian Surveillance type scenario and thus, the Right to be free from unwarranted surveillance becomes a crucial aspect of a person's right to control over his/her personality. The court also highlighted that the Right to Privacy was important for the enjoyment of other Fundamental Rights enshrined under Part III. The preceding chapters have highlighted how the use of Unmanned Aerial Systems impacts the 7 different kinds of privacy. The court highlighted the primary 3 aspects as follows:

1. There must be some invasion pertaining to a right related to a person's physical body
2. Informational Privacy, which deals not with the physical aspect but with the mental aspect
3. The privacy of choice, which is meant to protect the autonomy of an individual over his fundamental personal choices.

Unregulated use of Unmanned Aerial Systems pose a threat to all the aforementioned aspects of the right to privacy and thus, the Indian administration has ensured that the legal framework takes into proper consideration the need to preserve the privacy of individuals. Yet another significant aspect of the Right to Privacy is the Right to control the dissemination of personal information. Privacy's limits vary depending on the connection and situation. Confidentiality is very important in professional environments, including those involving physicians or solicitors. This idea also applies to UAS operations, particularly in cases when the gathered data relates to private properties or personal activities and calls for sensitive zones.

Breaking these limits without permission weakens confidence and generates major ethical and legal questions.[16]Privacy is essential in the field of UAS mostly because it helps to reduce social conflicts and avoid embarrassing circumstances. Illegal drone use for data collection or surveillance, for instance, might create unease and strife among individuals, companies, or communities. Most personal information, as Daniel Solove correctly notes, falls under "none of your business."[17] UAS operators, who must grasp the limits of their data collection activities, particularly find this idea rather relevant. Moreover, the voluntary exchange of personal data in

[16]"Sidharth, A., Sinha, P. and Sheikh, S., 2023. Drone Rules 2021: Analysis and Implications for India's UAV Programme. In *Interdisciplinary Perspectives on Sustainable Development* (pp. 420-427). CRC Press."
[17] Ibid

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 743-752

UAS-related activities—such as registration of drones or compliance with UAS traffic control systems—guarantees confidentiality. Any breach of this trust undermines public confidence in the technology as well as invasion of privacy. Openness regarding the techniques used in data gathering, storage, and utilisation is really vital. People should be allowed to edit, know, or correct their data so they maintain control over their personal records. In a democratic society, the measure of freedom is the ability to make sensible life decisions. Using UAS has to follow this concept since it encourages accountability and transparency. Decisions on the use and deployment of drones should not be made in silence. People must be aware of and engaged in discussions on the management of UAS data if they are to ensure their rights are protected.

The Digital Data Protection Act, 2025

Draft Digital Personal Data Protection Rules, 2025 (DPDP Rules) were published by the Union Ministry of Electronics and Information Technology (MeitY) on January 3, 2025, under the Digital Personal Data Protection Act, 2023 (DPDP Act). These suggested rules are a significant step towards India's whole data protection framework coming into effect. MeitY began a public consultation campaign to ensure transparency and stakeholder participation, asking for feedback, concerns, and suggestions from individuals, companies, and experts. Running until February 18, 2025, the consultation process emphasises the government's desire to encourage participatory governance and ensures that the legislation are responsive to the needs of a data-driven environment.

Comprising seven schedules and twenty-two clauses, the suggested DPDP Rules, 2025 almost match the forty-four DPDP Act components. This consistency indicates an effort to provide procedural standards and operational clarity for the effective application of the Act. The rules cover several significant issues in considerable depth, including notification criteria businesses must follow to ensure data processing transparency. They specify the information a data fiduciary must provide to data principals: the objectives of data gathering, the processing techniques, and the rights the data principle has.

Emphasising the requirement of obtaining explicit, informed, and affirmative permission from data principals before processing their personal data, the standards also provide robust techniques for consent management. To ease concerns about data security, the suggested policies include security steps companies must take to protect personal data against unlawful access, breaches, and use.

These safeguards are organisational and technical efforts consistent with global best standards. The proposal also calls for data fiduciaries to notify affected individuals if the breach poses a significant risk and to report breaches to the Data Protection Board of India. Processing the

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 743-752

personal data of children and those with disabilities has been particularly addressed with specific regulations ensuring their data is handled with extra care and protection in accordance with their individual needs.

The release of these early recommendations marks a turning moment in India's road to establish a robust digital personal data protection framework. Once completed, the DPDP Rules, 2025 are intended to provide the operational backbone for the DPDP Act, hence offering a clear road map for companies operating under India's data governance framework and so safeguarding the rights and interests of data principals.

A structured framework intended to secure personal data and preserve the basic privacy rights of people is provided by the proposed Digital Personal Data Protection Rules, 2025. Among its key elements, the guidelines call for thorough notice issuing by data fiduciaries and strict controls on consent management.

