Journal of Law, Market & Innovation

ISSUE 2/2024

Journal of Law, Market & Innovation

2/2024

Editors: ***Riccardo de Caria – Corrado Druetta – Cristina Poncibò - Andrea Santos López***

Journal of Law, Market & Innovation
Vol. 3 - Issue 2 - 2024
ISSN 2785-7867
Journal of Law, Market & Innovation

TABLE OF CONTENTS

Riccardo de Caria - Corrado Druetta - Cristina Poncibò - Andrea Santos López

FOREWORD TO ISSUE 2/2024

The present issue of the Journal of Law, Market & Innovation covers, with a comparative perspective, various topics surrounding the regulation of civil drones.

Like many other innovative items which become part of our everyday's life, drones as aircraft to be piloted remotely first appeared on the military field. Although the first experimental pilotless aerial vehicles started flying a century ago, unmanned aerial technology became more and more sophisticated in the last decades, thanks to the constant enhancement of telecommunications, electronic calculators and controllers and aircraft manufacturing.

As remote piloting improved, so did the range of possible professional usages of drones beyond the battlefield, eg the use of drones equipped with optical cameras found its way into professional photography and videomaking or large infrastructure inspections, while drones outfitted with sensors were increasingly deployed in vast agricultural fields or in security services. With the first wave of commercial drones, remote piloting technologies applied to drones proved to be very effective in making the aerial perspective a viable source of profit for many businesses.

In recent years, the market of highly performing commercial drones exploded, democratising their use for recreational purposes and paving the way to a new generation of *amateur* drone pilots. A few pioneer countries (notably the UK, but also US) stepped in with national amendments of air navigation codes, establishing the paramount importance of safe operation. Those attempts mainly addressed the registration of drones, basic requirements for certifications and pilot licences and mandatory insurance coverage, ie the entry requirements to ensure a more professional approach to drone piloting. However, the proliferation of unmanned flying objects in the sky brought forward also a new set of legal concerns. Any drone flying above the ground challenges the exclusive ownership of landlords and affects the privacy of citizens living below in a manner which is far more invasive than any other civil aircraft. This proximity to the victims led to an increasing number of casualties and intrusions, which have been and will be treated in the next future with traditional principles and remedies.

As the skies become increasingly populated with drones, a pressing social need arises for comprehensive regulatory frameworks addressing the liabilities associated with the use and misuse of drones. For once in the discourse surrounding the regulation of

innovative technologies, there is a broad consensus among legal scholars and practitioners on what a “drone” is (or is not). To the contrary, the possible application of traditional concepts, standards and remedies in tort law, which were presumably developed with traditional civil aircraft industry in mind, to commercial drone operators and manufacturers remains to be settled.

Moreover, the dynamic between ensuring the safe operation of drones and protecting human rights and other public interests has become pivotal in the evolving regulatory dialogue at national and supranational level, which is about to witness the rise of human transportation drones or AI-piloted ones, with foreseeable greater impacts. And, needless to say, the sky is not the limit anymore.

R.d.C., C.D., C.P., A.S.L.

Antonio Manganelli *

INNOVATION LETTER

THE INTERPLAY BETWEEN TELECOMMUNICATIONS OPERATORS AND DIGITAL PLATFORMS IN AN EVOLVING DIGITAL ECOSYSTEM

Abstract

Digital ecosystem comprises a composite array of complementary and substitutability relationships among its different actors, eg, telcos and very large digital platforms. Traditionally those actors have been regulated in different and separate fashion, and the evolution of their interactions disregarded. This asymmetric and uncoordinated regulation of different actors of the digital ecosystem has led to (unintentionally) generate market distortions or enhance situations of power unbalance. A new regulatory approach should focus on existing interdependences and trade-offs, in order to build a level regulatory playing field.

JEL CLASSIFICATION: K23, L51, L96, D25

SUMMARY

1 Digital transformation and asymmetric regulation

The digital ecosystem is nowadays a networked multi-layered structure, whose fundamental backbone is composed of very high capacity fixed and mobile communications physical infrastructures. Over this backbone, services, contents, applications, and their providers permeate the digital ecosystem with immaterial pervasive networks made of economic, social, and operational interactions (human and non-human). Within this ecosystem, digital platforms are crucial actors and from the perspective of telecom industry, they are also called Over-The-Top providers (OTTs), because they provide services to users via the public internet and telecoms infrastructures, but "over the top" of the traditional telecoms market value-chain.

* Professor of Antitrust and Regulation at the University of Rome, LUMSA.

DOI 10.13135/2785-7867/10737

Digital platforms have a broad scope of activities, eg, online advertising, marketplace services, internet search engines, social media, creative contents aggregations and distribution, video-sharing, communications services, products price comparison, application distribution, payment system services, collaborative activities, and so on. These digital services are often complementary yet sometimes substitutes to those provided by 'traditional' communication companies, telecom and broadcasting providers. This disruptive industrial and competitive transformations in the communications market have taken place in a context of extreme regulatory asymmetries.

These asymmetries started to be very partially and slowly addressed with a partial adaptation of the European Electronic Communications Code (EECC) and of the Audiovisual Media Service Directive (AVMSD).

In particular, in 2010, the first AVMSD[1] extended the scope of "Television without frontier" directive by including video-on-demand (non-linear) services with an editorial nature. However, only a few rules were extended symmetrically, while most involved a lighter touch, due to the higher degree of consumer control for on-demand services. The 2018 revision[2] further adapted the AVMSD to digital transformation, imposing a greater number of symmetric rules for on-demand services. Moreover, it also required video sharing platforms (previously completely excluded from the discipline) to adopt a few of the social regulation measures for the protection of minors, control of hate speech and compliance with the qualitative rules on advertising.

On the electronic communications side, the EU Electronic Communications Code (EECC)[3] introduced very few regulatory measures regarding platforms for the first time, categorizing communication services provided by digital platforms as electronic communication services (ECS), and, in particular, as Number-independent interpersonal communication services (NI-ICS). NI-ICS are subject to a light-touch regulation, e.g., OTTs are explicitly exempted from the general authorization regime and interoperability obligation is possible (yet never imposed) for NI-ICS under very specific and restrictive circumstances.

Nevertheless, very large online platforms (VLOPs) have been subject to very light touch (self-) regulation, which allowed few platforms to reach an unprecedented scale and scope of activities (enveloping users), becoming gatekeepers end-users and business users and acquiring an entrenched market and bargaining power.

[1] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) [2010] OJ L 95/1.

[2] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018] OJ L303/69.

[3] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L321/36.

Indeed, despite the recent adjustments of the regulation digital services and "traditional" communication services are based on an unlevel playing field: the electronic communications pro-competitive regulation has created highly competitive telecoms markets, also by blocking consolidation through a strict enforcement of merger regulation, whereas no obstacles (if not a slow and problematic application of competition law)[4] have impeded market monopolisation, consolidation, and envelopment strategies by VLOPs/Gatekeepers.

In this context, when VLOPs/Gatekeepers, on one side, and traditional communications and audio-visual media players, on the other side, provide substitute services and products, these regulatory and market asymmetries resulted in a clear direct competitive advantage for the digital players. This is the case, for example, of the tremendous increase in competition faced by broadcaster for advertising (by ads-based platforms) and audience markets (by online streamers and video-sharing platforms) as well as that suffered by telecom operators for their messaging services and voice calls (by online messaging and vocal calls platforms).

The recent approval of Digital Markets Act (DMA) and Digital Service Act (DSA)[5] has introduced a more stringent set of rules for very large online platforms (as defined by DSA) and gatekeepers (as defined by the DMA), yet these rules do not aim to create a pro-competitive pressure similar to what telecom operators are subject to, and do not discipline at all the various relationship between them.

2 Complementarity relationships and asymmetric regulation in the extended value chain

Further to the increasing substitutability, VLOPs/Gatekeepers have a fundamental complementary relationship with Telcos, as Telcos enable the distribution of their content and services to end-users, by deploying high-speed telecommunications infrastructures and providing internet access services.

The asymmetric regulatory approach between VLOPs/Gatekeepers and Telcos has had a profound impact also in their relationship as complements. Indeed, the complementarity relationship has been profoundly shaped by the Open Internet Regulation (OIR),[6] dividing the connectivity and digital ecosystem into Content and Application Providers (CAPs) and

[4] Which was finally considered not sufficient to address the contestability and fairness problems in digital markets, so to require an ex-ante regulatory framework (DMA).
[5] Respectively, Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.
[6] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union [2015] OJ L310/1.

Internet Service Providers (ISPs) and affirming a "net neutrality" concept. In short, the Net Neutrality regulation's objective is to reduce the material possibility of ISPs to exert market power trough non-price discrimination practices and therefore granting internet users rights to access and distribute contents through the internet.

Indeed, a "net neutrality" regime is conceived for a market context where (i) content distribution over internet is decentralised and based on a very high number of providers, none of which having an entrenched market power and/or (ii) ISPs can be (competitive) bottlenecks for CAPs to access end-users, which could be particularly problematic when there are vertically integrated actors, both as ISP and CAP.

As a matter of fact, nowadays digital markets and services are very concentrated and few CAPs (VLOPs/Gatekeepers) have significative and entrenched market power, supply "must-have" content/application. In such a situation, notwithstanding the 'termination bottleneck', ISPs cannot exert market power even in absence of non-discrimination rules. Indeed, due to the intense competition between ISPs for end-users, any lack of agreement with VLOPs/Gatekeepers, implying that ISPs cannot cater must-have content/applications to their subscribers, would be 'sanctioned' by end-users switching to another provider.

Moreover, in the EU most of ISPs are not vertically integrated as CAP. Indeed, no EU operators have developed a strong vertical integration between internet access and audio-visual content as in the US-Comcast merged with NBC-Universal in 2011 and with Sky in 2018, while AT&T merged with Time Warner in 2018. Moreover, in the US broadband and Internet access markets are very concentrated end-to-end, whereas most EU end-users can choose, due to the pro-competitive regulatory framework, from several internet access providers.

Therefore, in the EU, Net Neutrality's rules substantially address only discrimination issues between CAPs having different market and bargaining power, granting that none of them could induce ISPs to provide a more favourable treatment.

EU net neutrality rules therefore address possible discrimination issues between CAPs, limiting the influence of VLOPs/gatekeepers, by placing obligation (and opportunity cost) on ISP, thus again resulting in a very asymmetric and unbalanced set of rules.

As complementary products, VLOPs/gatekeeper's must-have contents can drive ISP connectivity demand. However, in this asymmetric regulatory setting, Telcos can neither (easily) increase end-users' price, because the electronic communications pro-competitive regulatory regime, nor monetize otherwise any increase in traffic demand vis à vis, VLOPs/gatekeeper's, because of Telco's negotiation and bargaining power being limited by the net neutrality rules.

3 Telcos' market financial crises and market failures (externalities)

This situation reflects very well the situation of economic and financial crisis in which EU telcos operate as they are subject to highly competitive pressure, public policy

objectives to build and deploy ubiquitous very high-capacity networks (fiber and 5G connectivity),[7] in order to provide users with innovative and higher quality services and contents, which imply an increase in network traffic that telcos are unable to monetise.

Opportunity costs derive from the impossibility (created by regulation) for ISPs to monetise an increase in traffic and demand, because of both the pro-competitive regulation, on one side, and above all the Net Neutrality regulation, eg, prohibition of zero rating,[8] on the other side.

These opportunity costs were blatantly evident in the market dynamics across the last decade, where a steep increase in data traffic resulted in revenue and price decrease for Telcos. Instead, VLOPs/Gatekeepers have been having high returns from traffic increase, and for this have no incentives to discipline and optimize their traffic, on the network perspective (ie, considering the costs that traffic generates), thus imposing economic negative externalities on ISPs.

