

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 3

2022

© 2022 *International Journal of Law Management & Humanities*

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestion or complaint**, please contact Gyan@vidhiaagaz.com.

To submit your Manuscript for Publication at the **International Journal of Law Management & Humanities**, kindly email your Manuscript at submission@ijlmh.com.

Game of Drones: The Invisible Surveillance and Protection of Fundamental Right to Privacy in India

ANKITA SHARMA¹ AND HIYA DAS²

ABSTRACT

The rise of technological innovation and advancement has reached new levels of progressive development. One hallmark of this development is drones. Drones, or unmanned aerial vehicles, are a legion of modern day technology which are capable of flying; and whose capabilities increase, with reduction in cost, by the day. Whether remotely controlled or via an application, they have the capability of reaching remote places, hence why they are being incorporated into various sectors. Globally, drones are used for security monitoring, checking borders, surveillance, and storm tracking. However, these advancements are not bereft of the possibilities of being misused and inflicting damage that they usher in with their introduction. The surveillance function of drones, raises some serious concerns about infringement of citizen's fundamental right to privacy and warrantless search and seizure concerns in the course of conducting their duty and business respectively. To regulate on drone usage in India notified Drone Rules, 2021 which details out the application and registration process to be followed by the interested parties for the allotment of a Unique Identification Number (UIN) for operating a drone. Though the new Drone Rules, 2021 is a welcoming step in encouraging the usage of drones in the country, however, the rules fall short of addressing remedies to privacy harms. There is no mention of the privacy safeguards in the rules. The rules have clearly failed to provide and guarantee the right to privacy as it was held in the Puttaswamy judgment. These lacunae in the present Rules coupled with the conflicting interests of all stakeholders need to be harmonized to prevent excessive government and third party intrusions into an individual's privacy.

Keywords: *Technology, Drones, Surveillance, Right to privacy, Data protection.*

I. INTRODUCTION

The rise of technological innovation and advancement has reached new levels of progressive development. Its utility is self-evident in every sphere of a common citizen's life on a daily

¹ Author is a Research Scholar at North-Eastern Hill University, Shillong, Meghalaya, India.

² Author is a Research Scholar at North-Eastern Hill University, Shillong, Meghalaya, India.

basis for maximization of results and the minimization of the effort involved in achieving them. However, these advancements are not bereft of the possibilities of being misused and inflicting damage that they usher in with their introduction. One such relatively new and unexplored technology which is making inroads into our daily lives is that of Unmanned Aerial Vehicles, or Drones as they are commonly referred to. They are majorly deployed by law enforcement agencies for surveillance purpose and by private enterprises for conducting their operations. Since their inception, they have initiated debates revolving around the citizen's fundamental right to privacy and warrantless search and seizure concerns in the course of conducting their duty and business respectively. While the use of this technology in public places is open to a certain degree of debate, its incursion into a citizen's private life cannot be sacrificed at the altar of law enforcement or profit generating endeavours at the expense of guaranteed civil liberties³.

Subsequent to the exposition of the right to privacy as a fundamental right protected by the Constitution of India in the *Puttaswamy*⁴ judgment, this debate has come into limelight and needs to be addressed before a formal structure pandering to its implementation can be framed. Pursuant to the drastic evolution in drone technology, the Ministry of Civil Aviation had issued Drone Rules, 2021 to regulate on drone usage in India which came into effect from 25th August 2021 and the same has been recently amended on February 11, 2022 as Drone (Amendment) Rules, 2022. The said regulations detail out the application and registration process to be followed by the interested parties for the allotment of a Unique Identification Number (UIN) for operating a drone. Unlike the Unmanned Aircraft Systems Rules, 2021⁵ (UAS Rules, 2021) which puts an obligation on the operator to ensure the privacy of person and property during its operations⁶ and required the drone operator to ensure the privacy of individuals and their property while collecting any video footage or image,⁷ the new Drone Rules 2021 which replaced the UAS Rules, 2021 do not have these safeguards and even the term 'Privacy' has not been mentioned in the document. Further, the Drone (Amendment) Rules, 2022 even remove the requirement of remote pilot certificate (earlier it was called license) for flying small to medium size drones of up to 2kg for non-commercial purposes.⁸ Hence, taking into account the significance of the fundamental right to privacy, these regulations poses a significant doubt

³ Michael C. Heatherly, *Drones: The American Controversy*, 7 J. STRATEG. SECUR. 25 (2014).

