*Floriana Granieri*[*]

SPECIAL SECTION

# NAVIGATING THE SKIES: A CROSS-COUNTRY EXPLORATION OF DRONE POLICIES IN EUROPE, USA AND CHINA, UNVEILING PRIVACY AND CYBERSECURITY CHALLENGES

***Abstract***

The article begins with a comprehensive examination of the evolutionary trajectory of drone technology, originally conceived for exclusive military applications but progressively diversifying to encompass a multitude of commercial uses. Notably, the technology has also made its foray into the realm of entertainment, captivating enthusiasts and amateurs alike.

Given this relentless technological advancement and the surging interest in drones - which extends beyond governmental bodies to encompass corporate and individual stakeholders - a multitude of risks associated with the proliferation of these aerial devices has surfaced. Equipped with increasingly intrusive applications, drones have also the potential to significantly impact individual rights such as privacy and security.

The focal point of this article revolves around the intricate nexus of risks concerning privacy and cybersecurity. It delves into an analysis of how major economic powers, attuned to the implications of these technologies, have taken measures to regulate the utilization of drones in order to mitigate the associated risks, while highlighting some issues that still remain in the shadows.

**JEL CLASSIFICATION**: F50, K20, K24, K33

**SUMMARY**



[*] Legal counsel, qualified to practice law in Italy, she is specialised in providing legal assistance and guidance to companies operating in the technology and digital sectors.



DOI 10.13135/2785-7867/10740

## 1 Origins, evolution and contemporary applications of drone technologies

Over the past decade, there has been significant progress in drone technology, leading to their widespread adoption in sectors and environments where their utilisation was previously unforeseen.

A drone is an unmanned aircraft with no onboard crew or passengers. Specifically termed Unmanned Aerial Vehicles (UAVs) or Unmanned Aircraft Systems (UASs) or Remotely Piloted Aircraft Systems (RPASs),[1] drones essentially function as flying robots. These aerial vehicles can be remotely operated (from ground, another aircraft or space) or autonomously navigate through pre-programmed flight paths using software-controlled systems embedded within, which collaborate with onboard sensors and a global positioning system (GPS).

UAVs initially found their roots exclusively in military applications, with their inception dating back to the World War I era. During this period, both the United States and France were actively engaged in the development of automatic, unmanned airplanes for strategic military purposes. However, delving further into history reveals an even more ancient connection: the earliest documented instance of an unmanned aerial vehicle employed in warfare traces back to July 1849. This marked a pivotal moment in military history as it involved the utilisation of a balloon as a carrier, foreshadowing the concept of the contemporary aircraft carrier. In a ground-breaking offensive deployment of air power in naval aviation, Austrian forces besieging Venice embarked on an ambitious endeavour. They sought to launch approximately 200 incendiary balloons, each equipped with a 24 to 30 pound bomb. These airborne devices were intended to be released over the besieged city with precise timing, utilising a time fuse mechanism. Remarkably, this event stands as an early precedent for the strategic use of unmanned aerial vehicles in warfare.

Venturing even further into the annals of history, we find traces of unmanned aerostats being experimented with as early as 1782 by the visionary Montgolfier brothers in France.[2] Their pioneering efforts involved the initial exploration of balloons as unmanned platforms before they themselves ascended into the skies. This prelude to manned flight serves as a testament to the progressive evolution of unmanned aerial technologies, stretching back through centuries of innovation and experimentation.

Initially conceived for applications in the military and aerospace sectors, drones have seamlessly integrated themselves into "mainstream" usage. This widespread adoption can

[1] In its Briefing on the '*Civil and Military Drones - Navigating a disruptive and dynamic technological ecosystem*" the European Parliament has tried to "*decipher the vocabulary of drones*': the term "drone" is generically used to simplistically refer to various unmanned aircraft, such as UAVs (unmanned aerial vehicles), RPAS (remotely piloted aircraft systems), and UAS (unmanned aircraft systems), which actually differ significantly from each other. For example, the term RPAS refers exclusively to a remote pilot station and control functions. Drones (in the all-encompassing meaning of the term) vary in size, with categories such as micro, mini, small, medium, and large, each serving different purposes. The autonomy of drones, involving independent sensing, decision-making and action, has been debated and has roots in artificial intelligence, robotics and control theory.

[2] For a brief historical overview of the origins of drones: John Romero, 'When were Drones Invented? History From 1783 to 2024' (*Drone Guider*, 25 May 25 2023) <https://droneguider.com/when-were-drones-invented> accessed 8 May 2024.

be attributed to the manifold benefits they offer, including elevated safety standards, pioneering technological innovations, and a marked increase in operational efficiency.

Numerous drones in the modern era showcase a diverse range of sophisticated features, exemplified by the incorporation of cutting-edge cameras designed for the acquisition of visual data. Additionally, the inclusion of sophisticated propellers plays a key role in ensuring and stabilising their flight patterns, further contributing to their versatility and adaptability.

This transformative technology has sparked a paradigm shift in various industries.[3] Enhancing operational efficiency and boosting productivity, reducing workloads and production expenses, enhancing precision, refining customer service, and fostering improved customer relations represent just a few of the key advantages that drones confer upon industries on a global scale.

However, the influence of drones is not confined to the realm of business utility. The burgeoning popularity of drones among hobbyists underscores their multifaceted appeal, extending beyond professional applications. The drone technology in recent years has been fuelled also by the enthusiasm of recreational users, who engage in recreational drone flying purely for enjoyment, diverging from any commercial objectives.

This broader recognition has therefore permeated various sectors, with individuals, commercial enterprises, and governmental bodies acknowledging the myriad advantageous features that drones bring to the table.

The multifaceted applications of drones in all these domains underscore their capacity to revolutionise traditional practices and enhance overall productivity. As these sectors continue to integrate and explore the potential of drone technology, paired with the evolution of Artificial Intelligence, the trajectory of innovation is poised for further expansion and diversification.

[3] Drones are employed, by way of example: (1) in the **agriculture** business for crop monitoring purposes (assessment of crop health, identification of diseases, and an overall evaluation of crop conditions) or for facilitating the precise and efficient application of fertilisers, pesticides, and water; (2) in the **videography and photography** business (cinematography, particularly in the film and entertainment industry, relies on drones to achieve dynamic and creative aerial perspectives, adding a new dimension to visual storytelling); (3) in the **infrastructure** sector, enhancing safety and efficiency in monitoring utility infrastructure, bridges, buildings, etc. monitoring construction sites, track progress, and provide valuable data for project management; (4) for **searching and rescuing** purposes, proving invaluable during disaster response; (5) for **environmental monitoring** purposes, firefighting, or wildlife conservation, tracking and studying animal behaviour, and assessing the health of ecosystems; (6) in **delivery services**; (7) for **public safety initiatives**, event surveillance, monitoring large public gatherings, enhancing security measures and crowd management; (8) for **scientific research** purposes, even ocean research, where drones are utilised for studying ocean currents, wildlife, and pollution levels, providing valuable insights into marine ecosystems, (9) for **surveillance** purposes.
These are just a few examples testifying how the diverse applications of drones underscore their transformative impact across industries, contributing to efficiency, safety, and innovation.

## 2 Implications in civil drones' usage and regulatory responses in Europe, USA and China

With the increasing prevalence and diverse applications of drones - even among non-professionals and amateurs - the risks associated with the use of these UASs have increased significantly.[4]

First, liability profiles emerge regarding personal injury and property damage.

