Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Are Indian drones flying above privacy concerns? - A legal analysis

Alfonsa Saji[a]

[a]Ramaiah College of Law, Bangalore, India

Received 16 July 2022; *Accepted* 05 August 2022; *Published* 08 August 2022

Drones are extensively operated by governmental and non-governmental agencies today. Drones can be controlled remotely or by following a pre-planned flying route. It can be as small as an insect or as large as a traditional jet. The rapid rise in drone popularity and their adoption by various governments over the past few years, has sparked a number of privacy concerns. Because privacy is a complex and sensitive issue, it necessitates the contentious debates of security versus privacy. Due to the perverse results, it has prompted calls for a regulatory and legislative framework that controls, regulates, and limits the use of drones or Unmanned Aerial Vehicles (UAVs). Concerns surrounding privacy invasions that may be either intentional or not have yet been addressed by the Indian government so far. This paper tries to gauge the focus into analysis and attempts to understand the current legal framework of governance of drones in India, with special attention to privacy concerns. It also attempts to provide sensible suggestions to overcome the current privacy-related issues and problems.

Keywords: *drone, privacy, mosaic theory, security, unmanned aircraft system.*

INTRODUCTION

Our country has seen an incredible amount of development in technology in a very short time span in the last decade. One of the major developments can be seen in the form of drones, also known as unmanned aerial vehicles. This electronic device has secured the goal of being used

as a modern-day flying tool with cost-effective usage in various parts of the world. It was first invented to assist in warfare. However, gradually this device was found useful for multiple purposes, e.g., to help with marine and wildlife protection, use as an aerial camera in film production, to help with disaster response, and most importantly, to help with immediate search and seizure in any rescue mission or police investigations. At present, drones have also been used by several online businesses for delivery purposes, which has increased their profits due to their rapid delivery options. The discussions about how to govern drones and the problems with their use are expanding along with the drone sector. Governments are attempting to introduce drones in their domestic aviation legislation in an effort to minimize casualties and offer precise information surveillance as the market for drones grows. Given the many properties and uses of drones, it is essential that the regulations follow the goal of closing the gaps.

Like any other technology, the use of drones is mostly influenced by the objectives of the person using them. Therefore, criminals can use drones for nefarious or destructive activities, as was the case with the drone attack on an Indian Air Force station in Jammu. Therefore, it is crucial to control who owns them and how they are used. To govern the same, the Drone Rules, 2021 were introduced, which then came into effect from August 2021. In light of India's efforts to compete internationally on technological and drone usage concerns, it is vital to determine if this applicable Indian regulation is enough to offer the appropriate protections against privacy infringement.

LEGISLATIVE FRAMEWORK SURROUNDING DRONES IN INDIA

India’s Ministry of Civil Aviation (MoCA) finalized and earlier this summer disclosed draught rule when it unveiled a new drone policy on August 26, 2021. Based on comments from the public, the government thereby repealed the Unmanned Aircraft System Rules, 2021 (UAS Rules) and substituted them with the latest and more liberalized Drone Rules, 2021. Herein, the UAS, or drones, are used extensively in a variety of fields, including transport, agricultural purposes, defense, public safety, monitoring, and emergency management, to name just a few. The new drone regulations are designed to make it simpler to deploy drones in India for a

variety of uses, including non-commercial ones. For instance, there is no special permission required to fly and operate any small drones in the air under India's new drone regulations. To make freight deliveries easier, the government is also creating drone routes.

A number of approvals were previously required by the Indian government, including "a special authorization number, a special prototype identification number, a certificate of manufacturing and airworthiness, a certificate of conformance, a certificate of maintenance, acceptance of pre-existing drones, authorization for remote pilot instructors"[1], and so forth. According to the decision the Indian government released on August 26, 2021, none of these permissions are now necessary for drone usage in India. In India, the maximum extent of fines for drone-related non-conformity is reduced to one lakh rupees. Even so, this does not account for additional rules that may be broken when operating drones, which the authorities have not yet made clear.