⁴ *KS Puttaswamy v. Union of India*, AIR 2017 SC 4161 (India).

⁵ Unmanned Aircraft Systems Rules, 2021 which came into effect from March 2021 was replaced by the Drone Rules, 2021 dated 25th August, 2021.

⁶ Rule 27(h) of the UAS, Rules 2021.

⁷ *Id* [Rule 39(2)].

⁸ Rule 6 of the Drone (Amendment) Rules, 2022.

on the credibility of these regulations to administer the functioning of drones within the Country.

These lacunae in the present Rules coupled with the conflicting interests of all stakeholders need to be harmonized to prevent excessive government and third party intrusions into an individual's privacy.

This paper will focus on studying the contours of right to privacy in India vis-à-vis its application to the use and functioning of drones. Furthermore, it will elucidate on the controversy between privacy rights and use of drones prevailing in foreign jurisdictions. After reviewing the controversy, this paper suggests a model which can be derived for application in the Indian context and conforms to International Standards.

II. THE CONFLICT BETWEEN DRONES AND THE RIGHT TO PRIVACY IN INDIA

In the most basic terminology, drones can be classified as miniscule flying devices that are deployed for aerial navigation.⁹ They are usually designed by fixing a camera and microphone on the aerial device to help them manoeuvre through their path under the control of a human operator with the objective of recording their trajectories and mapping out their surroundings¹⁰. This helps in their utilization by three possible domestic actors who can benefit from their use – commercial entities, law enforcement agencies and the media.

The widespread use of drones for surveillance by the state and for domestic purposes by private entities seems inevitable. The existing privacy law is silent on this, as evident from the Drone Rules 202. Admittedly, drones will further erode our individual and collective privacy. However the inverse may happen. Drones may even help re-establish the present model of privacy violation.¹¹

Drones in India

Drones have been used in India for an extended period of time; however their use caught public imagination recently with India's innovation flight taking off with the launch of key initiatives such 'Make in India', 'Digital India' and a strong focus on IT start-ups.¹² Drones are quickly becoming cost effective and more capable and have been widely acknowledged and adopted by different stakeholders in India, including the government, law enforcement agencies. Indian

⁹ Timothy T. Takahashi, *Drones and Privacy*, 14 COLUM. SCI. & TECH. L. REV. 72 (2012).

¹⁰ *Ibid.*

¹¹ M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. 29 (2011).

¹² *Unravelling the Future Game of Drones, Can they be legitimized?*, NISHITH DESAI ASSOCIATES (April 2018), http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research%20Papers/Unravelling_The_Future_Game_of_Drones.pdf.

law enforcement agencies have been increasingly relying on the use of drone technology for patrolling and surveillance during election campaigning, riots, etc. For instance, drones were used to monitor potential protests during the foundation of the Ram temple in Ayodhya while the Indian Railways have recently procured them to keep railway premises under surveillance.¹³

Such use of drones has become further normalised in India during the COVID-19 pandemic. The Ministry of Civil Aviation conditionally exempted the Government agencies for using drones for aerial surveillance, aerial photography and public announcements relating to COVID-19. Drones were hired to conduct surveillance and collect data in the form of images and videos to ensure people were following lockdown norms.

Drone Regulations in India

Earlier, before the Drone Rules 2021, drones in India were regulated under the Aircraft Rules, 1937 along with provisions of the Civil Aviation Requirements, 2018.¹⁴ The Civil Aviation Requirements (CAR) prescribed manufacture, operation, and registration parameters for drones. However, in terms of privacy safeguards, the 2018 Requirements merely states that the drone operator is required to ensure that the privacy of any entity and did not elaborate on any privacy standards or safeguards for such an obligation.