The increasing accessibility of drones is also expected to increase the number of disruptive incidents in public spaces,[5] increase noise pollution, and thus affect bird and wildlife populations.[6]

Important and worrying implications also involve issues of privacy and cybersecurity. It is on these issues that the following chapters of this article will focus.

Precisely because of the increasing uses and risks associated with the use of drones, governments, aviation, aeronautical and international authorities have expressed growing concerns, leading to discussions and the formulation of appropriate safety standards, as well as legal and ethical regulations for both drones manufacturers and drone flyers.

An integral player in this international discourse is the International Civil Aviation Organization (ICAO), a specialised United Nations agency tasked with overseeing the Convention on International Civil Aviation, commonly known as the Chicago Convention. Collaborating with its 193 member states,[7] the ICAO endeavours to establish universal

[4] See Sarah J Fox Dr, 'The Rise of the Drones: Framework and Governance - Why Risk It!' (2017) 82(4) Journal of Air Law and Commerce 683.

[5] There are already a large number of recorded incidents between drones and other aircraft. Just to mention a few: in July 2017, an Airbus 319 was preparing to land at Gatwick Airport when a UAV appeared and flew over the aircraft's starboard wing. The U.K. Airprox Board report on the incident stated that there was a high risk of collision and that "*a larger aircraft might not have missed it and in the captain's opinion, it had put 130 lives at risk*". The report stated that the estimated distance and the pilots' inability to avoid the UAV "*portrayed a situation where providence had played a major part*" in avoiding a crash. The pilot described the situation as a "*worrying near-miss that could have ended in tragedy*".
In September 2017, a civilian UAV collided with a UH-60 Black Hawk helicopter of the 82nd Airborne Division on duty for the United Nations General Assembly over the east coast of Staten Island, New York, in the United States. Fortunately, no one was injured, and the National Transportation Safety Board's report on the accident found that the responsibility for the accident was solely attributable to the pilot of the UAV who had deliberately flown the UAV 2.5 miles away from himself, was unaware of the presence of the helicopters, and had shown only a general and cursory knowledge of the regulations.
More recently, in August 2021, a Canadian Flyers International Inc. single-engine aircraft collided with a drone operated by York Regional Police while on approach to Buttonville Municipal Airport. The aircraft fortunately landed without injury to the people on board, but sustained severe damage, including a bent airbox, a damaged engine cowling, and a struck propeller.

[6] In most of the National Parks in the USA, such as Glacier National Park, Arches National Park, Acadia National Park, Yellowstone National Park and Yosemite National Park the use of drones is prohibited. Same limitations apply to the use of drones is in most of the National Parks and natural reserves in Europe and in China.
Several studies have shown how the buzzing of drones negatively affects the bird population: on one hand, the ability of birds to communicate during reproduction is hindered by the sound of drones; on the other hand, the noise emitted by drones can escalate to levels that disturb and agitate birds, prompting defensive reactions such as attacking the drone. Birds may perceive the drone as a threat and a potential predator, leading to confrontations that can result in injuries.

[7] The list of the ICAO member states can be found at this link: <https://www.icao.int/about-icao/Pages/member-states.aspx> accessed 8 May 2024.

standards and practices, addressing various aviation matters, including the evolving landscape of drone usage. In response to the escalating regulatory challenges posed by the rapid proliferation of UASs, the ICAO introduced a UAS toolkit.[8] This toolkit serves as a comprehensive resource, offering guidance for both drone operators and regulatory bodies in navigating the complexities associated with drone operations.[9]

On a national scale, the following paragraphs seek to explore key regulations implemented by governments of major economic powers that have made substantial investments in these emerging technologies in recent years.

### 2.1 General overview of UAS legislation in Europe

At European level, the authority to regulate civil drones was delegated to the European Commission in the wake of the introduction of Regulation (EU) 2018/1139, commonly referred to as the "Basic Regulation".[10] This regulation establishes uniform guidelines in the realm of civil aviation, encompassing drones with an operating mass exceeding 150 kg but excluding those designated for military, customs, police, or fire-fighting purposes. As drone technology evolves, the Commission is empowered by this Regulation to enact delegated acts.[11] The responsibility for collecting, analysing and publishing safety information concerning drone operations lies, at EU level, with the European Union Aviation Safety Agency ("**EASA**"), established with this Regulation and, nationally, with Member States' authorities.

EASA aims to establish a unified regulatory framework across European Union Member States, fostering a seamless internal aviation market within the EU.[12] The agency is tasked with formulating operational rules, certifying products and organisations, conducting

[8] UAS Toolkit <https://www.icao.int/safety/UA/UASToolkit/Pages/default.aspx> accessed 8 May 2024.
[9] The role and importance of the ICAO has increasingly grown as this technology has developed and spread to provide clearer guidance and uniformity in the regulation of drones. In this regard, see Ewen Macpherson, 'Is the World Ready for Drones?' (2018) 43(2) Air and Space Law 149.
[10] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 [2018] OJ L 212/1.
[11] On 11 June 2019 the Commission published the Commission Delegated Regulation (EU) 2019/945 and the Commission Implementing Regulation (EU) 2019/947 to ensure drone operations across Europe are safe and secure. The regulations will, among other things, contribute to safeguarding the safety and privacy of citizens in the European Union. Simultaneously, they will facilitate the unimpeded movement of drones and establish equitable conditions across the EU. The Commission Delegated Regulation (EU) 2019/945 has been amended by the Commission Delegated Regulation (EU) 2020/1058. The Commission Implementing Regulation (EU) 2019/947 has been amended and integrated several times, lastly with the Commission Implementing Regulation (EU) 2022/425.
[12] For this purpose, the EASA has initiated a project, known as "eRules," which consists of a single, easy-access online database for all aviation security rules applicable to persons and organisations subject to the Basic Regulation. The result of that project is the Easy Access Rules ("**EAR**"). These are consolidated versions of these rules, combining EU regulations with EASA's Acceptable Means of Compliance (AMC) and Guidance Material (GM) in an easy-to-read format with advanced navigation features.

supervision, and collaborating with international entities on aviation safety issues.[13] Notably, EASA was entrusted by the Commission, Member States, and various stakeholders to formulate recommendations for a regulatory framework governing civilian drone operations.[14]

The synergy between the European commission and the EASA, along with other actors on aviation safety matters, has made Europe the first region in the world to have a comprehensive set of regulations ensuring safe and sustainable drone operations.

In the European context, there are three main categories of UAS (open, specific and certified) to which correspond different technical characteristics, different categories of associated risks, and with respect to which, depending on the case, prior authorisation for use by the competent national authority and/or declaration by the UAS operator is required.

Each category provides for sub-classifications of UAS that must be certified by manufacturers according to precise technical requirements covering elements such as maximum take-off weight (MTOM), sound power level, the presence of certain safety features, and the ability to share information.

As for operators, they must proceed to apply for an authorisation with the National Aviation Authority of the European country of residence, unless the drone (*a*) weighs less than 250 g and has no camera or other sensor able to detect personal data; or (*b*) even with a camera or other sensor, weighs less than 250 g, and it is a toy (meaning that its documentation shows that it complies with the 'toy' Directive 2009/48/EC).

The drone operator registration number must be mandatorily displayed with a sticker on all drones owned by the registered operator.

Drone operators are always required to have insurance for their drone if they are using a drone with a weight above 20 kg. However, most of EASA Member States mandate a third-party insurance also for operating a lighter drone.