Therefore, telcos highlighted the need for some mechanism to provide incentives for CAPs to efficiently dimension the data transmitted (internalise the negative externalities) and compensate the regulatory opportunity costs imposed on ISPs.[9]

Moreover, Telcos as well as The EU Commission stressed that "there is a correlation between the increased deployment of fixed and mobile broadband and economic development".[10] This implies that there is a great magnitude of positive externalities across the digital ecosystem. Under an economic perspective, this also represents the justification for direct public funding spending to augment private companies' investment capacity.[11]

Indeed, as positive externalities are pivotal and crucial in the economics of network deployment, it is important to assess the magnitude of those externalities and how they are distributed within the digital ecosystem. In other words, what subjects and companies

[7] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Connectivity for a Competitive Digital Single Market-Towards a European Gigabit Society (Burssels, COM(2016) 587 final), European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 2030 Digital Compass: the European way for the Digital Decade (Burssels, COM(2021) 118 final).

[8] Zero-rating is a commercial practice whereby an ISP does not subtract data usage associated with specific content or a class of content from a customer's data allowance. This means that the customer can access the zero-rated content without it counting towards their general data allowance. Initially this practice has been considered compatible, on a case-by-case basis, with net neutrality regulation (2020 BEREC net neutrality guidelines). Afterwards, in September 2021, the Court of Justice of the European Union (CJEU) issued three rulings that found certain zero-rating offers to be in breach of the requirement of equal treatment of traffic in Article 3(3) of the net neutrality rules. BEREC subsequently revised its Guidelines in June 2022 to reflect these rulings.

[9] Of course, those costs depend on the quantity of data that CAPS distribute through the Telcos network that also depends on their productive data-efficiency (ie, how much data is necessary to deliver a specific content). The more efficient are CAPs the lower the capacity needed to deliver the same amount of traffic and, therefore, the less significant the network investments needed to maintain quality. Likewise, the greater the capacity of the network resulting from network investments, the less efficient CAPs need to be in order to deliver the same quality.

[10] European Commission, 'How to master Europe's digital infrastructure needs?' (2024, White Paper, COM(2024) 81 final).

[11] As a matter of fact, in absence of positive externalities, an uncomplete deployment of new networks is the result of a well-functioning market which allocates resources where the companies' investment can be remunerated, and therefore it is a not a market failure.

are enjoying those externalities and whether and how those are otherwise contributing to those social benefits.

Under an efficiency point of view, those positive externalities could be tackled either (i) à la Coase, ie, reducing transaction costs and letting the parties within the ecosystem to bargain on rights' transactions or (ii) à la Pigou providing subsidies aimed at internalising those externalities and re-align social and private benefits.

Net neutrality rules create ineliminable transaction costs by qualifying as illicit certain transaction between telcos and CAPs, thus making it impossible to use a coesian solution. Therefore, de *iure condito*, subsidised are the only solution to address this issue. However, if those positive externalities are not evenly distributed across society but there are some players who enjoy a big portion of it, it would be fairer to have some mechanism channelling contributions from those parties and not necessarily entirely from public money.

In this contribution scheme should be also considered the complementarity features of digital services with the provision of electronic communication networks. Indeed, that's true that a complementarity between access and content weakens a "free riding" argument linked to positive externalities. However, access and content are not perfect complements. Namely, access and content are not consumed in "fixed proportions": consumers demand access for reasons other than consuming VLOPs/gatekeepers' content, and they may demand and consume more or less content without adjusting their demand for access. Moreover, it is not (anymore) relevant the access to the internet in itself yet rather the quality of access, and the overall demand for content increases in the quality of the network. Whereas the overall demand for access (and even its price) is not mainly driven by the quality. Access quality in turn depends on the network investments made by TELCOs, primarily, and CAPs, to a lesser extent. In other words, investment in network quality allow higher revenue for CAPS, yet not necessarily additional revenue for network operators.

So, this is not a pure free riding story yet one about an incomplete market, due to regulation, within which the externality created by network investment should be internalised. Therefore, a regulatory approach aimed at efficiently incentivising the ubiquitous deployment of networks should first define a "relevant ecosystem", where the markets and players who rely on the telecommunications high-speed networks and exploit the positive externalities are mandated to compulsory contribute to an investment fund.

This regulatory setting is, more or less, what current universal service obligations and universal service funds aim to do in the electronic communications framework, yet those rules only cover a universal provision of very basic service provision and impose contribution obligations only to telcos operators.

Therefore, the regulatory approach, on one side, should adapt to an advanced concept of universal service, focusing also on the upstream market (network deployment) and not

only on the downstream service provision, and, on the other side, should consider all the actors within digital ecosystem, especially very large online platforms/gatekeepers.

Finally, de *iure condendo*, the net neutrality regime should be softened and adapted to the current market situation, still granting end-users rights to receive and distribute all type of contents, yet giving ISPs more flexibility to differentiate their retail offers therefore getting back some countervailing bargaining power vis à vis very large online platforms/gatekeepers.

Aurelien Portuese *

SPECIAL SECTION

NAVIGATING THE SKIES OF REGULATION AND INNOVATION: THE CASE OF CIVIL DRONES

Abstract

The deployment of Unmanned Aerial Vehicles (UAVs), colloquially known as civil drones, necessitates an in-depth analysis of regulatory frameworks to understand their impact on market competition and technological innovation. This study presents a comparative examination of the regulatory landscapes governing UAV operations in the European Union (EU) and the United States (US), focusing on the interplay between legal provisions and market dynamics within the drone industry.

In the EU, the imminent introduction of UAV-based package delivery systems exemplifies a regulatory environment conducive to drone technology advancement. Governed by the European Union Aviation Safety Agency (EASA), the EU's regulatory structure is characterised by its coherence and integrative nature, fostering a regulatory milieu that balances safety and privacy concerns with the promotion of technological development. The uniform regulatory guidelines across EU Member States serve as a catalyst for innovation, providing clarity and stability for UAV operators and manufacturers, thereby enhancing competitive dynamics within the market.

Conversely, the US regulatory context, as illustrated by the legal confrontation between SZ DJI Technology Co. Ltd. and Autel Robotics USA LLC, highlights a multifaceted and litigious approach. Central to this is the role of the Federal Aviation Administration (FAA) in navigating the intricate interplay between antitrust litigation and competitive practices in the UAV sector. The US framework's reactive nature, often mired in judicial proceedings, introduces a degree of uncertainty and complexity for industry stakeholders, potentially impeding technological innovation and market diversification.

The juxtaposition of the EU and US regulatory frameworks unveils contrasting methodologies in governing civil drone operations. The EU's unified and innovation-centric approach markedly diverges from the litigious and segmented regulatory landscape in the US. These disparities exert considerable influence on the UAV industry, shaping the contours of market competition, technological advancement, and regulatory industry equilibrium.

The disparate regulatory paradigms in the EU and US present distinct challenges and opportunities in the realm of UAV operations. The EU's streamlined and proactive regulatory approach encourages innovation and market growth; while the US's intricate and adversarial regulatory environment poses substantial

* Research Professor and Founding Director of the GW Competition & Innovation Lab at The George Washington University; Special Editor of the Antitrust Law Journal.

DOI 10.13135/2785-7867/10738

hurdles for industry stakeholders. This comparative analysis is vital for policymakers, legal experts, and industry participants in navigating the complex and evolving domain of UAV technology and its regulatory governance.

JEL CLASSIFICATION: L40

SUMMARY

1 Introduction: the market dynamics of competition for civil drones

The market for drones well illustrates the complex relationship between regulation and innovation.[1] While aerial activities remain one of the most regulated sectors of the economy in most countries, drones and the inherent innovations they bring about remain relatively less regulated, thereby allowing for innovation competition between market actors scattered all over the world.[2] However, the fine balance to be found between regulation and innovation in the development of drone technology, especially related with AI-embedded drones, will determine the competition in a nascent, yet rapidly growing, market[3]. Malicious use of civil drones force enforcers to have a "wake-up call" and force

[1] See, for instance, Steve Calandrillo, Jason Oh and Ari Webb, 'Deadly Drones? Why FAA Regulations Miss the Mark on Drone Safety' (2020) 23(1) Stanford Technology Law Review, 182; Timothy M Ravich, 'Grounding Innovation: How Ex-Ante Prohibitions and Ex-Post Allowances Impede Commercial Drone Use' (2018) 2 Columbia Business Law Review 495 (advocating for 'permissionless innovation' to civil drone regulations); Jake Nelson and Tim Gorichanaz, 'Trusts as an Ethical Value in Emerging Technology Governance: The Case of Drone Regulation' (2019) 59 Technology in Society; Abderahman Rejeb, Karim Rejeb, Steven J Simske and Horst Treiblmaier, 'Drones for Supply Chain Management and Logistics: A Review and Research Agenda' (2023) 26(6) International Journal of Logistics: Research and Applications 708 (reviewing the burgeoning literature on civil drones).

[2] See, more generally, Joseph Awange and John Kiema, *Environmental Geoinformatics: Extreme Hydro-Climatic and Food Security Challenges: Exploiting the Big Data* (2nd edn, Springer International Publishing 2019) 265, 289; Jackie Alkobi, 'The Evolution of Drones: From Military to Hobby & Commercial' (*Percepto*, 15 January 2019) <https://percepto.co/the-evolution-of-drones-from-military-to-hobby-commercial/> accessed 20 May 2024.; Larisa Kapustina and others, 'The Global Drone Market: Main Development Trends' (2021) 129 SHS Web of Conferences; David Streitfeld, 'Look, Up in the Sky! It's a Can of Soup!' *The New York Times* (New York, 4 November 2023) mentioning that "Amazon said last month that drone deliveries would expand to Britain, Italy and another, unidentified U.S. city by the end of 2024"; Eleonora Bassi, 'From Here to 2023: Civil Drones Operations and the Setting of New Legal Rules for the European Single Sky' (2020) 100 Journal of Intelligent & Robotic Systems 493.

[3] Whether the regulatory framework strikes a reasonable and correct balance is highly debated with opposite conclusion. See, for instance Patrick F Hubbard, "'Sophisticated Robots': Balancing Liability, Regulation, and Innovation" (2014) 66(5) Florida Law Review 1803 (arguing that "the legal system's method of addressing physical injury from robotic machines that interact closely with humans provides an appropriate balance of innovation and liability for personal injury"). On the other hand, see Lavi M Ben Dor and Jonathan M Hoffman, 'The Emerging Airspace Economy: A Framework for Airspace Rights in the Age of Drones' [2022] Wisconsin Law Review 953 (concluding that "With the inevitable integration of drone delivery services and commercial UAS into society, our current legal and regulatory framework is ill-prepared for the opportunities and challenges that lie ahead."); Sara M Smyth, 'Keep Calm but Don't Carry on: New Drone Regulations in the United States' (2021) 25(2) Journal of Law, Information and Science 49.

legislature to change in regulations.[4] In that regard, the regulation of drone competition is and should be of interest to antitrust authorities, alongside other regulatory authorities focused on safety, privacy, and AI regulation.

Drones, often hailed as the pinnacle of contemporary technology, owe their lineage to an invention that dates to the waning days of 1783. It was then that the Montgolfier brothers, Joseph-Michel and Jacques-Étienne, pioneers hailing from France, embarked on a ground-breaking endeavour. They successfully launched the first unpiloted aerial device, a hot-air balloon, marking a significant milestone in the annals of aviation.[5] This early experiment laid the foundational stone for the development of unmanned flight, illustrating a remarkable journey from the simplicity of buoyant air to the complexity of today's sophisticated drones. This historical context enriches our understanding of drones, not merely as modern marvels but as a culmination of human curiosity and innovation that spans centuries. Thanks to considerable technological developments, drones are increasingly ubiquitous. Drone "invasion"[6] is unavoidable: drone ownership and use have been on the rise, with registrations for recreational and commercial operators topping one million in the United States in 2018.[7] Civil drones are used for unlimited number of purposes, including recreational purposes (ie photography), shopping delivery purposes,[8]

[4] For instance, the US Congress passed the Protecting Emerging Threats Act of 2018 as codified in the FAA Reauthorization Act of 2018—that gives certain federal agencies, namely the DHS and the DOJ, important new authority to detect, identify, monitor, and track drones without prior consent; to warn the operator of a drone, including by passive or active and direct or indirect physical, electronic, radio, and electronic means; to disrupt or seize control of a potentially threatening drone; to seize or otherwise confiscate the drone; and if necessary to use reasonable force to damage or destroy a threatening drone. See US Department of Justice, Drones: A Report on the Use of Drones by Public Safety Agencies – and a Wake-up Call about the Threat of Malicious Drone Attacks, COPS, Police Executive Research Forum (2020) <https://portal.cops.usdoj.gov/resourcecenter/RIC/Publications/cops-w0894-pub.pdf> accessed 21 May 2024. See also Colin T Ross and Kevin M Jinks, 'DOJ and Drones: Protection, Policy, and Enforcement' (2021) 69(3) Department of Justice Journal of Federal Law and Practice 278, 288 ("Drones present tremendous potential for commerce, public safety, and transportation, yet this technology is no different than others in that it comes with unique challenges").