In March, 2021, the Unmanned Aircraft System Rules, 2021 (UAS Rules) were issued by the Ministry of Civil Aviation replacing the provisions pertaining to drone regulation in the Aircraft Rules, 1937 and the Civil Aviation Requirements, 2018. The UAS Rules were issued to regulate the manufacture, registration, and operation of drones and auxiliary drone infrastructure. The Rules also prescribe some measures for data protection and privacy such as - the drone operator is required to ensure the privacy of a person and their property, to adopt 'suitable' and 'appropriate' mechanism for protecting the data, and prohibit sharing of data gathered by a drone with third parties without explicit consent from the data subjects.¹⁵

However, the UAS Rules offers overarching discretion on crucial aspects of privacy and data protection to the drone operator. That is, the entire onus of protecting individual privacy is on the drone operator, without any procedural safeguards to deal with situations when there is a breach of user data.

¹³ Ibid.

¹⁴ Civil Aviation Requirements, 2018 (CAR) issued by the Director-General of Civil Aviation under the Aircraft Act, 1934.

¹⁵ Abhishek Chakravarty & Archana Sivasubramanian, *The Privacy Question in India's Drone Regulation*, JURIST (April 14, 2021, 11:57:41 PM), <https://www.jurist.org/commentary/2021/04/chakravarty-sivasubramanian-privacy-drone/>.

To overcome this cumbersome nature of the UAS Rules, the Government issued a new drone policy to supersede the UAS Rules, 2021, and replace them with the liberalized Drone Rules, 2021. However, these new rules do not address privacy concerns and it does not include any of the incremental provisions of the UAS Rules on citizen privacy and protection of data collected by the drone. In fact there is no *mention of the term 'privacy' or 'data protection' in the Rules*. This is appalling, especially since in the UAS Rules 2021 which imposed an obligation on authorised unmanned aircraft system operators to safeguard the privacy of a person and its property during operation.¹⁶

Drone Rules 2021 which came into effect from on 26th August 2021 is applicable to everyone who “owns, possesses, or is involved in the leasing, exporting, transferring, or maintaining an unmanned aircraft system in India; or has an unmanned aircraft system in India”.¹⁷ Additionally, these rules would even apply to unmanned aircraft which are flying above the territory of India.¹⁸ It extended the weight limit to regulate the drones with maximum weight up to 500 kilograms¹⁹ which was 300 kg in UAS Rules 2021.

The rules lay down the category of the drone on the basis of their weight. Drones are classified in into following categories: Nano,²⁰ Micro,²¹ Small,²² Medium²³ and Large.²⁴

The Rules mandated that after getting trained from an authorised DGCA-approved drone training institute a person is required to get registered as a Remote Pilot and get a “Pilot Identification number” and Unmanned Aircraft Operator Permit (UAOP) to officially fly drones except nano models up to 250 grams weight in India. It permits nano drones which weigh less than 250 grams²⁵ without mandating the said procedure, except for flying in controlled airspace like airports or other sensitive facilities, which further made it easier to use drones to sneak into anyone’s person or property and take photos and videos of people.

Among the other key provisions of Drone Rules 2021 is the development of the online platform called Digital Sky Platform²⁶ which will be hosted by the Directorate General of Civil Aviation for the management of unmanned aircraft system activities in India. This platform provides a

¹⁶ *Supra* note 6.

¹⁷ Rule 2 of the Drone Rules 2021.

¹⁸ *Ibid*.

¹⁹ *Supra* note 13 [Rule 2(2)].

²⁰ Nano drones are drones of weight upto 250 grams or less (.55 pounds).

²¹ Micro drones are of weight between 250 grams (.55 pounds) and 2 kg (4.4 pounds).

²² Small drones weigh between 2 kg (4.4 pounds) and 25 kg (55 pounds).

²³ Medium drones weigh between 25 kg (55 lbs) to 150 kg (330 lbs).