The management of drone traffic will be ensured through the U-space:[15] an air traffic control system for UASs. The U-space Regulation establishes and harmonises the necessary requirements for manned and unmanned aircraft to operate safely in the U-space, so as to prevent collisions between aircraft and to mitigate air and ground risks.[16] The U-space

[13] The EASA has issued the ED Decision 2019/021/R, amended by the ED Decision 2022/002/R, issuing Acceptable Means of Compliance and Guidance Material to Commission Implementing Regulation (EU) No 2019/947.

[14] Regulatory framework background for drones <https://www.easa.europa.eu/en/domains/civil-drones/drones-regulatory-framework-background> accessed 8 May 2024.

[15] There was already talk of this in the past: Matteo Carta, Costantino Senatore, Filippo Tomasello, 'U-Space is Coming' (2018) 17(2) The Aviation & Space Journal 16; Mikko Huttunen, 'The U-space Concept' (2019) 44(1) Air and Space Law 69.

[16] The U-Space aims at avoiding collisions between unmanned and manned aircraft; minimising the risk to persons and objects on the ground; facilitating the orderly conduct of unmanned flights; providing information necessary for safe flight operations; informing the appropriate authorities when a drone poses a danger to other aircraft or people on the ground due to a disaster; ensuring compliance with Member States' security, privacy and environmental requirements.

consists of a set of agreements, protocols, means of communication, and standards[17] that together must ensure that the growth of unmanned air traffic will proceed in an orderly manner in the future.

## 2.2 General overview of UAS legislation in USA

Drones are allowed in the U.S, whether they're for recreational or for commercial uses. The Agency responsible for regulating drones in the United States of America is the Federal Aviation Administration ("**FAA**"), which has set several federal rules and regulations that, together with local laws, draw the boundaries of legitimate UAS production and use in the USA.

Title 14 of the Code of Federal Regulations establishes that unmanned aircraft produced for operation in the airspace of the United States are subject to the production requirements of Part 89.[18] Subpart D of such Part 89 requires a remote identification system ("Remote ID") for unmanned aircraft operated in the airspace of the United States.

Remote ID is the ability of a drone in flight to provide identification and location information that can be received by other people through a broadcast signal.

The FAA has implemented performance-based requirements that describe the desired outcomes, goals, and results for Remote ID without establishing a specific means or process for regulated entities to follow.

A person producing a standard remote identification unmanned aircraft or remote identification broadcast module for operation in the United States must show that the unmanned aircraft or broadcast module meets such requirements by following an FAA-accepted means of compliance (MOC).

Regarding, however, the use of drones and, in particular, the recreational use the USA Hobbyist Drone Law[19] applies: under this law a person may operate a small unmanned aircraft of less of 55 pounds (250 g) without specific certification or operating authority from the FAA if they follow certain limitations, such as operating strictly for recreational purposes,[20] adhering to safety rules made by a community-based organisation in collaboration with the FAA,[21] and flying within visual line of sight.

[17] The U-Space regulatory package was published on 22 April 2021: <https://www.easa.europa.eu/en/regulations/U-space> accessed 8 May 2024.
[18] US Code of Federal Regulations <https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-89> accessed 8 May 2024.
[19] Section 44809 of title 49 of the United States Code (49 USC 44809) is the law that sets out the limitations for operating small, unmanned aircraft for recreational purposes. The law is sometimes called the FAA 44809 or FAA Recreational Flyers 44809.
[20] A recreational flyer is a person who operates an unmanned aircraft system strictly for recreational purposes: flying only for fun and not for work, payment, or as part of any business. Compensation, or the lack of it, does not determine if a flight is recreational or not. To be considered a recreational UAS drone flyer, the aircraft must be flown strictly for recreational purposes, and the operator must follow the conditions set by the FAA in accordance with 49 USC 44809.
[21] Under the USA Hobbyist Drone Law the term "community-based organization" refers to a membership-based association entity that: (*i*) is described in section 501(c)(3) of the Internal Revenue Code of 1986; (*ii*) is tax-exempt

The law requires that all recreational flyers pass an aeronautical knowledge and safety test and provide proof of passage of such TRUST (Recreational UAS Safety Test) if asked by law enforcement or FAA personnel, and registering and marking the aircraft.

The violation of the USA Hobbyist Drone Law exposes the recreational flyer to criminal and/or civil penalties.

As per the commercial use the FAA Part 107[22] applies: under this law, drone pilots may operate a small UAS of fewer than 55 pounds, for work or business, with specific certification or operating authority from the FAA. The law also requires passing an aeronautical knowledge and safety test and registering and marking the drone.

If the drone is used for commercial activities a "drone license" is needed. The Remote Pilot Certificate is issued by the FAA to flyers that meet certain requirements: be at least 16 years old; be able to understand, speak, read, and write English; be mentally and physically fit to fly a drone; pass the required aeronautical knowledge exam "Unmanned Aircraft General – Small (UAG)".[23] Once the certificate is obtained this must be readily available during all UAS operations and certificate holders are required to complete an online recurrent training to maintain aeronautical knowledge recency, every 24 calendar months.

Drone insurance is not required but recommended for both recreational and commercial drone operations.

In terms of drone air traffic management in the United States, as in many other jurisdictions, airspace is classified as regulatory and nonregulatory and, within these categories, as controlled (Classes A, B, C, D and E) and uncontrolled (Class G). The different airspace classes are defined according to the level of air traffic control services provided to flights: Class A airspace is the highest level of controlled airspace, while Class G airspace is the least restrictive and uncontrolled. The airspace classes have different requirements for pilot certification, equipment and communication with air traffic control.

In order to fly in controlled airspaces (Classes A-E) a permit is required. Low Altitude Authorisation and Notification Capability (LAANC), run by the FAA, is the only way to get permission to fly in controlled airspace and it is available for pilots operating both under USA Hobbyist Drone Law and Small UAS Rule Part 107.

Although Class G is defined as the "uncontrolled" zone, there are still instances where drones can't fly in this class airspaces. There are areas within class G that are regarded as Special Use Airspace which consists of areas where specific activities must be confined

under section 501(a) of the Internal Revenue Code of 1986; (*iii*) whose mission is demonstrably the advancement of model aviation and (*iv*) provides a comprehensive set of safety guidelines for all aspects of model aviation addressing model assembly and operation.

[22] Title 14, Chapter I, Subchapter F, Part 107 of the United States Code is the law that sets out the FAA Regulations for Small Unmanned Aircraft Systems.

[23] The test consists of 60 questions and covers different parts of drone operation, such as FAA rules, airspace, weather, what to do in an emergency etc.

to that area or where limitations are imposed upon other aircraft that are not a part of those activities, "No-Fly zone" and "No-Drone zone".

The National Aeronautics and Space Administration (NASA) agency has developed a drone traffic management platform to manage large numbers of drones flying at low altitude along with other airspace users, known as UAS Traffic Management, or UTM.

UTM represents an architectural framework leveraging the industry's capability to offer third-party services developed within the industry. These services function in harmony with the Air Traffic Service (ATS) provided by the FAA. The primary objective is to facilitate the exchange of pertinent air vehicle information within UAS operations and establish seamless communication between the UTM and the traditional Air Traffic Management (ATM) system.[24]

## 2.3 General overview of UAS legislation in China

It is a well-known fact that China has emerged as a global leader in the development of unmanned systems, showcasing significant advancements in technology and innovation. The country's robust commitment to research and development, coupled with substantial investments in cutting-edge unmanned aerial, ground, and maritime systems, has propelled it to the forefront of this rapidly evolving field. China's achievements are evident in various sectors, but most of all the nation has demonstrated prowess in the manufacturing and deployment of drones for surveillance, disaster response, and scientific research.[25] The comprehensive regulatory framework implemented by Chinese authorities reflects a proactive approach to managing unmanned systems, fostering an environment that encourages growth, safety, and responsible use.