PRIVACY SAFEGUARDS UNDER THE DRONE RULES, 2021

Indians now have serious privacy concerns as a result of both private and public entities using drone technology. Unfortunately, the present legal and regulatory framework is insufficient to fend off intrusions on drone users' privacy. The use of drones by government organizations is currently widespread. To provide light on the situation, Indian Railway and the Indian Forest Department have both utilized drones to observe the plantations and the Seawoods-Nerul-Uran railway project, respectively. In order to map the lands of Indian rural communities and demonstrate their clear ownership of their holdings, the government has created the Survey of Villages and Mapping with Improvised Technology in Village Areas Scheme (SVAMITVA) as part of its development programs. The numerous advantages of drones cannot be disputed, but at the same time, their potential for misuse must be taken into consideration, as the aforementioned cases show. The widespread use of responsive, covert drones outfitted with a wide range of sensors, video cameras, recording devices, optical devices, and other surveillance

[1] 'Ministry of Civil Aviation Notifies Liberalised Drone Rules, 2021' (*Press Information Bureau*, 26 August 2021) <https://pib.gov.in/PressReleseDetailm.aspx?PRID=1749154> accessed 13 July 2022

tools raises the unsettling suspicion that these drones are capable of collecting an excessive amount of private information, both accidentally and on purpose.

According to a press release from the MoCA, this worry is exacerbated by the fact that many organizations have been approved by the MoCA and Directorate General of Civil Aviation to use drones for tasks like surveillance, the availability of quality medical supplies, aerial surveys of crop health, and research studies. Following COVID-19, numerous police agencies were permitted to employ drone technology to track lockdown infractions in real-time and to use thermal cameras mounted on drones to measure the body temperatures of people in congested locations. The Civil Aviation Requirements for Operation of Civil Remotely Piloted Aircraft Systems, which were released by the DGCA in August 2018 together with the DGCA RPAS guidance handbook, 2020, have governed the drone sector since 2018. Regarding privacy protections, a general duty was placed on the remotely operated aircraft operator or virtual pilot to make sure that any entity's privacy standards were not violated in any way.[2]

The Guidance Manual also stated that certain privacy principles had to be incorporated into the design of every Remotely Piloted Aircraft System (RPAS), which would include proactive efforts to protect privacy to be made rather than reactive ones, wherein the approach had to be preventative rather than remedial. Secondly, privacy had to be the default setting and visibility and transparency had to be preserved in the RPAS's design; Lastly, all stakeholders' privacy had to be respected. The MoCA published the drone ecosystem policy roadmap in January 2019.[3] It included suggestions for the protection of personal data resulting from drone activities. The Drone Policy advises manufacturers to consider the standards of privacy and security of personal data by purpose and by default while conducting design and implementation. It also suggests that the establishment of performance appraisal and evaluation mechanisms, including queries to access, anonymize, or erase the data of the data principal, be made mandatory for DigitalSky Service Providers, which are service providers registered on a DigitalSky platform,

[2] Mamidala Jagadesh Kumar, 'The Sky Is Not The Limit: The New Rules Give Wings To The Drone Technology In India' (2021) 38 IETE Technical Review

[3] Arun Kumar, 'Commercial Drone Use In The Context Of Governance, Ethics, And Privacy: A Techno Ethical Review' (2021) 11 ACADEMICIA: An International Multidisciplinary Research Journal

which was hosted by the DGCA for activities related to the management of unmanned aircraft systems in India.

The Unmanned Aircraft System Rules, 2021, which were published on March 12, 2021, thereafter took the place of the aforementioned regulations. The UAS Rules 2021 needed the unmanned aircraft system operator to protect people's privacy and their property while the system was in operation, and they also permitted the capture of images and data by an unmanned aircraft only after making sure that doing so was legal and protected people's privacy and their property. It is important to highlight that the UAS Rules 2021 do not include the data protection standards advocated by the Drone Policy. The MoCA produced the Drone Rules 2021 on August 25, 2021, superseding the UAS Rules 2021 in response to complaints about the onerous compliances. Surprisingly, the Drone Rules 2021 completely omitted the word 'privacy' from their text, failing to take into account the potentially dangerous effects that the widespread use of drones may have on people's fundamental right to privacy and all of its various aspects as outlined by the Supreme Court in *Justice K.S. Puttuswamy (Retd.) v Union of India*.[4]

The rights of an individual to maintain their physical integrity, defend their informational privacy, and maintain their decisional autonomy are just a few of the many different facets of privacy. Of course, before these technological gadgets are made available to the general public, such a right to privacy should be balanced with the legal criteria that the parties in the drone ecosystem must satisfy. The broad privacy principles found in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, issued under the Information Technology Act, 2000, and the Justice Srikrishna Committee Report on Data Protection, are the only available and applicable legal requirements for new technologies like drones, unmanned aerial systems, etc.