²⁴ Large drones are all drones exceeding 150 kg (33 pounds).

²⁵ *Supra* note 13 [Rule 5(a)].

²⁶ *Supra* note 13 [Rule 3(1)(g)]: ‘Digital sky platform’ means the online platform hosted by the Directorate General of Civil Aviation for various activities related to the management of unmanned aircraft system activities in India.

single-window operating system for all the required approvals & clearances and makes sure that every drone has been given a unique identification number. This single-window operating system made it easier to get a certificate for flying drones. Also, the “Unmanned Aircraft System Traffic Management”²⁷ will be made on the same platform to give automated permission.²⁸

The Rules provides direct access to the State Governments, Union Territory Administrations and law enforcement agencies to the data available on the digital sky platform.²⁹ Further it empowered the Central Government to exempt any person or class of persons from the operation of these rules, either wholly or partially.³⁰ These rules oversteps the mandate of law that privacy may only be interfered with when it is backed by law by authorizing direct access to data on the platform to governments and law enforcement agencies.³¹

The Government under Ministry of Commerce and Industry issued an order on 9th February 2022 banning the import of drones in India,³² after which the civil aviation ministry has made another major change to the new drone laws in the country with the Drone (Amendment) Rules, 2022. These new amended Rules of 2022 made it more easier for people to fly small drones legally for non-commercial purposes as it removed the requirement of obtaining remote pilot certificate (earlier it was called license)³³ for flying small to medium size drones of up to 2kg for non-commercial purposes.³⁴

Also, the amended Rules removed the requirement of ‘Remote Pilot License’ to legally fly even those drones that are beyond 2kg in weight or for commercial purposes and now they simply require a Remote Pilot Certificate which can be issued by an authorised remote pilot training organisation to any individual.³⁵ This is a major step to make things easier for drone enthusiasts to own and use drones.

²⁷ *Supra* note 13 [Rule 3(1)(zc)]: ‘Unmanned Aircraft System Traffic Management System’ means a system that provides traffic management for safe and expeditious flow of unmanned aircraft traffic and avoids collision between manned and unmanned aircraft through the collaborative integration of persons, information, technology, facilities and services;

²⁸ *Supra* note 13 [Rule 43 (1)].

²⁹ *Supra* note 13 [Rule 25].

³⁰ *Supra* note 13 [Rule 48].

³¹ *Supra* note 4.

³² *All about the import ban on drones*, THE HINDU (Feb. 22, 2022 11:28AM) <https://www.thehindu.com/news/national/watch-all-about-the-import-ban-on-drones/article65073267.ece>.

³³ *Supra* note 13 [Rule 34(4)].

³⁴ *Supra* note 8.

³⁵ *Supra* note 8 [Rule 4].

Thus, most of the rules for drones in India are only for bigger drones (beyond 2Kg weight) and for commercial purposes and for flying a small drone in India one do not require any permission from any authority.

While primary focus has been directed towards the benefits of cost and manpower reduction which can't be entirely negated, some irregularities with its implementation have been overlooked.³⁶ For example, these drones are expected to traverse over areas of personal property, mapping residential blocks or facial features of individuals, creating a database during the course of their journey, as a result compromising his informational and physical privacy. The question pops up as to who will own this data and have access to it. Also how much and in what manner can this data be used further by the data fiduciary. Admittedly, the answers to these questions will vary on a case to case basis, but the position of law still remains silent on these aspects.³⁷

Interface between Right to Privacy and Use of Drones in India

In India, drones are the latest entrants into the debate on infringement of privacy rights with advancements in technology. The advanced drones come with a lot of features including face recognition, a very high-resolution camera, and several other sensors which can very easily invade someone's right to privacy.³⁸