[5] Paula Hohrova, Jakub Soviar, and Wlodzimierz Sroka, 'Market Analysis of Drones for Civil Use' (2023) 14(1) Scientific Journal on Transport and Logistics 55.

[6] Amanda Graham, Haylee Kutzli, Teresa C Kulig, and Francis T Cullen, "Invasion of Drones: A New Frontier for Victimization" (2021) 42(3) Deviant Behavior 386, 403 ("To protect privacy rights, federal and state legislative approaches provide insight into how law enforcement drones can be regulated." and exploring "the extent to which the public is being victimized by recreational drones (eg, spied on, followed, privacy invaded)").

[7] US Department of Transportation, FAA Drone Registry Tops One Million, January 10, 2018, <https://www.transportation.gov/briefing-room/faa-drone-registry-tops-one-million#:~:text=The%201%2C000%2C000%20total%20registration%20figure,drones%2C%20which%20are%20individually%20registered> accessed 21 May 2024.

[8] Azamat Seidakhmetov and Omid Fatahi-Valilai, 'Drone based Delivery System: Restrictions and Limitations' in Wolfgang Kersten, Carlos Jahn, Thorsten Blecker, and Christian M Ringle (eds), *Changing Tides* (Epubli 2022) (citing Amazon as one of the most successful e-commerce business and leading the way to drone delivery with Amazon Prime Air); Jean-Philippe Aurambout, Konstantinos Gkoumas, and Biagio Ciuffo, 'Last mile delivery by drones: an estimation of viable market potential and access to citizens across European cities' (2019) 11(30) European Transport Research Review 1; Khalid Aljohani and Russell G Thompson, 'An Examination of Last Mile Delivery Practices of Freight Carriers Servicing Business Receivers in Inner-City Areas' (2020) 12 Sustainability MDPI 1; Capgemini Research Institute, 'The Last-mile delivery challenge', Research Institute Report (2019) <https://www.capgemini.com/wp-content/uploads/2019/01/Report-Digital-%E2%80%93-Last-Mile-Delivery-Challenge1.pdf> accessed 21 May 2024 (considering Amazon as "a pioneer in this space" of last-mile delivery).

or agricultural purposes.[9] Consumer increasingly perceive the usefulness of drone delivery for their shopping experience, and decreasingly perceive privacy risks related with drone delivery such as proposed by Amazon Prime Air who pioneered the sector.[10]

But not all drones are created equal. Drones are either UAVs (*Unmanned Aerial Vehicle Systems*) or UCAVs (*Unmanned Combat Aerial Vehicle Systems*).[11] While the former are commonly referred as "civil drones," the latter partake to military drones. I will focus on this article exclusively on the market dynamics and regulatory implications, from a comparative approach to the US and EU, on the civil drones – or UAVs. Before delving into this comparative approach, it is critical to grasp the market dynamics of civil drones. For, the market for civil drones is characterised by unique features which illustrate the complex relationship between innovation, regulation, and other concerns such as national security, but also shed lights for any antitrust analysis of such market.

Within the civil drone category, many sub-categories can apply such as recreational drones versus commercial drones, or fixed-wing drones versus propeller drones. I shall take civil drone as a single category without further categorisation.[12] For, taken as a whole, the market for civil drone makers is highly asymmetric. For, one company – the Chinese drone maker DJI – accounts for 76% of the entire market. The other companies are Intel (4%), Yuneec (2%), and Parrot (2%):

[9] Francisco Klauser and Dennis Pauschinger, 'Entrepreneurs of the Air: Sprayer Drones as Mediators of Volumetric Agriculture' (2021) 84 Journal of Rural Studies 55 (citing the European Commission that portrayed agriculture 'one of the primary sectors expected to see sharp uptake of drone technology in the near future' and citing the US-based Association for Unmanned Vehicle Systems International expects 80% of the future drone market to relate to agriculture.) See also Steve Calandrillo, Jason Oh, and Ari Webb, 'Deadly Drones? Why FAA Regulations Miss the Mark on Drone Safety' (2020) 23 Stanford Technology Law Review 182, who outline the use case of civil drones in commercial applications (journalism, construction, insurance), entertainment, real estate, tourism, rescue, medical delivery, scientific research, animal conservation, law enforcement, and recreational drone use.

[10] Steven Leon, Charlie Chen, and Aaron Ratcliffe, 'Consumers' Perceptions of Last Mile Drone Delivery' (2023) 26(3) International Journal of Logistics: Research and Applications 345 (finding "consumer acceptance of delivery by drone increases if they perceive drone delivery to be useful and if they trust the service provider."). See also Wonsang Yoo, Eun Yu, and Jaemin Jung, 'Drone Delivery: Factors affecting the public's attitude and intention to adopt' (2018) 35(6) Telematics and Informatics 1687.

[11] See *Dassault Aviation / Tsa / Thales* (Case COMP/M.5426) Commission Decision 2009/C81/03 [2009] *OJC81/2*.

[12] Paula Hohrova, Jakub Soviar, and Wlodzimierz Sroka (n 5) ("*Classification based on use can be divided into recreational drones and commercial drones […]*" and noting that civil drones "*can be divided into 4 categories: drones with fixed wings, multi-propeller drones, single-propeller helicopters, and hybrid helicopter*").

TOP 10 DRONE MANUFACTURERS' MARKET SHARES IN THE US

Rank	Manufacturer[1]	HQ Location	Founding Date	US Market Share[2]
1	dji	Shenzhen, China	2006	76,1%
2	intel	Santa Clara, USA	1968	4,1% (+0,4%)
3	YUNEEC	Hong Kong, China	1999	2,6% (-0,5%)
4	Parrot	Paris, France	1994	2,5% (+0,3%)
5	3DR	Berkeley, USA	2009	0,6% (-0,8%)
6	AUTEL ROBOTICS	Bothell, USA	2014	0,6% (-0,2%)
7	Skydio	Redwood City, USA	2014	0.3% (+0,1%)
8	senseFly	Lausanne, Switzerland	2009	0,2% (-0,1%)
9	kespry	Menlo Park, USA	2013	0,1% (-0,2%)
10	AeroVironment	Simi Valley, USA	1971	0,1% (-)

Source: Drone Industry Insights, March 2021[13]

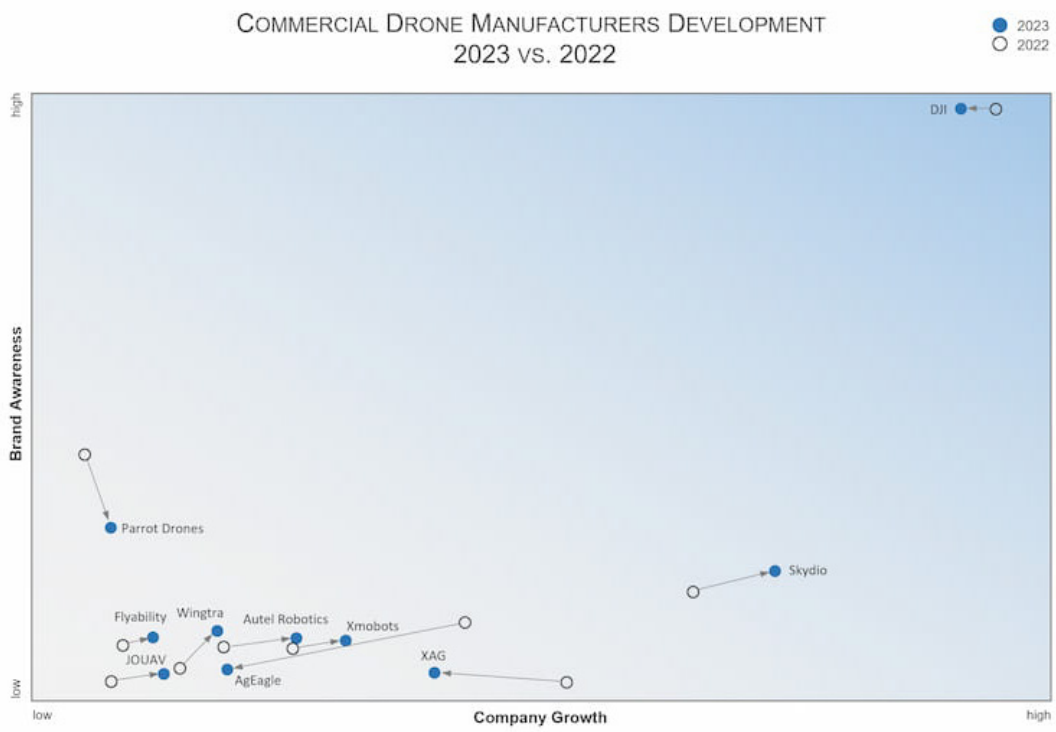
The supremacy of DJI is unparalleled, with a global market leadership that put its competitors to shame. This dominance is further reinforced by the fact that DJI is the only drone company in the world, together with MMC another Chinese drone manufacturer, of "*fully designing and producing major industrial chains, including aircraft, power supply, flight control, video transmission and ground control*".[14] In assessing the civil drones' relative market shares, Hohrova and others conclude that DJI's super-dominant position is uncontested:

"SZ DJI Technology Co., Ltd. ("DJI") had a dominant position due to its market share of 76.8% [32]. The value of its relative market share is more than 20 times higher than the closest competitor, Intel Corporation. Thus, DJI's leadership is clearly visible and the remaining 5 included competitors are at the very tail, reaching values not exceeding 0.05".[15]

In the US, DJI Sciences and Technologies Ltd ("DJI) has 90% of the US's consumer drone market, 70% of the industrial drone market, and 92% of the first responder market.[16] Not

[13] Lukas Schroth, 'Drone Market Shares in the USA after China-US Disputes' (Drone Industry Insights, 2 March 2021) <https://droneii.com/drone-market-shares-usa-after-china-usa-disputes> accessed 21 May 2024
[14] Larisa Kapustina and others (n 2) 3.
[15] Paula Hohrova, Jakub Soviar, and Wlodzimierz Sroka (n 5).
[16] Eric Sayers and Klon Kitchen, 'DJI isn't the only Chinese drone threat to US security. Meet Autel' (DefenseNews, 15 September 2023) <https://www.defensenews.com/opinion/2023/09/15/dji-isnt-the-only-chinese-drone-threat-to-us-security-meet-autel/> accessed 21 May 2024. See also Association for Uncrewed Vehicle Systems International,

only is DJI the most famous and popular drone brand, but it also is the highest-growth company in the sector:



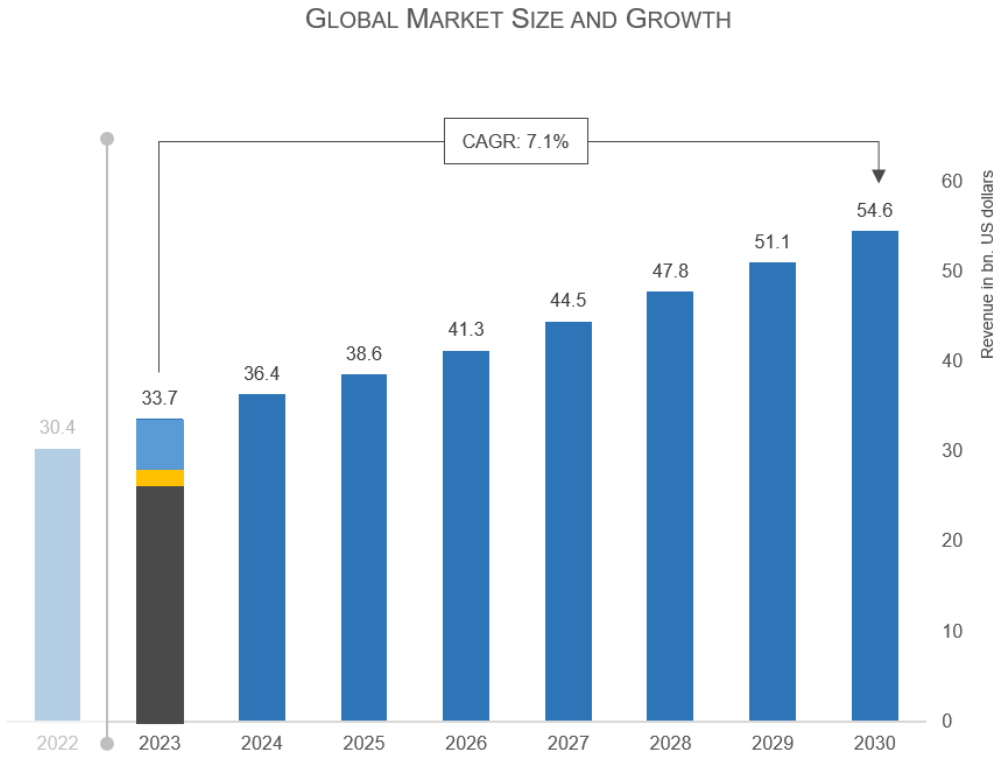
Source: Drone Industry Insights, November 2023[17]

This market structure asymmetry is even more relevant because of the dynamism of the market.[18] For, the market is growing fast, hence amplifying the need for vigorous competition in the market, otherwise entrenched market positions may prove difficult to disrupt incumbents for the benefit of dynamic competition and innovation:

"Whitepaper: AUVSI Partnership for Drone Competitiveness, 18 January 2024, <https://www.auvsi.org/sites/default/files/AUVSI-Partnership-for-Drone-Competitiveness-White-Paper.pdf> accessed 21 May 2024.