[24] Jaewoo Jung, Joseph L Rios, Min Xue, Jeffrey Homola, Paul U Lee, 'Overview of NASA's Extensible Traffic Management (xTM) Research' (AIAA SciTech Forum, San Diego, CA & Online, 10 January 2022) <https://ntrs.nasa.gov/citations/20210025112> accessed 8 May 2024.
The paper takes an in-depth look at the evolution of this system. In the wake of the success of the UTM architecture, the characteristics of UTM have been broadened to evolve into a new Extensible Traffic Management (xTM). This adaptation aims to support operations extending beyond small Unmanned Aircraft Systems (UAS), encompassing activities like high-altitude operations exceeding 60,000 feet.

[25] The outbreak of the coronavirus in China has spurred extensive exploration into various cutting-edge technologies, with drones at the forefront. The government has adeptly leveraged these technologies to overcome a time when human contact and proximity posed significant risks. One notable application involves the aerial spraying and disinfection conducted by drones. Drawing upon the established use of drone technology in agriculture for pesticide spraying, authorities have employed drones to disinfect large public spaces and outbreak prevention vehicles, effectively minimizing the spread of the virus. Furthermore, drones have been instrumental in the efficient delivery of medical samples and essential consumer items, mitigating the need for direct human contact while ensuring the continued accessibility of food, basic necessities, and vital medical services. Additionally, drones have been harnessed for surveillance purposes, serving as a deterrent for gatherings and offering real-time monitoring for rule enforcement. Numerous videos circulating online showcase how drones relay live messages and reprimands to individuals, urging them to adhere to safety measures such as wearing masks and maintaining social distance, thus demonstrating China's ever-increasing commitment to implementing sophisticated vehicles and smaller unmanned platforms as a tool of mass surveillance, as well as real social control.

China's leadership in the development of unmanned systems underscores its strategic vision and dedication to shaping the future of autonomous technologies on a global scale, and it is poised to play a dominant role in shaping industry trends.

Drone use in China is subject to the Civil Aviation Administration of China ("**CAAC**") regulations.

Drones are classified into 5 categories,[26] depending on their weight (empty vs. full), to which correspond different maximum height and maximum speed rules. Every drone over 250 g must have a real-name registration[27] with the CAAC, whether it's used for recreational or business purposes, and the registration sticker must be printed and displayed on the drone at all times.

For commercial uses and for all drones weighing between 7 and 116 kilograms a CAAC license is needed.[28] For all drones weighing more than 116 kilograms a pilot's license and UAV certification are required.

Drone pilots must insure themselves against liability to third parties[29] and must not have had or have any illnesses that could affect their flying behaviour and a history of drug use and/or criminal convictions for intentional crimes that endanger national security, public safety or the personal rights of citizens within the past five years. They must abide by No-Fly Zones that include areas over airports and surrounding areas, border lines, military security areas, nuclear facilities, the production and storage areas of flammable and explosive dangerous goods, public infrastructure such as power plants, substations, fuelling stations (gas), water supply facilities, public transportation nodes, navigation and power nodes, large water conservation facilities, ports, freeways, rail electrification lines and specific cities such as Beijing and sensitive areas such as Xinjiang and Tibet.

On 28 June 2023, the State Council and the Central Military Commission of China jointly issued the Interim Regulation on the Administration of the Flight of Unmanned Aircraft (hereinafter referred to as the "New Regulation"), which consists of 63 articles in 6 chapters and has come into force on 1 January 2024. According to this new set of rules the use of drones in China must adhere to and reinforce the party leadership, adhere to

[26] Micro (Class 1): weight less than 250 grams, maximum height 50 m, maximum speed 40 km/h, low power radio signal; Light (Class 2): empty weight up to 4kg with MTOM up to 7 kg and maximum speed 100 km/h; Small (Class 3): empty weight up to 15 kg with MTOM up to 25 kg, with systems that allow it to fly in controlled airspace and be monitored for traffic management; Medium (Class 4): MTOM up to 150 kg and Large (Class 5): MTOM greater than 150 kg.

[27] Registration requires the individual's personal information and information about the drone and its intended use: proprietor's name and a valid personal identification number (such as an ID or passport number), a telephone number and e-mail address, model and serial number of the product and a declaration about the intended use of the drone. Registration may require knowledge of the Chinese language and possession of a Chinese mobile phone number.

[28] To apply for a commercial drone flight permit in China, the following requirements must be met: the legal business entity must have a legal representative who is a Chinese citizen; it must already own at least one registered drone with the Aviation Authority; it must have a liability insurance to cover the use of the drone and the drone operator must be certified through a Chinese government-approved training programme.

[29] According to article 12 of the Interim Regulation on the Administration of the Flight of Unmanned Aircraft liability insurance is not legally required for the use of civil UAS in micro and mini category. In any case, insurance coverage is always recommended.

the overall concept of national security, and adhere to the principles of security first, service development, classified management, and coordinated supervision.[30]

The New Regulation marks the first comprehensive governance of unmanned aircraft flight management in China, with new rules and directions regarding the management system, procedures, a new official classification of UASs, and specific requirements and recommendations about high-quality safety management in low-altitude operations. The New Regulation serves to enhance and reinforce the establishment of a safety control system, fostering the creation of standardised frameworks for the research and development, production, and utilisation of unmanned vehicles. Its aim is to facilitate the systematic and organised growth of the market. Oversight and enforcement will involve key governmental bodies, including China's General Administration of Civil Aviation, the Ministry of Public Security, the Ministry of Industry and Information Technology, and the State Administration for Market Regulation, among other relevant state authorities.

The New Regulation also aims to strengthen the air traffic management system by entrusting national air traffic management regulators with the construction of an integrated and comprehensive supervision service platform for unmanned aircraft and the implementation and dynamic supervision for unmanned aircraft throughout the country.

In this regard, there is an emphasis on enhancing the oversight of low-altitude airspace. Considered a crucial strategic asset for nations, low-altitude airspace holds significant economic, national defence, and social value, being the airspace closest to the surface. The regulations dictate that, while prioritising safety, the state must proactively innovate the systems governing airspace provision and utilisation. Furthermore, the provisions specify that areas beyond the controlled zone are deemed suitable for micro, small, and light unmanned aircraft.

These measures are designed to optimise airspace resources, ensuring effective regulation of the organisation and implementation of flight activities.

## 3 "Unmanned eyes" in the skies: privacy implications in drone utilisation

As delineated in previous paragraphs, the escalating interest in the production, commercialisation, and utilisation of drones is affecting several fronts, from governmental bodies, to industries, small and medium-sized enterprises, and private companies, which are recognising drones as a burgeoning resource. Moreover, given their current affordability in the market, the utilisation of drones by individuals has experienced a remarkable exponential surge.

The current and prospective development of drones has several positive impacts, particularly for industrial development, and safety and growth in general. Indeed, drones

[30] See article 3 of the Interim Regulation on the Administration of the Flight of Unmanned Aircraft.

can perform operations in emergency situations, where human intervention is impossible or difficult, and in any case greatly facilitate other human operations.