While right to privacy is a constitutionally protected right in India under Article 21 which grants the freedom of life and liberty, there is no legal safeguard against the misuse of personal data gathered through the use of advanced technology such as drones. India's drone regulations have been accused of paying lip service to the issue of privacy.³⁹ In the Drone Rules 2021 which came into effect from August 26, 2021 and has been recently amended in 2022, important privacy concerns remain unaddressed or under-addressed at best as the words like the right to privacy or even privacy haven't been included anywhere in the rules. There are grave repercussions of framing new regulations to govern technologies without ensuring that user data is adequately protected. Personal data is collected, used, processed, analyzed, shared, transferred, copied, and stored by companies at an extraordinary speed and volume than ever before. Data dominance is one of the key drivers to monopolization and abuse of dominance

³⁶ Nigel McKelvey, Cathal Diver & Kevin Curran, *Drones and Privacy*, 6 IJHCR 44 (2015).

³⁷ *Supra* note 12.

³⁸ Dhruv Somayajula, *Eye in the Sky-India's Drone Operation and Privacy concerns*, THE VIDHI (Jul 31, 2021), <https://vidhilegalpolicy.in/blog/eye-in-the-sky-indias-drone-operations-and-privacy-concerns/>.

³⁹ Ananth Padmanabhan, *Drones: It is important to address the privacy issues*, THE HINDUSTAN TIMES (Aug 26, 2019 07:52 AM), <https://www.hindustantimes.com/analysis/drones-it-is-important-to-address-the-privacy-issues/story-T59cmtwbbe7uM2ktOTEEBM.html>.

by firms. Similarly, governments are also expanding their data collection capabilities, evincing mass surveillance.⁴⁰

Although privacy right like any other right is not an absolute right as it has not been categorically mentioned as a constitutional right, judicial interpretation, over the years, has acknowledged the right to privacy as a fundamental freedom under Article 21. The honourable Judiciary at several occasions such as in the case of *Kharak Singh v. The State of Uttar Pradesh*,⁴¹ *Gobind v. State of Madhya Pradesh*⁴² and *R Rajgopal & Anr v. State of Tamil Nadu*,⁴³ has recognized “Right to Privacy” as a part of the “Right to Life and Personal Liberty” guaranteed under Article 19 and Article 21 of the Constitution of India.⁴⁴

The landmark judgment with respect to privacy right in India was delivered in 2017 in the case of *Justice KS Puttaswamy v. Union of India*⁴⁵ in which the Supreme Court upheld privacy as a fundamental right under Article 21 of the Indian Constitution. The apex court also held that although the expectation of privacy in public places cannot be unreasonably high, it does not mean that privacy of an individual should altogether be given up in such places. Addressing the issue of danger of violation of informational privacy in the evolving technology the Court further held that,

*“Information has three facets: it is non rivalrous, invisible and recombinant...invasions of data privacy are difficult to detect because they can be invisible. Information can be accessed, stored and disseminated without notice. Its ability to travel at the speed of light enhances the invisibility of access to data, "information collection can be the swiftest theft of all...”*⁴⁶

The court laid down a four-pronged test of proportionality that must be satisfied for restrictions on privacy to be reasonable:⁴⁷

- i. Restriction on privacy must be enabled by a law:** The first principle laid down by the Court against curtailment of privacy is that of its legality i.e., the action of the State to restrict privacy must be pursuant to an enacted statute. However, the Drone Rules, 2021 do not regulate surveillance and most of the surveillance is being carried out through executive notification only, without any procedural safeguards. Rule 25 of the said Rules oversteps the mandate of law by authorizing direct access to data on the

⁴⁰ *Supra* note 15.

⁴¹ *Kharak Singh v. The State of Uttar Pradesh*, 1963 AIR 1295 (India).

⁴² *Gobind v. State of Madhya Pradesh*, 1975 AIR 1378 (India).

⁴³ *R Rajgopal & Anr v. State of Tamil Nadu*, AIR 1995 SC 264 (India).

⁴⁴ M.P. JAIN, INDIAN CONSTITUTIONAL LAW, (8th ed. 2021).

⁴⁵ *Supra* note 4.

⁴⁶ *Supra* note 4 (Para 173).