[17] Ed Alvarado, Ranking the Leading Drone Manufacturers (Drone Industry Insights, 28 November 2023) <https://droneii.com/ranking-the-leading-drone-manufacturers> accessed 21 May 2024.

[18] Paula Hohrova, Jakub Soviar and Wlodzimierz Sroka (n 5) - noting that "Drones have caught on in the market due to their advantage of operating virtually anywhere, allowing them to reach inaccessible terrain or health-threatening areas."



Source: Drone Industry Insights, 3 August 2023[19]

Mass produced in Asia,[20] the civil drone market epitomises not only the imbalance toward one market actor – DJI – but more structurally toward one region for production – China. This dual dependency generates both antitrust concerns and national security concerns. This reliance is further intensified by the fact that the United States market leads the world in drone sales, accounting for 30% of civil drone purchases, significantly surpassing China, which ranks second in sales with 8% of global drone purchases.[21] Surprisingly, both categories of concerns have remained so far timid, if not inexistent.

[19] Esteban Zanelli and Hendrik Boedecker, Global Drone Market Report 2023-2030 (Drone Industry Insights Report July 2023) <https://droneii.com/product/drone-market-report> accessed 21 May 2024.
[20] Paula Hohrova, Jakub Soviar and Wlodzimierz Sroka (n 5) 61, 62 ("Mass production in Asia using standardized parts and procedures is very likely to contribute to the further spread of this technology. We can conclude that these are attractive products."). See also Larisa Kapustina and others (n 2) 4 *("The main manufacturers of both unmanned aerial vehicles and their components are China, France and, to a lesser extent, America, while the software and service development industry is developed in Europe").*
[21] Larisa Kapustina and others (n 2) 5 (largest markets for demand of civil drones are USA (31%), China (9%), Russia (8%), Great Britain (6%), Australia, France, Saudi Arabia, India and South Korea.)

Regarding delivery drones, some speculate that 2024 will be a "breakout year"[22] with leading companies such as Amazon (who expects 500 million drone deliveries by the end of the decade), Zipline and Alphabet's Wing having obtained the necessary regulatory approvals. And the market structure of delivery drones differs from the one portrayed in civil drone makers. For, when it comes to drone delivery service providers, the market looks more fragmented and balanced:

Source: Drone Industry Insights, October 2023[23]

The regulation of civil drones predominantly take place in the US via ex-post litigation whereas Europe characteristically favors ex-ante precautionary regulations. I study each approach successively, before providing a comparative assessment.

2 US antitrust cases in drones: regulation through litigation

Antitrust laws in both the United States and the European Union aim to promote competition and prevent abusive monopolistic practices. However, their application to the drone industry reflects the unique regulatory and market dynamics within each region. This analysis explores how antitrust laws apply to the drone industry in the US and EU, drawing on specific cases and regulatory proposals.

[22] Joann Muller, "2024 will be a breakout year for delivery drones" (Axios, 2 January 2024) <https://www.*axios*.com/2024/01/02/delivery-drones-2024-amazon-zipline-wing> (announcing among other introductions, Amazon's introduction of a "smaller, quieter delivery drone, which will be fully integrated into Amazon's delivery network this year").
[23] El Alvarado, Drone Services: The Top Companies in 2023 (Drone Industry Insights, 24 October 2023) <https://droneii.com/top-drone-service-companies-in-2023> accessed 21 May 2024.

Initially, the US experienced years of an ex-ante ban on civil drones.[24] This unfortunate ban stifled drone innovation.[25] The FAA Modernization and Reform Act of 2012[26] (FMRA) directed the FAA to produce a comprehensive set of regulations to "safely accelerate the integration of civil unmanned aircraft systems into the national airspace system". Section 336 of the FMRA for "model aircraft ... flown strictly for hobby or recreational use". Following this regulatory change, the FAA "imposed stringent permitting requirements on would-be commercial UAV operators […]."[27] But, the FAA's "ex-ante, one-size-fits-all ban on commercial drones was ineffective and sometimes flouted"[28]– a change was necessary to provide for legal clarity and technological innovation by mass adoption. In 2018, the adoption of Part 107 of the relevant regulations laid down the principles for ex-ante permissions subject to ex-post enforcement.[29] Such approach not only allows for broader scope for technological innovation without regulatory overreach, but also is more consistent with a Common law, evolutionary approach that characterise antitrust enforcement. Nevertheless, criticisms persist as the new rules allegedly stifle innovation still.[30] This is certainly demonstrated by the fact that Amazon has to test its drone outside the US due to regulatory obstacles inside the US.[31]

More generally, the Federal Aviation Administration (FAA) oversees drone regulations with a focus on safety and integration into the national airspace. Privacy concerns related to drones are addressed through a more fragmented approach, with significant involvement from state legislatures. The FAA has been cautious in regulating privacy broadly, leaving room for states to experiment with regulations that balance First Amendment rights and privacy concerns.[32] The US approach to drone regulation – beside a traditional antitrust enforcement that has its limits as discussed above – remains focused

[24] Timothy M Ravich, 'Grounding Innovation: How Ex-Ante Prohibitions and Ex-Post Allowances Impede Commercial Drone Use' (2018) 2 Columbia Business Law Review 495, 531.
[25] Mehbook Jeelani, Is the FAA limiting drone innovation? (Fortune, 28 August 2014) <https://*fortune*.com/2014/08/28/faa-limiting-drone-innovation/> accessed 21 May 2024.
[26] See, FAA Modernization and Reform Act of 2012, Pub. L. 112- 95, § 332(a)(1), 126 Stat. 11 (2012).
[27] Timothy M Ravich (n 24) 528.
[28] ibid 531.
[29] Small Unmanned Aircraft Systems, 14 C.F.R. pt. 107 (2018).
[30] Steve Calandrillo, Jason Oh, and Ari Webb, 'Deadly Drones? Why FAA Regulations Miss the Mark on Drone Safety' (2020) 23 Stanford Technology Law Review 182.
[31] Amazon Says It May Take Drone Testing Outside U.S. (*BBC*, 9 December 2014) <https://perma.cc/KS45-839F> accessed 21 May 2024; Jack Nicas, Amazon Says FAA Approval To Test Delivery Drones Already Obsolete (*WALL STREER JOURNAL*, 24 March 2015) <https://perma.cc/85LY-ZQRF> accessed 21 May 2024; UAS Test Sites (*FED. AVIATION ADMIN.*, 23 October 2018) <https://perma.cc/V24B-L45K> accessed 21 May 2024. See also Steve Calandrillo, Jason Oh, and Ari Webb (n 30) 235 ("Without regulatory flexibility from the FAA, major American companies (eg, Google and Amazon) are investing in drone technology outside the United States' borders. […] The United States cannot reap these benefits until the FAA removes its line-of-sight regulation.")
[32] Dasom Lee, David J Hess, and Michiel A Heldeweg, "Safety and privacy regulations for unmanned aerial vehicles: A multiple comparative analysis" (2022) 71 Technology in Society 1.

on safety over privacy concerns. Indeed, "Congress has not been as productive in the field and has yet to address privacy, focusing instead on safety".[33]

2.1 Ex-post regulation of civil drones: an evolutionary antitrust approach

Antitrust enforcement of ex-ante permissions subject to ex-post enforcement is best illustrated with the DJI case whereby the super-dominant Chinese company was challenged for allegedly having competed unfairly by using predatory pricing. The drone industry in the US has seen its share of antitrust scrutiny, as evidenced by the legal battle between DJI, the market leader, and Autel, a competitor. Interestingly, both drone makers – DJI and Autel – are "threats to US security".[34]

Autel accused DJI of predatory pricing and monopolising the market on prosumer drones, violating both federal and state antitrust laws. However, a federal judge in Delaware dismissed Autel's counterclaims, stating that Autel had failed to provide sufficient evidence that DJI sold drones below cost in a predatory manner. DJI filed a lawsuit on 11 August 2016, against Autel for patent infringement related to drone technology.

In response, Autel filed antitrust counterclaims on 23 May 2018 against DJI, counterclaiming for monopolisation in violation of the Sherman Act, attempted monopolisation in violation of the Sherman Act, predatory pricing in violation of sections 17043 and 17044 of the California Unfair Practices Act, and predatory pricing in violation of section 481-3 of the Hawaii Unfair Practices Act. Autel described its antitrust counterclaims as focused on the "prosumer" drone market, defined as products that are advanced beyond mere toys yet not as complex as fully equipped professional models. These drones are highlighted for their user-friendly design and are equipped with professional-grade features, such as enhanced cameras, sophisticated navigation software, and increased smart capabilities. Autel claimed that DJI engaged in predatory pricing strategies to maintain and extend its market dominance by selling drones below cost to undercut competitors and drive them out of the market. Autel argued that DJI's practices harmed competition by preventing new and potentially better drones from entering the market, citing instances where DJI lowered its prices below cost in response to new competitive threats. Autel contended that DJI has significantly dominated this segment's growth, thereby bolstering its monopoly influence in the industry. Arguably, Judge Stark sums up Autel's predatory pricing claims as:

[33] Jacob Montgomery, 'Protecting Reasonable Expectation of Privacy in an Age of Drones: A Framework for Balancing Privacy Interests with the Utility of Drones in Law Enforcement' (2023) Gonzaga Law Review 485, 517 (advocating that "Any approach taken must balance the interests of law enforcement to apply drones with the individual's interest in privacy. A system capable of balancing these interests would recognize the expectation of privacy that existed before the introduction of drones into the national airspace and legislate to protect those privacy interests covered explicitly by the Fourth Amendment.")

[34] Eric Sayers and Klon Kitchen (n 16).

"DJI has repeatedly engaged in predatory pricing to blunt the advance of new competitors and ultimately drive them out of the prosumer drone market entirely or, at a minimum, to its fringes." "[N]early a dozen companies have attempted to bring new and better 'prosumer' drones to American consumers . . . [b]ut each time DJI has perceived a new threat, DJI has used its dominant market share to maintain and extend its monopoly by predatorily cutting its prices, below cost, to undercut the advent of the competitor drone." "[There is] a continuing pattern of DJI's anti-competitive conduct," whereby DJI tactically lowers its price below cost to drive out each new competitor that enters."[35]

In response, DJI contended that its success in the drone market was due to its significant investments in research and development, as well as its efficient manufacturing capabilities. DJI disputed having monopoly power, pointing out that multiple companies had entered the market with competitive pricing. Also, DJI argued that Autel's allegations of predatory pricing were speculative and not based on concrete evidence of below-cost pricing. DJI highlighted that Autel did not provide specifics on the prices DJI charged or demonstrate that those prices were below DJI's costs.