While the development of drones has multiple positive impacts, it also requires conscientious consideration of the associated risks. Like any other technology, drones introduce potential challenges that stakeholders, regulators, institutions, and citizens must address to avert, minimise, and counter negative impacts.

For example, the ability of civil drones equipped with advanced cameras and sensors to capture high-resolution images and videos, coupled with their capacity for agile and discreet flight, raises pertinent questions about the boundaries between public safety and personal privacy.

This paragraph sets the stage for an exploration of the nuanced and complex privacy implications entwined with the burgeoning use of civil drones in our contemporary society.

The latest generation of drones are often integrated with certain applications, such as video cameras and other recording tools, high-power zoom, facial recognition, behaviour profiling, movement detection, number plate recognition, thermal sensors, night vision, radar, see-through imaging, Wi-Fi sensors, microphones, audio recording systems, biometric sensors, GPS systems, IP address reading, and RFID device tracking.[31] This multifaceted functionality underscores the collection, processing, recording, organisation, storage, use, and combination of data capable of directly or indirectly identifying individuals. These activities intrinsically interfere with the right to private life and data protection.

A crucial aspect of this discussion is the unobtrusiveness and inconspicuous nature of certain drones due to their small size, noiseless performance, or disguises,[32] amplifying the complexity of the privacy concerns as, in this way, they are not perceived as such by people and blend in with their surroundings, sometimes making data processing concealed.

The evolving capabilities of UAS and their technological integrations magnify the nature of surveillance, presenting distinctions from conventional tools like satellites, aircraft, helicopters, and CCTV: drones are not always detectable, as they are not always visible or heard, especially micro and small drones; they allow for a mobile and detailed view, including 3D; they can access more locations, including private properties and, unlike

[31] Ottavio Marzocchi, '*Privacy and Data Protection Implications of the civil use of drones*' (European Union, Brussels, 2015) <https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/519221/IPOL_IDA (2015) 519221_EN.pdf> accessed 8 May 2024. Back in 2015, the Directorate-General for Internal Policies of the European Union, in its in-depth research had pointed out the privacy risks generated by the implementation and integrations of these applications.

[32] In this regard, as reported by the South China Morning Post, Beijing has dedicated substantial resources to the advancement of swarms of unmanned aerial vehicles meticulously crafted to emulate the appearance and movement of birds, particularly doves. Remarkably convincing, these devices can effortlessly navigate over groups of sheep, which are typically highly alert and sensitive to aircraft, without arousing suspicion among the animals. This showcases the remarkable capability of these machines to effectively disguise themselves and operate undisturbed.

other technologies present certain advantages such as being cost-effective and persistent.[33]

Consequently, the following paragraph emphasises the vital need for comprehensive regulation governing drones and their applications, seen as essential to ensure the respect of fundamental rights, particularly privacy and data protection, as well as safety and security, across the whole drones' chain, from manufacturing to commercialisation to usage.

## 4 Regulatory perspectives on privacy management in drone usage

Data protection is a major issue today, having gained significant prominence in most jurisdictions and, especially, in Europe. The European Union has taken a pioneering role in establishing comprehensive regulations to safeguard people's privacy and personal data. The right to the protection of personal data is a fundamental right of the individual under the Charter of Fundamental Rights of the European Union.[34] Nowadays it is protected, in particular, by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data ("GDPR")[35] which represents a milestone by setting strict standards for the collection, processing and storage of personal data. This legislation reflects a growing awareness of the central role that data plays in our interconnected world and underscores the importance of ensuring that people's rights are respected also in the digital landscape. GDPR not only imposes obligations on companies and organisations, but also gives individuals greater control over their data.

Yet, enforcing these regulations encounters challenges, especially when it comes to drones.

The Basic Regulation mandates that drone operators and remote pilots must be well-versed in applicable European Union and national rules, emphasising safety, and data privacy. It underscores the necessity for drones to possess specific features aligning with privacy and personal data protection principles from the design phase onward. In addition, as we have seen in previous paragraphs, the Basic Regulation provides for measures that are aimed not only at protecting physical safety but, among other things, protecting privacy: requirements to register the drone and/or receive authorization with the National Aviation Authority, rules inherent in-flight heights etc.

[33] See the '*Privacy and Data Protection Implications of the civil use of drones*' (n 31).
[34] Article 8 of the Charter of Fundamental Rights of the European Union states "*Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority*".
[35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

However, the issue of data protection is not directly addressed by European UAS regulations and does not form an integral part of such regulation, but has remained entrusted to other, stand-alone regulations, which are, in fact, referred to by the EU regulations governing and regulating UAS. In particular, the reference is to the GDPR, and to regulations, guidelines and recommendations issued by individual member states, national and supranational Agencies and Authorities.[36]

Thanks to this fragmented but rich set of information, it is therefore possible to outline a privacy-proof set of rules and proper practices for the use of drones.

First of all, it is fundamental to adhere to the technical-operational-design principles of privacy by design and by default. These innovative concepts, introduced by the GDPR, on the one hand (privacy by design), aim to ensure the existence of a proper level of privacy and protection of personal data from the design phase of any system, service, product or process as well as during their life cycle; and on the other hand (privacy by default) it requires protecting the privacy of data subject "by default", ie, as a default setting, by requiring the controller to comply with the fundamental principle of data minimisation, ie, to identify, before starting data processing, which personal data are strictly necessary for the specific purpose for which they were acquired.

In addition, compliance with all general principles outlined in Article 5 of the GDPR is mandatory.

The processing must, first and foremost, be lawful: to this end, it will first be necessary to carry out a study of the national legislation to ascertain that it permits the use of drones and, if necessary, to apply for authorisations - where required - from the competent authorities. Failure to comply with national requirements on how drones should be used could in fact make the processing of data acquired through the use of these tools unlawful. Data acquisition and processing must rest on legal bases provided by Article 6 GDPR and align, when applicable, with the principles of Article 9.

Given the unique challenges posed by data collected through drones, conducting an impact assessment under Article 35 or seeking prior consultation with the Data Protection Authority under Article 36 is recommended, ensuring compliance with the principle of accountability and a comprehensive risk assessment regarding the rights and freedoms of data subjects.

Transparency, a fundamental principle under Article 5, is crucial. Operators should strive to make flight operations transparent by providing notices, where permitted by law, clarifying the purpose of data processing. To this end, it is also advisable that the pilot is

[36] In this regard, the Agencia Española de Protección de Datos (AEPD) has always been an important information resource and, also on this issue, has published a *vademecum* with a guide for privacy-proofing aerial operations, outlining the preliminary operations and activities deemed necessary in this regard.
The Italian Data Protection Authority has also published a simple and intuitive infographic *'Consigli per rispettare la privacy se si usa un drone a fini ricreativi'* to direct the behaviour of data controllers toward ethical and correct conduct in September 2021
<https://www.garanteprivacy.it/documents/10160/0/Utilizzo+di+droni+a+fini+ricreativi+e+privacy_+l%27infografica+del+Garante.pdf/482c901c-acc1-4aeb-9a9a-556376f84156?version=2.0> accessed 8 May 2024.

always visible and easily identifiable by anyone who wishes to ask for information or wants to object to the filming or other data acquisition activities or deny consent to the processing of the data collected, or exercise any other right recognised by the GDPR to the data subjects.

*

The impact of privacy regulation in Europe has spread globally, influencing privacy and data protection discussions beyond European borders, marking a pivotal moment in the ongoing dialogue about digital rights and personal privacy.