⁴⁷ *Supra* note 4.

platform to governments and law enforcement agencies. This rule completely ignores guiding principles of privacy such as purpose limitation, necessity and proportionality. Under the rules, neither is there any compelling state interest for individual data to be accessed nor is there any regulator who will investigate the legitimacy of the request of access to data. Direct access is *ipso facto* provided to all law enforcement agencies. This is a flagrant violation of the consent principle of data. Therefore, there is a need to enact a comprehensive legislation dealing with data protection in general and regulating drone surveillance in particular.

- ii. **Restriction on privacy must be for a legitimate aim:** Most drone surveillance by the government is carried out for maintenance of law and order. However, there is no data to prove that this has facilitated in improving law and order. On the contrary, mass surveillance has severely hampered the free movement of women and other vulnerable groups subjecting them to constant moral policing.
- iii. **Restriction on privacy must be proportionate:** The government must choose the least intrusive means. The use of drone surveillance should be for defined offences and only where less intrusive means are not available. However, the the Personal Data Protection Bill, 2019⁴⁸ which is yet to be notified as law, empowers law enforcement agencies to grant themselves exemptions from the provisions both at the stage of data collection and data processing. Therefore, nothing prevents the law enforcement agencies from using drone surveillance for any purpose including petty offences.⁴⁹
- iv. **Procedural safeguards against excessive interference by the State:** When State agencies carry out covert surveillance during mass processions or festivals, the expectation of privacy cannot be too high. However, the agencies must at least inform the public that a particular area is being surveilled and also give information about the agency that is carrying out the surveillance so that they can access their own data collected through surveillance.

⁴⁸ The Personal Data Protection Bill 2019 (PDP Bill 2019) was tabled in the Indian Parliament by the Ministry of Electronics and Information Technology on 11 December 2019 which has not yet been passed as law and is being scrutinized by a Joint Parliamentary Committee (JPC) in consultation with experts and stakeholders. The Bill covers mechanisms for protection of personal data and proposes the setting up of a Data Protection Authority of India for the same. Some key provisions of the Bill include power of the Central Government to exempt any government agency from the Bill and the inclusion of Right to Be Forgotten.

⁴⁹ Section 35 of the PDP Bill, 2019.

Drones, being one such technological advancement in the country, can eavesdrop in many ways, when looking at state's intrusion on an individual's privacy. For instance, the law enforcement agencies use drones to initiate an incursion into a criminal's hideout, track his movements or monitor him to alert the authorities before he commits a crime. These benefits though are mostly welcome to help control criminal activities and strengthen the law and order regime, but increasingly risk transforming into unfettered powers of carrying out warrantless search and seizure operations in the absence of any definitive regulations addressing them. This unreasonable search and seizure covert operations conducted by drones strike at the very heart of Article 21 of the Constitution and are in violation of the right to life and liberty enshrined in it.

III. DRONE REGULATION AT THE GLOBAL LEVEL

The very first step towards creating an organized setup for drone usage was initiated by the adoption of the worldwide guidelines pandering to unmanned aerial vehicles which were conceived by the 1944 Convention on International Civil Aviation (the Chicago Convention).⁵⁰ It set out some basic rules including that all drones regardless of size are prohibited from flying over another state's territory without its permission.⁵¹ The organization and administration of the Chicago Convention is overseen by the International Civil Aviation Organization (ICAO). ICAO set up an Unmanned Aircraft Systems Study Group (UASSG) in 2007, which united specialists from Member States, partner gatherings and industry, to talk about the effect of drones on aviation directives.⁵²

In November 2014, because of rapid technological innovations in drone technology, the UASSG was conferred with the position and powers of a board, and it is expected to issue certain Standards and Recommended Practices (SARPs) on unmanned aerial vehicles by 2018.⁵³

Other than the ICAO, several countries are also cooperating with JARUS (Joint Authorities for the Rulemaking of Unmanned Systems), which is a body comprising of national civil aviation authorities from EU and non-EU countries and regional organisations. Its aim is to produce a single set of technical, safety and operational requirements for drones.⁵⁴

⁵⁰ ICAO, Unmanned Aircraft Systems (CIR328) (2011), https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf.