On the 18 March 2019,[36] Judge Leonard P Stark of the United States District Court for the District of Delaware delivered a judgment dismissing the accusations against DJI. The judge first outlined the legal framework for predatory pricing under the Sherman Act, requiring proof that prices were below an appropriate measure of costs and that there was a reasonable prospect of recouping investments in below-cost prices. The ruling favoured DJI, who, despite being the plaintiffs in the initial lawsuit, found themselves defending against antitrust counterclaims brought forth by Autel. Judge Stark considered that Autel's allegations were insufficient to plausibly support a claim of predatory pricing. Specifically, Autel failed to demonstrate that DJI's pricing was below cost. The legal standard for proving predatory pricing was not met.[37]

The court noted that Autel's calculations, based on dividing DJI's revenue by the quantity sold to determine monthly prices, were speculative and did not accurately reflect DJI's actual pricing strategies. Judge Leonard P Stark dismissed Autel's antitrust counterclaims, ruling in favour of DJI. The court emphasised the importance of not chilling competitive conduct that the antitrust laws are designed to protect, underscoring that competitive price cutting is often the essence of competition. Overall, Judge Stark found "robust competition" rather than "unfair competition":

[35] *SZ DJI Tech. Co. v. Autel Robotics, [2019] USDC Del, 3.*
[36] ibid
[37] See, for instances, *Brooke Grp. Ltd. v. Brown & Williamson Tobacco Corp., [1993] USSC 44, 509 U.S. 209, 222-24 (United States Supreme Court, 1993);* see also *Broadcom Corp. v. Qualcomm Inc.*, 501 F.3d 297, 317 (3d Cir. 2007). See also *Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 594 (United States Supreme Court, 1986)* 106 S. Ct. 1348, 89 L. Ed. 2d 538 (1986) where the Supreme Court warned that ""[C]utting prices in order to increase business often is the very essence of competition. Thus, mistaken inferences in cases such as this one are especially costly, because they chill the very conduct the antitrust laws are designed to protect."

"[A]ll of the facts alleged in the Counterclaim (as opposed to Autel's conclusory assertions) are fully consistent with robust competition in a growing market, including allegedly declining prices, increasing output, product innovation, and repeated new entry. Because there is no plausibly alleged anticompetitive conduct, Autel cannot satisfy the requirements for stating a predatory pricing claim under federal or state antitrust law".[38]

The court's decision hinged on the inability of Autel to convincingly argue that DJI had engaged in predatory pricing tactics. Specifically, the allegations fell short as Autel did not manage to adequately demonstrate that DJI's pricing strategies resulted in prices being set below cost—a critical element required establishing a claim of predatory pricing. Judge Stark's dismissal of the allegations underscores the high evidentiary bar required to prove such antitrust claims, marking a clear victory for DJI in this legal battle over competitive practices in the drone market.

The *SZ DJI Technology Co. Ltd. v. Autel Robotics USA LLC* case shows antitrust laws' limits: the judicial rationale highlights several reasons why antitrust mechanisms were inadequate in this case. First, Autel's claims of predatory pricing were rejected by the court due to a lack of evidence that DJI sold its drones below their production costs, a key antitrust requirement. The court's insistence on exact and detailed evidence of pricing below the cost shows that plaintiffs in antitrust cases have a high burden of proof, making it difficult for competitors to challenge dominant firms' bold or unfair pricing strategies.

Second, the court's reasoning shows an understanding of the prosumer drone market's constant change and competition. DJI's success is due to their pricing strategies, large R&D team, and efficient manufacturing processes. These factors suggest that antitrust laws may not cover situations where a company's dominant position is due to inherent competitive advantages and innovation rather than anticompetitive behaviour. Antitrust laws require not only pricing below cost but also the intent to eliminate competition and a chance of recovering losses. Autel's claims failed to prove that DJI's pricing strategy intentionally damaged competition and that DJI could recover its losses, the court ruled. Creating predatory pricing and using antitrust laws to limit market dominance are difficult.

Third, the court advised against incorrect conclusions that discourage competition. It stressed that courts prefer to let competitive market forces play out rather than enforce antitrust laws. This cautious approach to antitrust enforcement reflects concerns about overregulation hindering innovation and competition. Overall, the case shows the challenges of using antitrust law to address market control concerns, especially in fast-changing, innovation-driven markets like prosumer drones. Rivals seeking to challenge dominant market participants through antitrust litigation may face challenges due to the

[38] *SZ DJI Tech. Co. v. Autel Robotics (n 35)* 10.

courts' strict criteria for anticompetitive conduct and their focus on market dynamics and innovation.

2.2 Implications: benefits and limits of antitrust

One of the advantages of using antitrust enforcement as an ex-post regulation of civil drones is that it provides sufficient room for technological innovation to take place, as well as the opportunity for interventions to take place on a limited number of highly targeted matters and subjects. In fact, the default rule in antitrust law continues to be that innovations and market actors' strategies are permitted, unless ex-post antitrust interventions provide a different outcome.

In addition to the primary limitations of antitrust, which include the requirement that anticompetitive behaviour be supported by evidence, antitrust is unable to effectively sanction predatory pricing and is unable to effectively incorporate concerns regarding national security. The case of DJI exemplifies both limitations in a particularly severe and compelling manner.

The national security concerns regarding DJI, and more generally Chinese drone makers, are real. It is said that "the Pentagon is worried that DJI shares data with the Chinese government –the same claim the U.S. government makes about Huawei and one DJI denies".[39] China-based technology companies ought to turn over, by law and on demand, data they have collected through their business operations, to the Chinese government.[40]

To address this problem of a super-dominant company controlling the drone market while generating national security risks through data-sharing with the Chinese Communist Party requires change of policies and regulations[41] – something that antitrust cannot address at all. This took place in 2020 when Congress prohibited the Department of Defense from purchasing drones made by Chinese companies.[42] Also, in 2020, the Department of Justice banned the use of agency grants for purchasing Chinese drones due to national security concerns.[43]

[39] Lara Seligman, "Pentagon Seeks to Counter China's Drone Edge" (*Foreign Policy*, 27 August 2019) <https://foreignpolicy.com/2019/08/27/pentagon-seeks-to-counter-chinas-drone-edge/> accessed 21 May 2024.
[40] Jim Magill, 'Controversy Surrounding Data Security of Chinese-made Drone Sparks Intense Debate' (DroneLife, 1 March 2024) <https://dronelife.com/2024/03/01/controversy-surrounding-data-security-of-chinese-made-drones-sparks-intense-debate/> accessed 22 May 2024.
[41] ibid. (the U.S. government also needs to update policies and regulations governing sales and operations of drones across the country.")
[42] Section 848, Fiscal Year 2020 National Defense Authorization Act (NDAA) <https://www.congress.gov/bill/116th-congress/senate-bill/1790/text> accessed 22 May 2024.
[43] See Department of Justice, Policy on Funding Unmanned Aircraft Systems, 5 October 2020, <https://www.ojp.gov/sites/g/files/xyckuh241/files/media/document/ojporderfundingdrones.pdf> accessed 22 May 2024.

Nevertheless, the purchase of drones from Chinese makers for the consumer market remains untouched despite data leakage risks. Not only DJI's dominance threatens US's national security but it also undermines leadership in aviation sector:

"The U.S. must recognize that, in addition to national security concerns, China's subsidized drone market is harming the U.S. workforce, and ultimately our standing as the global leader in aviation. Drones are already playing an important role in the economy, and that role will continue to grow as drones become indispensable tools used for industrial inspection, lifesaving operations by first responders, and the delivery of products and services. Drones are also critically important to U.S. leadership in a new era of aviation defined by uncrewed and autonomous systems".[44]

The absence of actions for the drone consumer market is striking due to the fact that, in October 2022, the Department of Defense identified DJI as a "Chinese military company" operating in the US[45]. In 2023, President Biden signed the National Defense Authorization Act of 2024 which contained restrictive provisions originally proposed in the American Security Drone Act (ASDA) of 2023 which restricts government agencies from the use of drones manufactured in China.[46]

Antitrust actions cannot remedy or address the DJI's market dominance and its related national security issues because these data matters mostly remain outside the reach of antitrust. Hence, outside military regulation and public procurement or public funding rules, the regulation of civil drones in the US is primarily limited to antitrust actions which are highly limited themselves. This is in contrast with the European approach which embraces on more proactive approach to regulatory interventions on the civil drone market, through both competition law actions and ex-ante regulations.

3 EU regulation of civil drones: regulation through precaution

The European Union's approach to antitrust enforcement in the drone industry is part of its broader regulatory framework for digital and emerging technologies. The EU has proposed rules making it easier for individuals and companies to sue makers of drones, robots, and other AI-enabled products for compensation for harm caused by these technologies. This AI Liability Directive aims to address the increasing use of AI-enabled products and services and the patchwork of national rules across the EU. While not an

[44] Association for Uncrewed Vehicle Systems International, Whitepaper: AUVSI Partnership for Drone Competitiveness, 18 January 2024 <https://www.auvsi.org/sites/default/files/AUVSI-Partnership-for-Drone-Competitiveness-White-Paper.pdf> para 8 accessed 22 May 2024.

[45] Section 1260H of the Fiscal Year 2021 NDAA <https://www.defense.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/> accessed 22 May 2024.

[46] White House, 'Statement from President Joe Biden on H.R. 2670, National Defense Authorization Act for Fiscal Year 2024' (22 December 2023). See S. 473, American Security Drone Act of 2023, 118th Congress. Some pending bills would ban DJI from operating on US communications infrastructure by adding the company to the Federal Communications Commissions' Covered List of prohibited companies. See H.R., Countering CCP Drones Act, 118th Congress (2023).

antitrust regulation per se, this directive reflects the EU's proactive stance on regulating the digital economy, including the drone industry, to ensure consumer protection and fair competition.

3.1 Ex-ante regulation of civil drones: a precautionary approach

Interestingly, in the European Union, there is not a single case regarding the regulation of drones, let alone civil drones.[47] However, there are several merger decisions involving drone technology.[48]

The EU refers to drone regulation as part of the "U-space" regulation for "Unmanned" aircrafts[49]. The EU's "Drone Strategy 2.0", unveiled in November 2022, envisions drones playing a significant role in infrastructure, emergency services, and transportation, such as delivering medicines and serving as air taxis.[50] The EU drone market is expected to achieve a value of €14.5 billion and generate 145,000 employment opportunities by the year 2030.[51] The strategy outlines 19 specific operational, technical, and financial measures to create a favourable legal and commercial environment for drone operations[52]. The strategy promotes the use of standardised scenarios that are advantageous for both civil and military purposes and suggests a unified approach by the European Union in terms of drone technology and certification standards. This comprehensive strategy aligns with the current EU legal framework and the U-Space

[47] Indeed, the only cases cursively mention "*drones*" as part of asylum or foreign policy matters. See, comprehensively, Case C-901/19 *CF and DN v Bundesrepublik Deutschland* [2022] ECLI:EU:C:2021:472. The case deals with the question of whether secondary protection against a genuine risk of suffering serious harm can be contingent upon a minimum number of civilian fatalities and injuries in the nation of origin, and mentioning "*misguided US drone attack*" (para.19); Case *T-182/21 Kurdistan Workers' Party (PKK) v Council of the European Union* [2022] ECLI:EU:T:2022:807, regarding the EU's classification of the PKK as a terrorist group after a drone attack in Iraq.