China, as well, has demonstrated a heightened awareness of this matter, evidenced by the adoption of the Personal Information Protection Law ("PIPL")[37] in August 2021. This landmark national-level legislation comprehensively addresses issues related to the protection of personal information.[38] Bearing notable similarities to the European GDPR, the primary aim of the PIPL is to safeguard the rights and interests associated with personal information, govern the processing and utilisation of such data, and prohibits any infringement upon the personal information of the people in China.

The PIPL applies to organisations and individuals handling the processing of personal information[39] of individuals within the borders of the People's Republic of China and, under certain circumstances, to the processing of personal information occurring outside the PRC.

The principles governing the handling of personal information under China's PIPL closely mirror those of the GDPR. Processing must be lawful, sincere, and aligned with a clear and reasonable purpose, maintaining openness, transparency, and ensuring the quality of personal information. Processors bear responsibility for these activities, taking measures to safeguard personal information and providing adequate information about the processing.

Similar to the GDPR, China's PIPL establishes lawful bases for processing personal information. Processing is permissible with individual consent, to fulfil contractual obligations, meet statutory duties, respond to public health emergencies, protect life, health, and property in emergencies, process already-disclosed information, engage in news reporting, public opinion, or activities for public interests, or as specified by law.

The PIPL grants individual rights to be informed about the processing of their personal information, the right to limit or refuse processing, access a copy of their data, request

[37] The initial draft of the PIPL was submitted to the National People's Congress of China (NPC) on 13 October 2020. It was subsequently published and made available for public feedback on 21 October 2020. On 29 April 2021, the NPC released the second draft of the PIPL for public comments, with the commenting period extending until 28 May 2021. The final version was adopted on 20 August 2021, during the 30th Session of the Standing Committee of the 13th National People's Congress, officially coming into effect on 1 November 2021.

[38] In 2016, the People's Republic of China (PRC) introduced the Cybersecurity Law (CSL) with a focus on cybersecurity and safeguarding the Critical Information Infrastructure (CII) within the nation. Notably, it did not include specific provisions for the protection of individuals' personal information. In response to this gap, China enacted two laws in 2020: the Data Security Law (DSL) and, as mentioned, the PIPL.

[39] Under the PIPL, "personal information" is defined as any information related to identified or identifiable natural persons.

corrections, or seek deletion. Personal information handlers are mandated to take measures ensuring legal compliance, preventing unauthorised access, leaks, theft, distortion, or deletion of personal information.

However, despite this increasing sensitivity and concern for data protection, China remains committed to establishing an extensive government surveillance network, notably utilising drones for this purpose. Reports from the South China Morning Post indicate that Chinese military and government agencies have deployed bird-shaped drones for surveillance across at least five provinces.[40]

The integration of drone's technologies with an array of other advanced technologies, including facial recognition, artificial intelligence, smart glasses, and gait recognition systems will enable the collection and processing of an enormous amount of data and will strengthen and demonstrate the growing capabilities of what is arguably the world's most sophisticated surveillance system.

*

The virtuous influence of European privacy regulations also reverberated in the United States, thanks, in part, by the ongoing clashes and confrontations between European regulatory Authorities and major American corporations operating in the technology and digital sectors. These corporations are used to handle and process the personal data of their European users on servers located in the United States, albeit without the safeguards and protections mandated by the GDPR, which lacked (and still lacks) a direct equivalent in the United States.[41]

The underlying reasons for this substantial privacy regulation disparity can be attributed, foremost, to a fundamentally distinct conceptualisation of privacy and related rights within the legal systems of European matrix and those shaped by American influence.

Privacy in the United States is a nuanced and intricate concept shaped by a blend of legal, cultural, and technological influences. Although the term "privacy" is not explicitly articulated in the U.S. Constitution, the Fourth Amendment serves to shield citizens from

[40] These bird-like drones replicate the wing movements of actual birds through a set of crank-rockers powered by an electric motor. Each drone is equipped with a high-definition camera, a GPS antenna, a flight control system, and a data link featuring satellite communication capabilities.

[41] The transfer of personal data between the European Union and the United States continues to be based on a series of private agreements, through which U.S. companies undertake to comply with certain cardinal principles in the processing of European citizens' data. The first example of this was the so-called Safe Harbour of the early 2000s. This mechanism was invalidated in 2015 by the European Court of Justice in the famous Schrems I ruling as insufficiently protective. Shortly after this decision, the European Commission and the U.S. government began talking about a new structure, and in February 2016 they reached a political agreement that led a few months later to the adoption of the so-called Privacy Shield. However, even this agreement was soon declared invalid, in the ruling called Schrems II in 2020. Finally, in July 2023, the Commission adopted a new agreement on the transfer of EU-U.S. personal data, known as the Data Privacy Framework, a new set of rules that establishes a set of binding safeguards to limit access to data by U.S. intelligence authorities to what is necessary and proportionate to protect national security and for criminal law enforcement purposes. It is still too early to tell whether this new attempt can be considered more effective than previous agreements in establishing some sort of equivalence with the safeguards provided in European law.

unwarranted searches and seizures. This constitutional provision has been construed to encompass a right to privacy, particularly within one's residence.

Central to the American system is the notion of private autonomy, individual liberty, and the right to privacy within one's personal sphere, rooted in the original U.S. principle of "the right to be let alone". This right safeguards individuals from intrusions into their private realm by governments, corporations, and fellow citizens. It revolves around the entitlement to withhold access to one's data, body, or home.

While this concept of privacy remains closely tied to the cherished American principle of private property, it does not inherently include a right to data protection, as seen in the European context. In the U.S., privacy is primarily understood as the right to control access to one's information, distinguishing it from the European perspective that encompasses the right to exercise control over one's own data and information.[42]

In the United States, there is currently no federal legislation specifically addressing privacy or the protection of personal data. Nevertheless, the safeguarding of privacy is indirectly pursued through a range of consumer protection regulations. For instance, the Federal Trade Commission Act aims to shield consumers from unfair commercial practices, the Financial Services Modernisation Act provides protection in the financial services sector, and the CAN-SPAM Act regulates the collection and use of telephone numbers and email addresses for marketing purposes. Additionally, the Health Insurance Portability and Accountability Act (HIPAA) governs health information used by entities like hospitals, health insurance companies, pharmacies, and their data controllers. The recent enactment of Washington's My Health My Data Act (MHMDA) further contributes to health privacy regulations, imposing substantial compliance obligations on companies processing health data beyond HIPAA.

At the state level, several states, including California with the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), along with Virginia, Colorado, and Connecticut, have shown sensitivity to privacy concerns. Anticipated for 2024, a surge in state regulations is expected with the enactment of privacy laws in various states such as Iowa, Indiana, Montana, Tennessee, Texas, Oregon, Delaware, West Virginia, Rhode Island, and Missouri all of which worked on their privacy statutory frameworks in 2023 and in the beginning of 2024.

Within this diverse legal landscape, a federal law governing data protection in the use of drones is notably absent.[43] Privacy concerns related to UAS are presently addressed by state tort laws. These laws generally cover four privacy torts: intrusion upon seclusion,

[42] Veronica Gallo, Davide Mula, "USA, come sta cambiando l'approccio alla privacy: la grande svolta" (*Agenda Digitale*, 27 April 2021) <https://www.agendadigitale.eu/sicurezza/privacy/dal-diritto-alla-solitudine-alla-protezione-dei-dati-come-cambia-lapproccio-alla-privacy-negli-usa/> accessed 8 May 2024.