However, the SPDI Rules only apply to body corporates or people working on their behalf that collect, receive, hold, store, deal with, or handle the personal details of natural persons in India. They do not apply to the protection of personal data by government agencies. General laws like

[4] *Justice K.S. Puttuswamy (Retd.) v Union of India* (2017), AIR 4161

the IT Act and SPDI Rules are inadequate for developing technology like drones, which are inherently intrusive in nature. Drones may be used for real-time video-graphic/technical monitoring and position monitoring, as a data gathering device, or for law enforcement reasons.

MOSAIC THEORY OF PRIVACY AND INTERNATIONAL RULINGS

The US Supreme Court supported the "mosaic theory of privacy"[5] after it was created by the US Court of Appeals for the DC Circuit in United States v Maynard.[6] According to the mosaic theory of privacy, in order to assess the dangers of data collection to individual privacy, the notion of data gathering must be examined as a whole, not in part. Accordingly, GPS monitoring and policing based on cell site location data might each qualify as 'searches' under the Fourth Amendment of the United States Constitution and call for a valid warrant.[7] The state's indiscriminate collection of data on individuals, as opposed to simply information against suspects in criminal behavior pursuant to a legal procedure, is a fundamental problem with such pervasive data collection. Similar methods are used in India while using drones to enforce the law. The dangers of extensive and indiscriminate data gathering and processing are highlighted by the capabilities of drones to employ high-definition cameras, gather position coordinates, conduct thermal imaging and distance mapping, and capture photographs and footage of a broad population.[8]

An analysis of state surveillance cases in India reveals that these cases have served as the foundation for the country's current state surveillance jurisprudence. But when viewed through the mosaic theory, innovations like drone technology and its systematic application raise special issues like the function of informed consent in public drone monitoring and potential privacy infringement. Another example of promoting technology to support governmental duties and services in the absence of a thorough data protection regulation is the deployment of drones via exceptions without an underpinning data protection law. The implementation of facial

[5] *United States v Jones* [2012] 565 U.S. 400; *See also, Carpenter v United States* [2018] 84 U.S. 17 Wall. 489
[6] *U.S. v Maynard* [2010] 615 F.3d 544
[7] Matthew B. Kugler & Lior Jacob Strahilevitz, 'Actual Expectations Of Privacy, Fourth Amendment Doctrine, And The Mosaic Theory' (2016) 20 (15) The Supreme Court Review 205
[8] Sean Sullivan, 'Domestic Drone Use And The Mosaic Theory' (*SSRN Electronic Journal,* 6 February 2012) <Domestic Drone Use and the Mosaic Theory by Sean Sullivan :: SSRN> accessed 14 July 2022

recognition technology (FRT) for law enforcement in several Indian states is another illustration of how widely surveillance technology is used. Due to the current use of drones with high-resolution cameras and SD cards, it is possible to operate drones alongside FRT and compile significant amounts of personal data with little in the way of transparency, protection, or monitoring. In startlingly similar circumstances, the Supreme Court for Administrative Justice of France forbade and ruled that the Paris police's use of drones to enforce COVID-19 lockdown restrictions violated personal data protection laws, pending the approval of legal safeguards by France's data privacy watchdog.[9] The judge ruled that drones with a range of 80 to 100 meters may theoretically identify people, with the possibility of being used in violation of data protection regulations.

WAY FORWARD IN DRONE RULES, 2021

Numerous changes to drone legislation have been made in the past, but none have taken into account the unique privacy and data protection issues raised by technological advancements such as drones. The following are some recommended methods that might be incorporated into drone rules to protect people's privacy. In order to ensure that the least amount of personally identifiable information is gathered, filtered, and maintained during the operation of the drones, the drone manufacturers should first be encouraged to include correlating and particular features and functionalities that can account for the fundamentals of privacy by design and by default. In order to determine the appropriate security measures and factors that must be integrated into the build and design of the payloads, applications, and functionality of the drone, from the initial design stage, improvement, and production stage, they should comprehensively analyze the possible privacy effect of the drone technology and its probable usage.