[48] *Dassault Aviation / TSA / Thales* (Case Comp/M.5426) Commission Decision C(2009) 1947 [2009] *Matra / Aerospatiale* (Case IV/M.1309) Commission Decision IV/M.1309 [1999] *EADS* (Case Comp/M.1745) Commission Decision Comp/M.1745 [2000] *Sagem / Snecma* (Case Comp/M.3621) Commission Decision C(2004) 5084 [2004] *EADS / STA / Elbe Flugzeugwerke JV* (Case Comp/M.6554) Commission Decision C(2012) 6355 [2012] *Safran / MBDA / Compagnie Industrielle Des Lasers Cilas* (Case M.10640) Commission Decision C(2022) 7405 [2022] *EADS / Astrium* (Case Comp/M.2924) Commission Decision Comp/M.2924 [2002] *EADS / Astrium (II)* (Case Comp/M.3156) Commission Decision Comp/M.3156 [2003] *Thales / DCN* (Case Comp/M.4191) Commission Decision C(2007) 563 [2007] *Safran / Zodiac Aerospace* (Case M.8425) Commission Decision C(2017) 8782 [2017] *EADS / Israel Aerospace Industries / JV* (Case Comp/M.6490) Commission Decision C(2012) 4977 [2012] *MBDA / Bayern-Chemie* (Case Comp/M.4653) Commission Decision C(2007) 3776 [2007] *Faurecia / Michelin / Symbio / JV* (Case M.9474) Commission Decision C(2019) 8382 [2019] *Qualcomm / NXP Semiconductors* (Case M.8306) Commission Decision C(2018) 438 [2018] *Parker / Meggitt* (Case M.10506) Commission Decision C(2022) 2287 [2022] *Harris Corporation / L3 Technologies* (Case M.9234) Commission Decision C(2019) 4634 [2019]*UTC / Rockwell Collins* (Case M.8658) Commission Decision C(2018) 3052 [2018].

[49] Commission Implementing Regulation (EU) 2019/347 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft [2019] OJ L152/45 (categorising drone operations into 'open', 'specific', and 'certified' categories, each with varying levels of regulatory requirements based on the risk they pose and stipulating that existing national certificates for drone operators and remote pilots must be recognized until they are harmonized with EU standards by July 2021.)

[50] European Commission, 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe' COM (2022) 652 final, 29 November 2022.

[51] ibid.

[52] ibid.

Package,[53] with the goal of streamlining regulations and encouraging the widespread and responsible use of drones.[54]

On 26 January 2023, the European Commission (EC) has for example introduced new rules on dedicated airspace for drones.[55] The Implementing Regulation of 22 April 2021, on a regulatory framework for the U-space provides, beyond safety objectives, some provisions regarding data use and sharing. For instance, a 'common information service' for the purpose of the Regulation is defined as a "service consisting in the dissemination of static and dynamic data to enable the provision of U-space services for the management of traffic of unmanned aircraft".[56] The providers of common information service of each U-space ought to comply "with the necessary data quality, latency and protection requirements" established in the Regulation's Annex, according to Article 5.4(b) of the Regulation. Such Annex details the data quality requirements which include, among others, the need for the service providers to ensure that "the transfer of data is subject to a suitable authentication process such that recipients are able to confirm that the data or information has been transmitted by an authorised source".[57] In addition, service providers are required to "implement security policies, including data encryption and protection of critical data", "identify, assess, and mitigate, as necessary, the security risks and vulnerabilities" and to "adhere to security standards and regulations regarding where data can be stored and ensure that third-party providers agree to follow security practices".[58] This emphasis on risks, vulnerabilities, and requirements for a high data quality differs ensures that security risks related to data transfers to foreign powers are minimised.

This type of ex-ante regulation seems to better apprehend the complexity and diversity of threats and vulnerabilities associated with drones, especially when AI-embedded technology underpins such drones.[59]

[53] Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space [2021] OJ L139/161; Commission Implementing Regulation (EU) 2021/665 of 22 April 2021 amending Regulation (EU) 2017/373 as regards requirements for providers of air traffic management/air navigation services and other air traffic management network functions in the U-space airspace designated in controlled airspace [2021] OJ L139/184 as regards requirements for providers of air traffic management/air navigation services and other air traffic management network functions in the U-space airspace designated in controlled airspace, L 139/184, April 23, 2021; Commission Implementing Regulation (EU) 2021/666 of 22 April 2021 amending Regulation (EU) No 923/2012 as regards requirements for manned aviation operating in U-space airspace [2021] OJ L139/187as regards requirements for manned aviation operating in U-space airspace, L 139/187, April 23, 2021.

[54] See also European Commission, "A Drone Strategy 2.0 for Europe," Ref. Ares (2021)3664195, June 3, 2021.

[55] European Commission, 'New EU Rules on Dedicated Airspace for Drones Enter into Force' (26 January 2023).

[56] Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space [2021] OJ L139/161, art 2(4).

[57] Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space [2021] OJ L139/161, Annex III.A.4.

[58] Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space [2021] OJ L139/161, Annex III.B.4.

[59] See, for discussion, Ozmen Mustafa Meliksah, Aksoy Bekir, "An Example Application for An Identification of Friend and Foe (IFF) System Appropriate for Unmanned Aerial Vehicles (UAV) Based on Deep Learning" (2023) 107(3) Journal of

3.2 The privacy emphasis: constant and relevant

The European approach to drone regulation is characterised by two main aspects. First, drone regulation fits within the European Sky Strategy which is a strategy aimed at achieving a "European Single Sky" as part of the existential achievement of the European Single Market.[60] The removal of barriers to trade, the minimisation of the European market fragmentation as general principles of European regulation apply to drone regulation.

Second, in contrast to the conventional focus on the physical safety aspects of aerial activities, the European model expands the scope to encompass concerns about security and privacy.[61] Considering the global civil drone market's significant Chinese manufacturer dominance, this expanded perspective is imperative. This dominance, which is justified by the integration of military and civilian drone technologies, brings up relevant concerns about data exploitation and threats to national security. The GDPR requires that any activity involving the processing of personal data must guarantee transparency, limitation of purpose, minimal data usage, accuracy, integrity, and confidentiality. Unregulated drones, which are frequently equipped with cameras, sensors, and other data-gathering devices, have the potential to violate individual privacy rights.

One crucial element of GDPR compliance for drone operations is the necessity of conducting Data Protection Impact Assessments (DPIAs) in cases where there is a significant threat to individual privacy. Data Protection Impact Assessments (DPIAs) aid in the identification and mitigation of risks linked to data processing activities. Drone operations have the potential to collect substantial amounts of unauthorized personal data through video recordings and other surveillance activities, making this issue of utmost importance.

Drones filming in areas where individuals have a reasonable expectation of privacy in the European Union must adhere to the regulations set forth by the GDPR. Although GDPR provides extensive coverage, it poses various challenges for the implementation of drone technology. Initially, the regulation can be perceived as an obstacle that hinders the wider acceptance and implementation of drone technology in fields such as agriculture, emergency services, and urban planning, where the gathering of extensive data is crucial. The need to comply with regulations can result in higher operational expenses and intricacy, which may hinder the progress of innovation and technological development. Furthermore, the diverse interpretations of GDPR among EU member states can result in inconsistencies in the implementation and adherence to enforcement and compliance obligations. This not only adds complexity to the regulatory environment for drone operators but also impedes the progress of establishing a cohesive market for drone technologies across Europe.

Intelligent & Robotic Systems 36; Mateusz Osiecki, Agnieszka Fortonska, Matylda Berus, Marta Wlodarczyk, "Drone as a Target of Terrorist Attack and a Weapon Against Terrorism – Analysis in the Light of International Law" (2022) 106(6) Journal of Intelligent & Robotics System.

[60] Eleonora Bassi (n 2) 493.

[61] EU privacy rules predominantly remain dictated by the "GDPR", 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 L119/1.

Although GDPR imposes restrictions on the utilisation of drones, it also stimulates advancements in technologies that protect privacy. For example, the focus on 'privacy by design' promotes the development of drones by manufacturers that aim to reduce data collection or anonymize data to prevent identification. Geofencing technologies improve compliance by preventing drones from entering restricted areas, thereby reducing the likelihood of privacy violations. The implementation of GDPR has stimulated advancements in secure methods of transmitting and storing data, guaranteeing that the information collected by drones is safeguarded against unauthorised access and breaches. These advancements not only comply with GDPR regulations but also improve the overall security and effectiveness of drone operations.

The EU faces a dynamic challenge in maintaining a balance between innovation and strict compliance with privacy regulations. As the advancement of drone technology progresses, it is necessary to update the regulatory frameworks that govern its usage. These frameworks should promote innovation while also safeguarding individual privacy rights. Hence, the European approach to regulation tackles the possibility of privacy infringement and unapproved data collection in addition to reducing the physical risks associated with drones, such as collisions or mechanical failures. Drones with sophisticated sensors and cameras have the potential to gather substantial amounts of data, which raises concerns about potential misuse and privacy violations. It may even make it easier to obtain sensitive information without authorisation.

Furthermore, the technological similarities between military and civilian drones highlight the possible threats to national security, such as the potential for civilian drones to be modified for use in the military or the leakage of cutting-edge technology that could jeopardise national security. In that context, the promotion of a "large-scale European drone market" promotes technological sovereignty and minimise reliance on external suppliers.[62] Such market is envisioned as part of the "European Drone Strategy 2.0" which aims at "setting out possible ways to guide the further development of this technology and its regulatory and commercial environment".[63]

Europe is safeguarding its citizens against threats to national security and privacy, in addition to preventing immediate harm, by incorporating security and privacy considerations into drone regulations. Interestingly, characteristic to the precautionary approach, the EU has approached drone regulation is not the result of a harmonisation process from national rules to the European level but, instead, a proactive action from the European institutions to regulate in absence of national rules:

"Developing Union rules for drones has been all the more important as there were very few regulatory national frameworks in place in the EU Member States, or at the global level. Unlike in other sectors, where the EU regulatory harmonisation process started after the adoption at national level of sometimes diverging regulation, here, it has been

[62] European Commission, "Drone Strategy 2.0: Creating a large-scale European drone market" (29 November 2022) <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7076> accessed 22 May 2024.

[63] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe' COM/2022/652, 29 November 2022.

possible to start from the outset with a truly common set of rules. This continues to present a unique opportunity not to be missed"[64].

Embracing a "forward-looking vision for the future holistic development" of the drone market,[65] the EU has updated drone rules to boost the commercial drone market while planning measures against malicious use. These regulatory updates, although primarily focused on safety and security, indirectly influence market competition by setting standards that all drone manufacturers and operators must meet.

4 Conclusion: a comparative analysis

The application of antitrust laws to the drone industry in the US and EU reflects broader differences in regulatory philosophies between the two regions. The US legal battle between DJI and Autel demonstrates the challenges of applying traditional antitrust laws to a high-tech industry characterised by rapid innovation and global competition. In contrast, the EU's regulatory proposals, including the AI Liability Directive, indicate a more proactive approach to addressing the complexities of the digital economy, including potential antitrust issues, through comprehensive legislation. Both regions recognise the importance of fostering competition and innovation in the drone industry while ensuring consumer protection and national security. However, the mechanisms and focus of their regulatory efforts differ, with the US emphasising legal enforcement of antitrust laws and the EU adopting a more holistic regulatory approach that includes aspects of competition, consumer protection, and liability.

From a comparative perspective, safety is a more significant concern than privacy for UAV regulations.66 In that regard, the US approach best resemble the overall global approach. More generally, the EU and US drone regulation approaches greatly impact market competition, technological advancement, and regulatory industry equilibrium. These differences help explain how legal frameworks can promote or hinder technological advancement and market dynamics in civil drones.

Technology development and market entry are safe in the EU due to its harmonised and precautionary regulatory framework. EASA-regulated EU regulations promote consistency and lower market entry barriers, fostering competition and innovation. The coherent regulatory landscape across EU Member States allows UAV manufacturers to scale operations without having to navigate regional laws, improving competitive dynamics and market innovation.

However, the US regulatory environment is more fragmented and litigious, as shown by the SZ DJI Technology Co. Ltd. and Autel Robotics USA LLC case. The reactive US framework prioritises safety over privacy, which can lead to judicial proceedings that

[64] COM/2022/652, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe', 29 November 2022, para 6.
[65] ibid para 17.
[66] Dasom Lee, David J Hess, Michiel A Heldeweg (n 32).

create uncertainty and slow technological and market change. This may hinder drone industry innovation and new entrants.