[43] Certain state legislatures, including those in Florida and Texas, have implemented laws specifically addressing privacy concerns related to drones. Furthermore, California has modified its anti-paparazzi legislation to establish a legal recourse for individuals. This amendment allows individuals to take legal action against anyone utilising a drone to capture images or recordings of someone involved in private, personal, or familial activity.

appropriation of name or likeness, public disclosure of private facts, and placing a person in a false light.[44] The development of drone-related privacy torts is likely to be influenced by the First and Fourth Amendment concept of a reasonable expectation of privacy, a test used to determine whether a "search" has occurred.[45] These principles may shape courts' perspectives on future privacy interests in the context of civil torts.[46]

In this context, we cannot fail to mention that Artificial Intelligence will undeniably play a pivotal role in shaping privacy regulations, both at the state and federal levels. While it introduces unique challenges distinct from general data privacy and cybersecurity concerns, a notable overlap exists between these domains.

Towards the close of 2023, the American Data Privacy and Protection Act (ADPPA), a proposed federal law designed to afford consumers fundamental privacy rights, demonstrated some advancement in the ongoing efforts to establish a comprehensive federal privacy law. Furthermore, broader legislative and regulatory initiatives related to AI, spurred by the Biden Administration's executive order on AI, may include components directly addressing data privacy issues. As a result, a closely intertwined relationship between advancements in AI and the data privacy landscape is foreseeable in the coming years.[47]

In fact, with the above-mentioned executive order, the United States has begun to outline a political and strategic position that allows for a diffusion and use of AI systems that is "responsible" in several respects. At the forefront among these considerations is data protection: the executive order envisages the adoption of a bipartisan law that, upholding the privacy-preserving model, provides for the development of methodologies that enable the training of AI models while protecting users' personal data.

The European Union took the lead over the United States in officially regulating Artificial Intelligence. The European Parliament's approval of the Proposal for a Regulation on Artificial Intelligence (**"AI Act"**)[48] on 13 March 2024, marked the EU as the global pioneer in overseeing this emerging technology. This legislative initiative signifies a

[44] Sean Valentine, 'Geophysical Trespass, Privacy, and Drones in Oil and Gas Exploration' (2019) 84(3) Journal of Air Law and Commerce 507. In this paper dedicated to examining the regulation of drones in the United States, particularly in the gas and oil sector, there are interesting references to privacy torts related to the use of drones. The author explains that privacy harms can be delineated into two distinct categories: subjective and objective. Subjective privacy harm pertains to the individual's perception of being subjected to unwarranted surveillance, irrespective of actual observation. Objective privacy harms encompass the adverse repercussions arising from the utilisation of an individual's private information against them. Intrusion upon seclusion actions largely protect against subjective privacy harm, whereas actions against publication of private affairs protect against objective privacy harm.

[45] Joshua Turner and others, 'Torts of the Future: Drones' (U.S. Chamber of Commerce Institute for Legal Reform, January 2022) <https://instituteforlegalreform.com/wp-content/uploads/2022/01/1323_ILR_Drones_Report_V7_Pages_Digital.pdf> accessed 8 May 2024.

[46] Rebecca L Scharf, 'Drone Invasion: Unmanned Aerial Vehicles and the Right to Privacy' (2019) 94(3) Indiana Law Journal 1065.

[47] Kirk J Nahra, Ali A Jessani, and Samuel Kane, '2024 Privacy Law Preview' (*WilmerHale Blog*, 16 January 2024) <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240116-2024-privacy-law-preview> accessed 8 May 2024.

[48] EU Artificial Intelligence Act proposal, European Parliament resolution P9_TA(2024)0138 <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf> accessed 8 May 2024.

ground-breaking effort to foster secure and reliable AI adoption within the EU single market. And it may not only represent a major step forward for Europe but also establish a potential global benchmark for AI regulation, similar to what happened with the GDPR.

The AI Act provides, first of all, a comprehensive definition of artificial intelligence systems, defined as "*machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*" (art. 3(1) of the AI Act).

Employing a "risk-based" approach, the AI Act categorises AI systems based on their risk levels. Obligations and responsibilities escalate in tandem with the assessed risk, applying not only to suppliers but also to users, importers, distributors, and everyone involved in utilising such systems.

A key focus of the regulation lies in safeguarding individuals' fundamental rights. Operators of high-risk AI systems are mandated to conduct fundamental rights impact assessments before deployment, thereby enhancing rights protection. Notably, the regulation prioritises copyright and privacy rights.

To achieve these objectives, the AI Act first enumerates prohibited AI practices and technologies (art. 5 of the AI Act). These include AI systems employing subliminal or manipulative techniques, exploiting vulnerabilities of certain subjects (eg minors or people with disabilities), automated social scoring systems, as well as predictive policing systems that consider the likelihood of a natural person committing a crime, solely on the basis of physical profiling or the assessment of personality traits and characteristics. The AI Act also prohibits emotion recognition systems in the workplace and in schools, social credit systems, biometric categorisation systems based on sensitive characteristics and systems that consent the indiscriminate extrapolation of facial images from the internet or from CCTV recordings to create facial recognition databases.

Privacy protection emerges as a paramount concern in this context, prompting institutions to redefine and expand the boundaries of the right to privacy and its protections through these new regulatory interventions that will also serve to fortify and extend protections for individuals' privacy rights.

*

It is also thanks to the development of these new technologies that the topic of privacy is finding greater fervour and fertile ground for the expansion of the relevant legislation. The interconnectedness of these technologies can contribute to greater clarity in the regulation of the implications on this fundamental right.

However, still today, despite the growing sensitivity surrounding data protection in the aforementioned jurisdictions and emerging industries, it has yet to secure the prominence it merits within the specific regulatory framework established for the responsible use of drones. As previously emphasised, while data protection regulations offer some guidance

in this domain,[49] they still prove non entirely sufficient in fully addressing the complex implications that drone usage can exert on the fundamental right to privacy.

## 5 Unsecured skies: cybersecurity implications in drone utilisation

While privacy concerns are commonly highlighted, it's important to recognise the inherent link between privacy and security. The collection of personal data and personally identifiable information by UASs can present challenges not only to individual privacy but also to both private and governmental security.

Indeed, the risk of cyber-attacks and hacking in using these technologies is very high, given their unencrypted communication through radio, Wi-Fi or GPS.[50] This can mean anything from illegal information processing to hijacking control over a drone's command and control system and using it for malicious, even criminal activities.

For example, a drone has the potential to engage in data theft from mobile phones, eavesdrop on phone conversations, or exploit Wi-Fi networks. The *modus operandi* is straightforward: the drone runs an application designed to deceive unsuspecting users' phones by posing as a legitimate access point. Consequently, a hacker can intercept and steal all data transmitted to and from the compromised cell phones.

This isn't merely a theoretical exploration of potential hacking risks: a London-based security firm named Sensepoint has successfully developed a software called Snoopy. When deployed on a drone, Snoopy enables the vehicle to pilfer data from mobile devices in its vicinity. In initial tests conducted on the streets of London, Snoopy managed to capture user credentials for PayPal, Amazon, and Yahoo, along with credit card numbers and location data of unsuspecting individuals simply by hovering above them. The software manipulates a victim's mobile device by tricking it into believing it's connecting to a trusted access point, subsequently gaining access to the handset's data.