Notice Requirements for Data Fiduciaries

The proposed regulations set explicit responsibilities on data fiduciaries to provide standalone notifications that are straightforward, thorough, and accessible, hence improving openness and empowering data principals—people whose personal data is handled. These notifications have to be the main means of communication guaranteeing data principals are fully aware of the gathering and processing of personal data. The policies provide for such notifications to have:

1. A thorough inventory of personal data gathered: Fiduciaries have to reveal exactly what kinds of personal data are being gathered from data subjects, hence eliminating any uncertainty.
2. The notification has to clearly explain why the personal data is being processed, so clarifying its intended use and guaranteeing that the processing fits authorised and legitimate goals.
3. Fiduciaries have to clarify how the processing of personal data supports the delivery of products, services, or other purposes, hence justifying the data collecting in terms of measurable results.
4. Data subjects ought to be made aware of the processes for revoking permission, using their legal rights, and lodging concerns concerning data management. This guarantees that people have significant control over their personal data.

Moreover, the policies emphasise straightforwardness in communication and accessibility. Notices ought to include clearly accessible links to the fiduciary's platform and user-friendly instructions for revoking consent or filing complaints. This goal is to simplify processes so that data owners may engage with fiduciaries directly and effectively.

Consent Managers

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 743-752

The new regulations also highlight the fundamental need of consent managers—third-party organisations or platforms supporting data subjects in controlling their consent choices. Operationalising the consent-based system envisioned by the Digital Personal Data Protection Act, 2023 is made possible by these organisations. The guidelines provide certain eligibility and operational criteria to guarantee that consent managers run with integrity and efficacy including: Incorporation and financial requirements: Consent managers have to be registered in India with at least net wealth of INR 20 million (about USD 233,414). This financial criterion is meant to guarantee the stability and dependability of organisations handling sensitive personal data.
The system provided by consent managers has to enable data principals' effortless management, review, and withdrawal of permission. The interoperability criteria guarantees that the platform may work with other data fiduciaries and systems, hence fostering efficiency and user friendliness.

- Transparency and security standards: Consent managers are required to maintain high levels of openness in their operations, so guaranteeing that their actions are free from conflicts of interest. They also have to use strong security policies to defend the personal data under their control, therefore protecting the rights of data principals.
- The laws provide another protection that calls for consent managers to get prior authorisation from the Data Protection Board (DP Board) before any transfer of control or ownership. This clause seeks to stop unapproved management modifications that would endanger the neutrality, integrity, or security of the consent management system.
- These clauses taken together show a deliberate attempt to establish a data protection system emphasising human autonomy, responsibility, and trust, hence complementing world best practices in data privacy control.

Conclusion

The development of drone legislation in India, especially with regard to privacy and data protection, shows an increasing need to reconcile technical progress with individual rights. Starting with commercial projects like Domino's drone delivery tests, India's path into regulating Unmanned Aircraft Systems (UAS) has grown into a thorough legal framework addressing not only airspace safety but also constitutional rights, particularly the right to privacy under Article 21.

The Indian legal scene has made a major stride towards protecting personal data in the digital age with the passage of the Digital Data Protection Act, 2025. Aimed at guaranteeing informed and responsible data processing, the Act brings important tools like notice obligations, consent managers, and data protection impact assessments (DPIAs). For government agencies as well as private companies, the responsibilities of acceptable security measures, breach reporting, and data retention highlight a change towards more openness and responsibility.

ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-4 | April - 2025 | Page 743-752

The Act's clauses on cross-border data processing, research exemptions, and the function of data fiduciaries and consent managers also contribute to turn the abstract notion of privacy into enforceable legal obligations. These legal safeguards are more important as drones more and more cross data collecting and monitoring.

In the end, India's strategy shows a sincere effort to balance rights-based government with innovation. The effectiveness of this system, however, will rely not only on the strength of the legislation but also on its application, public knowledge, and ongoing regulatory practice improvement in reaction to technology development.

References

1. Sonia, R., Gupta, N., Manikandan, K.P., Hemalatha, R., Kumar, M.J. and Boopathi, S., 2024. Strengthening Security, Privacy, and Trust in Artificial Intelligence Drones for Smart Cities. In *Analyzing and Mitigating Security Risks in Cloud Computing* (pp. 214-242). IGI Global.
2. Stoica, A.A., 2021. Drones, Privacy and Data Protection. *LESIJ-Lex ET Scientia International Journal*, *28*(2), pp.96-111.
3. Altawy, R. and Youssef, A.M., 2016. Security, privacy, and safety aspects of civilian drones: A survey. *ACM Transactions on Cyber-Physical Systems*, *1*(2), pp.1-25.
4. Schlag, C., 2012. The new privacy battle: How the expanding use of drones continues to erode our concept of privacy and privacy rights. *Pitt. J. Tech. L. &Pol'y*, *13*, p.i.
5. Goyal, S.B., Rajawat, A.S., Solanki, R.K., Zhu, L. and Chee, W., 2023, October. Enhancing Privacy and Security for UAV and IoT Enabled Drones an Intelligent Integration of Blockchain, AI, and Quantum Computing. In *International Conference on Intelligent Computing & Optimization* (pp. 16-27). Cham: Springer Nature Switzerland.
6. Balasubramanian, V., Aloqaily, M., Guizani, M. and Ouni, B., 2025. Security Challenges and Solutions for Autonomous Vehicles and Drones in the AI Age. *IEEE Internet of Things Magazine*, *8*(2), pp.129-136.