EU regulations like the GDPR's strict privacy and data protection requirements for drone operations spur privacy-enhancing technology innovation. Drones must have geofencing to comply with privacy laws, pushing the industry to develop privacy-conscious technology. In contrast, the US emphasis on safety and integration into the national airspace has led to advanced detect-and-avoid systems to reduce drone flight risks. The US's piecemeal privacy approach through state legislatures creates a heterogeneous regulatory landscape that could stymie unified technological advancements. For, the United States has a more fragmented approach to privacy concerning drones, with significant involvement from state legislatures. The FAA has been reluctant to regulate privacy broadly, leaving room for states to experiment with drone regulations that address privacy concern. This results in a patchwork of state laws that may offer varying degrees of privacy protection, potentially leading to inconsistencies and challenges for interstate drone operations.

Which regulatory approach is more conducive to innovation gains and increased consumer welfare? The more evolutionary approach adopted in the US may seem to give more prospect for trial-and-error approach which is inherent to the innovation process. In contrast, the regulatory standards preventively adopted in the EU may deter innovation and incentivize drone makers to shift production in laxer regulatory environments. Policymakers can use these methods to combine the strengths of both regulatory approaches:

1. *Harmonisation of Regulations*: The US could benefit from harmonising drone privacy regulations like the EU's GDPR to reduce interstate regulatory burdens and create a more consistent market environment;

2. *Balanced Regulatory Frameworks*: Both regions should prioritise safety, privacy, and innovation. Like the US, the EU could consider more flexible frameworks that allow technological experimentation to spur innovation while protecting fundamental rights;

3. *Stakeholder Engagement*: Drone manufacturers, operators, and civil society must be engaged continuously. This engagement can help make regulations practical and promote innovation and competition;

4. *International Collaboration*: EU-US collaboration on standards and best practices could improve global standards, lower international market entry barriers, and set a global drone safety and privacy benchmark;

5. *Drone market competition*: Policymakers can ensure drone regulations support robust market competition and safe, privacy-respecting, and innovative drone technology use by addressing these recommendations. The drone industry is changing everything from package delivery to emergency services, so this balanced approach is essential.

In conclusion, as the drone industry continues to evolve, both the US and EU may need to adapt their antitrust and regulatory frameworks to address new challenges and ensure a competitive and innovative market landscape. The regulatory approaches to civil drones by the United States and the European Union reflect their distinct legal, cultural, and operational perspectives, leading to various implications for drone manufacturers, operators, and the broader society. These differences impact areas such as privacy, safety, market access, and innovation within the drone industry.

Andrea Parziale[*]

SPECIAL SECTION

DRONE USERS' AND LANDOWNERS' RIGHTS IN ITALY AND THE NETHERLANDS: THE MEDICAL USE OF DRONES

Abstract

Background. Drones are increasingly integrated into recreational and economic activities, including for medical uses. In this scenario, drones carrying medical equipment or patients may fly over someone else's property. This raises the question of how conflicts between drone users and landowners arising from the medical use of drones are resolved. This question predominantly revolves around the vertical extension of property rights.

Aim and methodology. This article offers a comparative study of how these conflicts are tackled in Italy and the Netherlands, exploring the different operational solutions offered by their respective legal frameworks. In particular, the aim of the article is two-fold. First, the article intends to assess to which extent the Italian and Dutch operational solutions differ or converge, based on insights from the legislative, judicial, and doctrinal legal formants. Secondly, based on this comparative analysis, the article makes use of socio-economic considerations to assess the potential impact of the reconstructed Italian and Dutch operational solutions on the advancement of drone medical uses.

Conclusions: The article argues that the current legal framework fails both to facilitate the use of drones, also for medical emergencies, and to protect landowners' rights. A clear-cut height above which drones can fly (and under which drones cannot fly) can provide more clarity over the respective spheres of interest of the parties concerned.

JEL CLASSIFICATION: I18, K10, K11, K13

SUMMARY

[*] Ph.D. Assistant Professor of Health Law, Department of Health, Ethics and Society, Faculty of Health, Medicine and Life Sciences, Maastricht University. Email: andrea.parziale@maastrichtuniversity.nl.

DOI 10.13135/2785-7867/10739

1 Introduction

The present article considers, from a comparative and socio-economic perspective, the role and limitation of property law in medical uses of drones (or unmanned aerial systems, UASs),[1] focusing on the Italian and Dutch legal systems and putting forth a proposal to regulate more clearly potential conflicts of interests between drone users and landowners.

The use of drones is becoming increasingly widespread in the recreational and economic activities of private individuals, with market forecasts generally optimistic in assessing the growth potential of the sector.[2] The delivery of medical products and patients is among the disparate use cases where the deployment of drones has been considered.[3] Indeed, the use of drones for medical purposes offers several advantages. These include rapid emergency response[4] and the possibility of reaching places (permanently or temporarily) inaccessible through more traditional means of transport.[5] In the context of epidemics caused by infectious diseases, the use of drones can also help minimize infection risks by limiting interpersonal contact.[6]

While drones are not yet widely employed in medical emergencies and in the transportation of medical equipment and patients, initiatives are underway in several European countries to facilitate the medical use of UASs. For instance, the Netherlands set up a nationwide experimental network of medical delivery drones in 2023.[7] Similar, albeit more local, initiatives have been launched in Italy.[8] The development and consolidation of such initiatives can benefit from a discussion of the legal and regulatory enablers and obstacles to using drones for professional or commercial purposes.

[1] Thus, the paper does not cover manned systems such as eVTLOs (electric vertical take-off and landing), popularly known as flying cars or air taxis.

[2] Esteban Zanelli and Hendrik Boedecker, Global Drone Market Report 2023-2030 (Drone Industry Insights Report July 2023).

[3] James C Rosser and others, 'Surgical and Medical Applications of Drones: A Comprehensive Review' (2018) 22(3) Journal of the Society of Laparoendoscopic & Robotic Surgeons; Sara De Silvestri and others, 'Challenges for the Routine Application of Drones in Healthcare: A Scoping Review' (2023) 7(12) Drones 685. Regarding the transport of patients, see EHang Sets Up Aerial Emergency Channels to Help Fight Coronavirus in Guangdong, China <https://www.ehang.com/news/778.html> accessed 20 May 2024.

[4] Anna M Johnson and others, 'Impact of Using Drones in Emergency Medicine: What Does the Future Hold?' (2021) 13 Open Access Emergency Medicine 487; Christian Wankmüller, Maximilian Kunovjanek, and Sebastian Mayrgündter, 'Drones in emergency response – evidence from cross-border, multi-disciplinary usability tests' (2021) 65 International Journal of Disaster Risk Reduction 102567.

[5] Jalel Euchi, 'Do drones have a realistic place in a pandemic fight for delivering medical supplies in healthcare systems problems?' (2021) 34(2) Chinese Journal of Aeronautics 182.

[6] Esthera Justyna Król-Całkowska and Daniel Walczak, 'The Use of Drones in the Area of Minimizing Health Risk during the COVID-19 Epidemic' (2022) 106(40) Journal of Intelligent & Robotic Systems.

[7] 'The path to a nationwide network of medical delivery drones' (15 October 2023) <https://www.amsterdamdroneweek.com/news/use-cases-and-solutions/the-path-to-a-nationwide-network-of-medical-delivery-drones> accessed 11 March 2024.

[8] Eg, in Lombardy, Alessandro di Stefano, 'Trasporto di organi, sangue e medicinali. Le startup della drone economy decollano anche per la sanità' <https://startupitalia.eu/startup/trasporto-di-organi-sangue-e-medicinali-le-startup-della-drone-economy-decollano-anche-per-la-sanita/> accessed 11 March 2024; in Tuscany, 'Sangue ed emoderivati. Il trasporto anche via drone' <https://www.quotidianosanita.it/toscana/articolo.php?articolo_id=110885> accessed 11 March 2024.

In recent years, European legislation has increasingly addressed the complexities of UASs, leading to a diverse legal landscape encompassing UAS-specific, aviation-specific, and general-purpose laws.[9] UAS-specific legislation targets UAS activities directly, such as operational rules and the management of unmanned traffic systems. In contrast, aviation-specific laws provide a broader regulatory framework, treating UAS as a subset of traditional aviation. Additionally, general-purpose laws, including property, liability, criminal, and cybersecurity regulations, though not originally designed for UAS, can become relevant as these technologies intersect with various aspects of daily life and existing legal norms.

Against this backdrop, the European scholarly discussion has already generated valuable insights regarding the role of private law in the regulation of drones for civil and commercial uses.[10] This is because the use of drones may interfere with the legal sphere of third parties. This can fuel disputes and conflicts of interest between drone users and third parties, which call for appropriate resolutions. Compared to other aircraft, such as helicopters, UASs pose peculiar challenges in such contexts because they may fly substantially closer to the ground, thus creating the conditions for more direct interferences with the legal rights and interests of third parties.

In private law, important scholarly contributions have been made regarding the role of civil liability (or tort) law[11] and privacy or data protection law.[12] Conversely, property law is an area of private law that has attracted much less scholarly attention. While being extensively studied in the US legal scholarship,[13] the role of property rights has remained on the sidelines of the European scholarly discussion of the role of law in civil and commercial uses of drones.

[9] Gijs van Dijck, Alexandru-Daniel On, Jasper Snel, and Rohan Nanda, 'Retrieving Relevant EU Drone Legislation with Citation Analysis' (2023) 7(8) Drones 490.

[10] Antohony A Tarr and others (eds), *Drone Law and Policy Global Development, Risks, Regulation and Insurance* (Routledge 2021); Giuseppe F Aiello, Maria A Biasiotti, and Erica Palmerini (eds), *Diritto dei droni. Regole, questioni e prassi* (Giuffrè 2018); Alexandre Cassart, *Droit des drones. Belgique, France, Luxembourg* (Bruylant 2017).

[11] *Ex plurimis,* Hyewon Hannah Choi, 'Delivery Drones: Inapt for Application of Current Negligence Theory' (2021) 86(3) Journal of Air Law and Commerce 435; Kristopher-Kent Harris, 'Drones: Proposed Standards of Liability' (2018) 35(1) Santa Clara Computer & High Technology Law Journal 65; Vivek Sehrawat, 'Liability Issue of Domestic Drones' (2018) 35 Santa Clara Computer & High Technology Law Journal110; Benjamin D Mathews, 'Potential Tort Liability for Personal Use of Drone Aircraft' (2015) 46 St Mary's Law Journal 573; Jordan M Cash, 'Droning on and on: A Tort Approach to Regulating Hobbyist Drones' (2016) 46 The University of Memphis Law Review 695.

[12] *Ex plurimis,* Ronnie R Gipson , 'The Rise of Drones and the Erosion of Privacy and Trespass Laws' (2020) 33(3) The Air & Space Lawyer 1; Timothy T Takahashi, 'Drones and Privacy' (2012) 14 Columbia Science and Technology Law Review 72; David Sella-Villa, 'Drones and Data: A Limited Impact on Privacy' (2021) 55 University of Richmond Law Review 991; Gregory S McNeal, 'Drones and the Future of Aerial Surveillance' (2016) 84 George Washington Law Review 354; Rebecca L Scharf, 'Game of Drones: Rolling the Dice with Unmanned Aerial Vehicles and Privacy' (2018) 2018 Utah Law Review 457.

[13] Tyler Watson, 'Maximizing the Value of America's Newest Resource, Low-Altitude Airspace: An Economic Analysis of Aerial Trespass and Drones' (2020) 95(4) Indiana Law Journal 1399; Brent Skorup, 'Drones, Airspace Design, and Aerial Law in States and Cities' (2022) 55(1) Akron Law Review 157; Hillary B Farber, 'Keep out: The Efficacy of Trespass, Nuisance and Privacy Torts as Applied to Drones' (2017) 33 Georgia State University Law Review 359; Troy A Rule, 'Airspace in an Age of Drones' (2015) 95 Boston University Law Review 155; Michael N Widener, 'Local Regulating of Drone Activity in Lower Airspace' (2016) 22 Boston University Journal of Science & Technology Law 239.

The present article aims to start filling this gap. This is important because the delimitation of the scope of landowners' rights, particularly their vertical extension, can help resolve conflicts arising between drone users and landowners.