Moreover, researchers conducted an analysis of drones produced by one of the leading and widely recognised manufacturers. By employing reverse engineering techniques, they revealed that the data transmitted to and from the drone lacked encryption. This vulnerability meant that the information was open to anyone, posing a substantial risk to the privacy of the drone operator.

[49] GDPR, for example, has certainly had an influence on the drone industry and its regulation. This is discussed in detail by Anna Konert, Marlena Sakowska Baryla, 'The Impact of the GDPR on the Unmanned Aircraft Sector' (2021) 46(4) Air and Space Law 517.

[50] The U.S. Department of Homeland Security (DHS) has repeatedly expressed its concerns about the vulnerability of civilian drones and the possibility that they could be hacked and used for illegal and malicious purposes.

And there is more. Drones have the potential for intentional sabotage, such as being deliberately crashed into unarmed populations or, more alarmingly, being hijacked for attacks on strategic targets.[51]

Security expert Samy Kamkar has developed software named SkyJack, capable of hacking all automated vehicles within its range once deployed on a drone. This allows the attacker to take control of these vehicles while in flight.

Numerous critical flaws were indeed identified in the firmware of some drones, enabling attackers to gain elevated privileges on the drones and their remote control and exploit the devices. These vulnerabilities ranged from denial of service to arbitrary code execution, where a threat actor could run commands on the targeted device. Furthermore, some of these vulnerabilities could be triggered remotely through the operator's smartphone, allowing the attacker to take over the phone and crash the drone mid-flight.

This level of access grants an attacker the ability to manipulate log data, alter the serial number, and effectively conceal their identity.

All of the above considered, the utilisation of drones for cyber espionage is therefore an increasingly plausible scenario. Given their high flexibility, these vehicles can effectively enable remote control over targets. A particularly intriguing application is the potential use of UASs to disrupt target communications.

Foreign governments and cyber terrorists may exploit this technology to launch attacks on a country and its critical infrastructure.

Consequently, major economic powers are heightening their security measures by imposing stringent restrictions on the import and export of such technologies.

As an illustration, the Department of Homeland Security (DHS) issued a warning against the use of drones manufactured by specific companies, mostly Chinese, citing safety concerns. Additionally, the U.S. Army has advised its units to cease the use of equipment from these same companies.

The prohibition of Chinese drones by the United States reflects mounting apprehensions regarding potential national security threats linked to the utilisation of such technologies. Emphasising concerns about data security and espionage, the ban underscores the intricate balance required between technological progress and the protection of sensitive information.

This restriction could significantly impact industries reliant on Chinese drone technology, prompting a demand for heightened scrutiny and a push for domestic

[51] Several incidents have been documented involving the malicious use of drones. In 2018, two small drones laden with explosives were detonated during President Maduro's outdoor speech, indicating a potential attempt to target the president and other government officials. In another incident in 2014, a drone operated by a film company crashed during an Australian triathlon, resulting in an injury to athlete Raji Ogden. The operator attributed the loss of control to deliberate interference with the wireless control link. According to the drone operator, an attacker executed a "channel hop" attack, gaining full control of the drone.

alternatives.[52] Moreover, this decision signifies a broader geopolitical tension, illuminating the intricate interplay between technological innovation, economic interests, and national security considerations in our interconnected world.

There is growing concern that the Chinese government actively engages in extensive data collection, with the United States being a primary target. Assessments from federal government intelligence and national security consistently highlight China's persistent and substantial cyber espionage threat, aiming to achieve economic advantages and enhance attack capabilities against critical infrastructure systems. China routinely focuses on corporate entities for economic espionage and intellectual property theft, considering every U.S. citizen a potential target for collection.[53]

The "*Worldwide Threat Assessment of the US Intelligence Community*"[54] underscores the tangible "*potential for Chinese intelligence and security services to utilise Chinese information technology firms as routine and systemic espionage platforms*". This assertion particularly points to China's 2017 National Intelligence Law, part of a series of laws designed to formalise and reinforce the state's extensive security activities.

Under the 2017 law and other components of China's domestic legal framework, the government can arguably compel Chinese businesses to cooperate with and provide access to intelligence and security services. The relationship between Chinese security services and the Chinese industry faces no substantial hindrance from legal limitations or privacy concerns.

In response to the ongoing commercial and technological rivalry with the United States, the Chinese New Regulation, effective from 1 January 2024, aimed at significantly restricting the usage of drones, particularly those manufactured abroad, within its borders. These measures, designed to enhance airspace control for security and safeguard national sovereignty, include prohibitions on the use of drones for collecting and disclosing state secrets or transferring information illegally from mainland China.

China intends to establish a national drone monitoring platform to meticulously record specifications, production details, and usage of drones within its territory, thereby protecting sensitive data from espionage or unauthorised disclosure.

[52] In 2018, the U.S. Defense Department initiated a programme aimed at fostering alternatives to small drones manufactured in China. This initiative supports non-Chinese companies recognised as reliable drone manufacturers by the Defence Innovation Unit (DIU), a branch of the Department of Defence dedicated to expediting the integration of commercial technology for national defence purposes.

[53] As FBI Director Christopher Wray has stated during July 7th, 2020 Hudson event titled China's Attempt to Influence U.S. Institutions: A Conversation with FBI Director Christopher Wray, regarding China's threat to national security, "*If you are an American adult, it is more likely than not that China has stolen your personal data*". The full transcript of the conversation can be found here <https://www.hudson.org/national-security-defense/transcript-the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states> accessed 8 May 2024.

[54] Daniel R Coats, 'Worldwide Threat Assessment of the US Intelligence Community, Statement For The Record' (Senate Select Committee on Intelligence, 29 January 2019 <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf> accessed 8 May 2024.

Furthermore, starting from September 2023, China has intensified its scrutiny of exports involving long-range civilian drones. Restrictions will be applied to drones surpassing visual operator range, having a flight duration exceeding thirty minutes, or weighing over 7 kilograms. Notably, the regulations outright forbid non-citizens and drones produced abroad from engaging in surveillance operations within Chinese territory.

China has clarified that these restrictions on unmanned drones aim to underscore its commitment to being a responsible global actor in implementing security initiatives and upholding world peace, as stated by the Ministry of Commerce. According to the department's clarification, these measures are not targeted at any specific country.

This development, however, unveils the flip side of the longstanding battle waged by the U.S. government against the use of Chinese drones, primarily within government agencies.

In summary, it is unequivocal that the issue of information security emerges as a highly sensitive concern, influencing strategic approaches and regulatory frameworks.

## 6 Conclusions

In the preceding sections, an initial effort was made to delineate the boundaries of data protection, cybersecurity, and the risks of cyberespionage associated with the deployment of drones. This perimeter, however, is poised to expand in tandem with the continuous growth and evolution of UAS technology.

While certain precautionary measures have been implemented both at the governmental and non-governmental levels in countries particularly attuned to the advancements in these emerging technologies, there remains a substantial distance to traverse in fortifying people and nations' defences.

In the forthcoming years, the utilisation of these technologies is anticipated to surge across diverse sectors. UAVs are poised to populate the skies extensively, demanding that security assumes the foremost priority to guarantee the safety and privacy of the populace.

This presents a formidable challenge, especially considering the escalating complexity of cyber threats. Consequently, it necessitates a collaborative effort involving manufacturers, industry stakeholders, security firms, governmental bodies, private enterprises, and, significantly, the general public.

Vigilance regarding the capabilities and risks associated with this technology is imperative, making it an essential responsibility for all stakeholders to collectively address the multifaceted challenges posed by the evolving landscape of drone technology.