⁵¹ Article 8 of the Chicago Convention.

⁵² *Supra* note 50.

⁵³ European Union Committee, *Civilian Use of Drones in the EU*, HOUSE OF LORDS (March 5, 2015), <https://www.publications.parliament.uk/pa/ld201415/ldselect/ldaucm/122/122.pdf>.

⁵⁴ *Ibid*.

Drone Regulations around the World

- **European Union**

Until now Personal data is protected by a set of legal principles in the EU which were found in the Data Protection Directive, which has been serving the EU since 1995. The first ever EU-wide regulations for the civil use of drones were agreed by European Parliament and Council negotiators in 2017 to enhance citizens' fundamental rights to privacy and data protection, to security and to safety. According to the new informal agreement, the design and manufacture of drones will have to comply with EU basic requirements on safety, security, privacy and personal data protection but it did not made any references to drone manufacturers and users.⁵⁵

However on January 1, 2021, the European Union Aviation Safety Agency (EASA) set out the framework for the safe operation of civil drones and has standardized drone regulations throughout its member states.⁵⁶ The new regulatory framework replaces existing regulations that were previously passed into law by individual member states. According to the EASA, flying a drone is legal in the European Union. The new regulations determine drone regulations based on the weight and the specifications of the drone and the operation it is intended to conduct. It defines three categories of civil drone operations that determine drone regulations: the 'open', the 'specific' and the 'certified' category.⁵⁷

- i. **Open Category:** It addresses the lower-risk civil drone operations where safety is ensured provided the civil drone operator complies with the relevant requirements for its intended operation. Operational risks in the 'open' category are considered low and, therefore, no operational authorisation is required before starting a flight.
- ii. **Specific Category:** This category covers riskier civil drone operations, where safety is ensured by the drone operator by obtaining an operational authorisation from the national competent authority before starting the operation. The drone operator is required to conduct a risk assessment, which will determine the requirements necessary for the safe operation of the civil drone(s).
- iii. **Certified Category:** In this category, the safety risk is considerably high; therefore, the certification of the drone operator and its drone, as well as the licensing of the remote pilot(s), is always required to ensure safety.

⁵⁵ Nigel McKelvey, Cathal Diver & Kevin Curran, *Drones and Privacy*, 6 IJHCR 44 (2015).

⁵⁶ *Civil drones (unmanned aircraft)*, EASA, <https://www.easa.europa.eu/domains/civil-drones>.

⁵⁷ *Ibid.*

The management of drone traffic will be ensured through the U-space: a set of services that will be deployed in airspace where heavier traffic is expected, such as in urban areas. The U-space Regulation was adopted in April 2021 which establishes and harmonises the necessary requirements for manned and unmanned aircraft to operate safely in the U-space airspace, so as to prevent collisions between aircraft and to mitigate air and ground risks. The U-space regulatory framework will provide for safe aircraft operations in all areas and for all types of unmanned aircraft operations.⁵⁸

- **United Kingdom**

The Civil Aviation Authority (CAA) in the UK lays down the rules & procedures regarding the operation of drones & unmanned aircrafts. The flying of any ‘drone’ or model aircraft in the UK is regulated by Unmanned Aircraft Systems (UAS) Regulations. Registration is mandatory for flying most drones or model aircraft in the UK. As per the ‘Drone and Model Aircraft Code’, it is illegal to fly a drone without having the required IDs. In the UK, two types of IDs are required to fly drones– Flyer ID (indicating that one has passed the basic flying test) & Operator ID (which is required to be labelled on the drone).⁵⁹

Further, the rules also lay down the category of the drone. Drones are classified in three categories: A, B and C – with the lightest and least complex category A, and the highest category C – based on their weight, technical complexity, and operative environment. The rules & regulations regarding – where to fly, the proximity to crowds, etc. vary based on the category. Category A includes drones weighing up to 7 kg. Drones in this category do not need certification, but pilots must demonstrate their skills to carry them out. Category B drones weigh between 7 and 150 kg. Drones in this group need aviation and operating authorizations as well as proof that they are pilot competence. Category C drones also weigh seven to 150 kg but are very complex to operate technically and are used in complex operating environments. The pilot and operational requirements are identical to those of Category B drones.⁶⁰