Moreover, in order to safeguard personally identifiable information throughout the entire lifetime of the drone, from collection to processing to storage to secure destruction of the data, the government should also incorporate required rules addressing privacy by design and by

[9] Rick Noak, 'In Victory For Privacy Activists, France Is Banned From Using Drones To Enforce Coronavirus Rules' (*Washington Post,* 14 January 2021) <www.washingtonpost.com/world/in-victory-for-privacy-activists-france-is-banned-from-using-drones-to-enforce-covid-rules/2021/01/14/b384eb40-5658-11eb-acc5-92d2819a1ccb_story.html> accessed 13 July 2022

default in the drone legislation. Additionally, the employment of only those drones that adhere to the concept of privacy by design and default must be required of the government agencies participating in the drone operations the government conducts. Furthermore, they must be required to set up systems for receiving comments and reviews, including requests for the principal's data to be accessed, anonymized, or deleted.

Further, in order to minimize privacy concerns, the government agencies involved in the operation of drones must be required to conduct privacy impact assessments (recognizing data protection issues and ensuring remedies to overcome them) and submit the report, in a specified manner, to the DGCA before beginning any program or service that involves handling personally identifiable information. They should also be required to support decent security safeguard policies that manage security risks associated with information recorded during drone operations in accordance with the size and complexity of the operator, the nature and extent of its operations, and the importance of the information collected and retained. The drone operators shall make a good faith attempt to restrict access to the information gathered during drone operations to those who have been given permission.

Thirdly, the government must provide guidelines for best practices in its rules addressing the gathering, storing, retaining, sharing, and erasing of data obtained through the use of drones. For example, drone operators should make reasonable efforts to limit drone activities and processes over an individual's property without that person's express consent, avoid purposefully collecting personal data about individuals without the permission of the data principal, and never keep personal data for longer than is reasonably required to achieve the intended purpose. A built-in system for opportunities to delete or de-identify personal data should also be included in the rule.

Having said that, the DigiSky platform may be used to submit requests pertaining to the deletion of personal data, making the process more transparent and open to the general public.[10] A

[10] 'Digital Sky Platform Launched – India To Start Registration Of Drones, Pilots, And Operators Registration Portal For Online Permission' (1 December 2018) <https://pib.gov.in/newsite/printrelease.aspx?relid=186069> accessed 11 July 2022

written request, a promise that the information won't be shared with anyone else, and a statement that even if it is shared, it will be done in accordance with Indian law are additional baseline procedural safeguards that should be included in the regulations regarding the sharing of data with third parties. Lastly, laws should mandate that reasonable measures be used to get the permission of individuals whose information is likely to be collected via drones. Giving the people advance warning and alerting them of the location and duration of the drone fly would help achieve this. The notice may include information on the following topics like the reason for collecting the data; the categories of data that are intended to be collected; the entities with whom the data will be shared; the process for handling complaints regarding privacy; the duration of the data's retention; and the people or organizations with whom such personal data may be shared. When obtaining consent is not possible, however, as in emergency medical situations or disaster management, for example, personal data may still be processed without the data principal's consent as long as appropriate security measures are taken, such as taking the necessary precautions to prevent misuse, unauthorized access to, modification of, disclosure of, or obliteration of personal data.

CONCLUSION

India is making an attempt to keep abreast of technological advancements occurring throughout the world, but it is falling short in upholding its obligation to protect individual privacy. The current drone usage legal framework falls short on the proportionality yardstick. India must thus pass strong data protection legislation and include protections in the Drone Rules, 2021, in order to guarantee the openness and accountability of monitoring. Regardless of the legislative exemptions granted as per the Puttaswamy Judgment, government agencies must meet the conditions of legitimacy, need, and appropriateness to their purposes. This will require the state to demonstrate that the restriction is supported by legislation, that it serves a legitimate state purpose, that there is a rational connection between the restriction and the purpose, and that the State has chosen the 'least restrictive measure' to accomplish the goal.

However, there is no legal justification for the government's use of drones for surveillance. Furthermore, there is no evidence to support the claim that they are the least restrictive options.

Despite all the advantages of employing drones with cameras, it is impossible to ignore the widespread drone spying that is taking place. Given that India's Drone Rules 2021 include no mention of the word 'privacy', it is critical to consider if such drone usage in India breaches the right to privacy. Unmanned aerial vehicle (UAV)-related technologies are developing at an accelerated rate. The evolution and adaptation of the law may be seen by examining all of India's drone-related legislation. From a complete prohibition on drone usage to a set of laws that didn't deal with all the problems, and eventually to the current drone rules law, 2021. Before the current regulations, there existed ambiguity or confusion surrounding the drone sector. It has been partially cleared up thanks to the new guidelines. However, there are still some important issues that need to be addressed, such as import rules, privacy, and public safety.