⁵⁸ Diganth Raj Sehgal, *A comparative analysis: Drone laws in India with laws in the UK and USA*, IPLEADERS (July 27, 2020), <https://blog.ipleaders.in/comparative-analysis-drone-laws-india-laws-uk-usa/>.

⁵⁹ Scott McLachlan, Kudakwashe Dube & Burkhard Schafer, *Anthony Gillespie, & Norman Fenton, “The Chaotic State of UK Drone Regulation*, RESEARCHGATE (April 2022), https://www.researchgate.net/publication/359721911_The_Chaotic_State_of_UK_Drone_Regulation.

⁶⁰ Agencies Responsible for regulating drones in the United Kingdom (UK), *Drone Laws UK – General rules for flying drones in the UK*, CIVIL AVIATION AUTHORITY (May 19, 2022), https://drone-laws.com/drone-laws-in-uk/#Drone_Laws_UK_-_General_rules_for_flying_drones_in_the_UK.

- **United States**

The USA's Federal Aviation Administration (FAA) retains the responsibility for enforcing Federal Aviation Regulations, including those applicable to the use of Unmanned Aircraft Systems (UAS).⁶¹ As per the regulations of the FAA, it is legal to operate Unmanned Aircraft Systems in the USA. However, every drone is compulsorily required to be registered. The registration is valid for up to a period of three years and requires to be renewed on expiry.

The rules for operating a drone vary based on the type of drone user. FAA categorized drones, based on the type of user into following:

- Recreational user
- Certified remote pilot or Commercial operator
- Public Safety or government user
- Education user.

For registration of drones, users are required to pass certain tests. Recreational users are required to undergo – The Recreational UAS Safety Test (TRUST) and certified user are required to clear FAA's Knowledge Test.⁶²

Further the rules also imposes certain restrictions on the usage of drones in Security sensitive air spaces, including – Military bases, national landmarks, critical infrastructure, etc.

IV. CONCLUSION

Though drones have helped solve some extraordinary problems during national disasters and COVID-19 in India, delivering immense public value, its implication on privacy rights has surprisingly managed to evade much public attention. The use of such new technology raises serious concern regarding the lack of safeguards, oversight, and accountability as no safeguards have been put in place to ensure the abuse of this technology to intrude into people's personal lives and gather information against them.⁶³

The new Drone rules, 2021 are a welcome step in encouraging the usage of drones in the country, however, the rules fall short of addressing remedies to privacy harms. There is no mention of the privacy safeguards in the rules. The rules have clearly failed to provide and

⁶¹ Bharath Kancharla, *Review: How do India's Drone rules compare with those of other countries like the USA & the UK?*, FACTLY (Aug 31, 2021), <https://factly.in/review-how-do-indias-drone-rules-compare-with-those-of-other-countries-like-the-usa-the-uk/>.

⁶² *Supra* note 58.

⁶³ *Supra* note 38.

guarantee the right to privacy as it was held in the *Puttaswamy*⁶⁴ judgment. And the question which arises here is that when the right was included in the previous UAS Rules 2021 explicitly, what was the need to remove it from the new draft when the new rules basically aims to liberalize and make the rules more inclusive and free?

The current drone regulations unaddressed the privacy concerns at best and that there is an immediate need to review these regulations to implement privacy-by-design practices including data minimization and transparency requirements in the current regulatory architecture. *There should be clear rules on data retention. Any information collected through drone surveillance must be kept in protected database for a particular time period during which it would only be accessible to law enforcement officials of certain seniority and that this data may be retained beyond a fixed time period only in exceptional circumstances subject to the approval of an independent higher authority.*

⁶⁴ *Supra* note 4.