Against this backdrop, the present article aims to critically consider the role of property law in the medical use of drones, focusing on the extension of the rights of the landowner on the 'air column' above their land.[14] In doing so, the article leverages the examples of two different European legal systems, ie, Italy and the Netherlands. While the selection of the relevant legal systems is always problematic in private comparative law and inevitably involves a certain degree of arbitrariness, the choice of the Italian and Dutch legal systems is driven by both practical and legal considerations. From a practical point of view, as already mentioned above, both Italy and the Netherlands are at the forefront in Europe in exploring ways to promote the use of drones in healthcare. From a legal point of view, the Italian and Dutch legal systems exemplify instances of the French and German branches within the Civil Law tradition, respectively. Although the results of the present article cannot be generalised due to the unique peculiarities of Italian and Dutch law, they can still offer some useful insights to other continental European legal systems belonging to the two main branches of the Civil Law tradition that are considering promoting the use of UASs for medical purposes.

Accordingly, the present article is structured as follows. First, the regulatory framework for the (medical) uses of UASs is outlined. Secondly, the Italian operational solutions are reconstructed by considering the potential application of relevant property law provisions from the Italian *Codice civile* (c.c.) to emergency and non-emergency medical uses of drones. In doing so, insights from Italian case law and legal scholarship are factored in as appropriate. Thirdly, a similar exercise is conducted for Dutch law, focusing on the relevant provisions of the *Burgerlijk Wetboek* (BW). Furthermore, the Italian and Dutch operational solutions are compared from a socio-economic perspective, with a view to assessing whether and to what extent, in practice, they seem conducive (or not) to medical uses of drones. Finally, based on the identified limitations of the selected legal systems, an alternative regulatory solution is proposed to policymakers to both protect the rights of landowners and facilitate the use of drones, including for medical emergencies and routine supply of medical products.

2 The regulatory framework for the medical uses of drones

A discussion of the role of private law in the conflicts between landowners and UAS users first requires a preliminary outline of the regulatory framework, focusing on the aspects thereof that contribute to defining the general regulatory boundaries where such

[14] Thus, the present article focuses on the role of property law. It only considers safety and privacy risks to the extent that they are relevant to the delimitation of the legal protection of the landowner's property rights. To this end, an extensive examination of safety regulations and privacy laws is unnecessary for the purposes of the article.

conflicts may arise.[15] From this point of view, particularly relevant are the European Commission Delegated Regulation (EU) 2019/945 and the European Commission Implementing Regulation (EU) 2019/947.[16] These regulations establish a framework for categorising UAS operations into three classes based on the associated risk levels: open, specific, and certified. The "open" category covers low-risk operations that do not require prior authorisation, but must comply with several restrictions, including UAS weight limits (up to 25 kg), operational conditions (such as maintaining the visual line of sight), and safety requirements (like geo-fencing and operator registration). This category is divided into three subcategories: flights over people (but not crowds), flights close to people while maintaining a safe distance, and flights far from people. Each subcategory has specific technical and operational limitations to ensure safety and minimise risks.

The "specific" category encompasses medium-risk operations that require authorisation from national aviation authorities. This authorisation is granted based on a detailed risk assessment and the implementation of risk mitigation measures. Operators in this category must provide a comprehensive operational risk assessment, known as the Specific Operations Risk Assessment (SORA), which outlines potential risks and mitigation strategies. The competent authorities may also recognise standard scenarios or grant a light UAS operator certificate with privileges for certain operations, streamlining the approval process.

The "certified" category addresses high-risk operations, which require certification for both the UAS and the operator. This includes operations over crowds, transporting hazardous materials, or using large drones (over three meters in dimension). Operators in this category might also need to obtain a drone pilot licence. The certification process ensures that safety standards akin to those in manned aviation are met. These operations undergo stringent scrutiny to ensure all risks are adequately mitigated.

Furthermore, the regulatory framework introduces provisions for cross-border operations within the EU, operational conditions for UAS geographical zones defined by Member States, and the competencies and powers of relevant authorities. Finally, the European Union Aviation Safety Agency (EASA) has developed Acceptable Means of Compliance (AMC) and Guidance Materials (GM)[17] to assist UAS operators and Member States in effectively implementing the rules.

UASs used to deliver medical products, such as vaccines, blood samples, and medicines, are likely to fall under the "specific" or "certified" categories, depending on the operational context and associated risks. For instance, if the delivery involves flying over urban areas or populated regions, the operation would require a detailed risk assessment

[15] Conversely, a comprehensive and detailed description of the applicable regulatory framework falls outside the scope of the present article.
[16] Antohony A Tarr and others (eds), *Drone Law and Policy Global Development, Risks, Regulation and Insurance* (Routledge 2021), chapter 13.
[17] European Union Aviation Safety Agency site <https://www.easa.europa.eu/en/document-library/acceptable-means-of-compliance-and-guidance-materials> accessed 20 May 2024.

and appropriate authorisation under the "specific" category. This would involve evaluating potential risks, implementing mitigation strategies, and securing approval from national aviation authorities. The "specific" category's requirement for a comprehensive risk assessment ensures that all safety measures are in place, making it suitable for such critical missions.

On the other hand, transporting patients or dangerous materials using UASs poses a significantly higher risk and would most likely fall under the "certified" category. The certification process for both the UAS and the operator under this category strives for the highest safety standards, akin to those in manned aviation. This includes obtaining necessary certifications, potentially including a drone pilot licence, and ensuring the UAS meets rigorous design and operational standards. The "certified" category's stringent requirements are essential for ensuring the safety and reliability of transport operations, given their critical nature.

Member States also play a role in defining the boundaries where UAS flights are permitted. In particular, Article 15 of Regulation 2019/947 allows Member States to establish geographical zones where certain UAS operations are restricted or prohibited. This is operationalised in Italian law by "*circolari*" of the Italian Civil Aviation Authority.[18] In the Netherlands, through Article 9 of the Flight Operations Decree, the law empowers these zones' designation via ministerial orders. Consequently, the ministerial order on Zoning Regulations for Unmanned Aerial Vehicles outlines prohibitions on UAS flights in specified zones.

The above shows that the EU and national regulatory framework restricts UAS flights on several levels. First, there are no-fly zones (which may also be enforced via geofencing solutions) where UAS cannot fly altogether. Secondly, mitigation strategies for UASs apply. Although the black letter of the law is not clear on this, these strategies may include measures to avoid flights over private properties.

While the approach of minimising UAS flights over private properties may be sensible when UASs are used for commercial purposes, its desirability may be more questionable when it comes to medical uses of UASs. Indeed, time is crucial in medical emergencies, and direct routes may be preferable, extending over someone else's property. Similar considerations apply to routine deliveries of medical equipment. In these cases as well, direct routes, albeit not required by emergency needs, may be much more convenient than longer and more time-consuming paths designed to avoid private properties. Indeed, it seems questionable that the delivery of critical medical equipment in the public interest should be slowed down to protect private property. The following paragraphs argue, more in detail, that Italian and Dutch property laws fail to provide the tools for a clear and

[18] Italian Civil Aviation Authority, 'Voli con droni (UAS): limitazioni e riserve dello spazio aereo', <https://www.enac.gov.it/sicurezza-aerea/droni/zone-geografiche-space/voli-con-droni-uas-limitazioni-riserve-dello> accessed 20 May 2024.

realistic regulation of the potential conflicts of interest between (medical) UAS users and landowners.

3 The role of Italian property law in medical uses of drones

Starting with Italian property law, a key relevant provision is Article 840, paragraph 2, c.c., which regulates the vertical dimension of land ownership.[19] This provision states that the landowner cannot oppose the activities of third parties at such a depth underground or at such a height in the space above the ground that they have no interest in prohibiting such third parties' activities. Thus, Article 840, paragraph 2, c.c. provides a flexible rule to resolve potential conflicts of interests between the landowner and third parties. The resolution of such conflicts depends on whether or not the landowner has an interest in excluding the activity of third parties. This, in turn, depends on an assessment of the concrete circumstances of the case.

The interest of the landowner must be somehow objectively assessable and cannot depend on the mere subjective will of the landowner.[20] In particular, the case law states that the landowner does have an interest in excluding third parties' activities if the landowner has a concrete possibility of using the air column.[21] This means that landowner can exclude third parties' activities if these actually undermine the possibility of using the space above the land. This is irrespective of the nature of the activity carried out by the third party, the legal status of said third party, or of the frequency of the flights (although the more frequent the flights, the easier it probably is for the landowner to demonstrate that the third party is undermining the use of the air column).

The case law had the opportunity to apply this test in disputes regarding apartment buildings. In particular, the *Corte di Cassazione* ruled that, regarding the air column above the co-owned courtyards of an apartment building, such courtyards provide air and light to the apartments from across them.[22] Thus, each individual owner has an interest in, and the right to, oppose the activity of third parties who intend to build protruding structures. On another occasion,[23] the *Corte di Cassazione* held that the plaintiff did not have an interest in opposing the installation of outward-opening windows in an apartment located at nine meters above their balcony. This is because the opening and closing of the windows could not limit the use of the balcony below, considering the significant distance between the balcony and the windows.

[19] Chiara Tenella Sillani, *I limiti verticali della proprietà fondiaria* (Giuffrè 1994).
[20] V DURANTE, *Proprietà (proprietà terriera)*, in *Enciclopedia giuridica* (Treccani 1991) vol 35, 3; Cesare Salvi, 'La proprietà fondiaria', in Pietro Rescigno (ed), *Trattato di diritto privato* (Utet 1982) vol 7, 38.
[21] Cassazione civile, 9 November 2001, no. 13852 (2002) 1 Rivista Giuridica Dell'Edilizia 596; Cassazione civile, 21 October 1991, no. 11117 [1991] Massimario di giurisprudenza italiana.
[22] Cassazione civile, 21 March 2016, no. 5551 [2016] Giustizia civile - massimario annotato dalla Cassazione.
[23] Cassazione civile, 16 October 2012, no. 17680 (2013) 4 Guida al diritto 32.

It follows that the landowner is entitled to oppose drone flights if these occur at such a low altitude that the integrity of people and things is jeopardised. Under these circumstances, it is hard to argue that the use of the drone does not limit the concrete possibilities for the landowner of using their land. In fact, the landowner's concrete possibilities of using their land can be limited even if the physical integrity of people and things on the land is not put at risk. This is because drones usually carry cameras, which may pose privacy concerns for the landowner even though recordings are not made. The prospect of being seen remotely can negatively affect the concrete potential uses of the land by its owner. This has the potential of further extending upwards the vertical scope of the right to exclude under Article 840, paragraph 2, c.c.

Thus, if a drone flies too close to their property, a landowner can seek a judicial injunction, seek damages, and even resort to self-defence, provided that its requirements under Article 52 *Codice penale* (the Italian Criminal Code), particularly those of necessity and proportionality, are met.

Against this backdrop, if the drone is delivering a medical product for an emergency, the drone user may invoke the state of necessity defence under Article 55 *Codice penale*. To save a life, infringing on someone else's property rights may indeed be justified. However, if damages are caused, the drone users will still have to pay an indemnity to the landowner according to Article 2045 c.c.[24] For the purposes of this Article, an indemnity is intended as a sum inferior to the level of full compensation.[25] This is a way to balance the interest pursued by the injurer and the interests of the individual concerned.[26]

Turning now to non-emergency situations, the drone user may intend to establish a routine supply route, for instance, to supply a hospital or clinic that is too costly or impossible to reach via more traditional transportation means or that can be reached more efficiently by an UAS. The drone user may prevent issues with the landowner by seeking their explicit prior authorisation to fly over their property. If, however, the land is bought by a third party, the drone user will need to seek the authorisation of the new landowner. A more stable contractual arrangement, which could be enforced against any new owner of the land, can be reached by establishing a servitude (or easement) on the land. Article 1027 c.c. defines servitude as the burden imposed on a land for the use of another land, which belongs to a different owner.[27] The land in favour of which the servitude is created is called dominant, whereas the other is defined as servient. The owner of the servient land must allow the owner of the dominant land to use the servient land for one or more

[24] Marco Comporti, 'Fatti illeciti: le responsabilità presunte. Artt. 2044-2048' in FD Busnelli (ed), *Commentario al Codice civile* (Giuffrè 2012).
[25] ibid 32.
[26] ibid 33.
[27] Paolo Vitucci, 'Servitù prediali', in *Digesto discipline privatistiche* (UTET 1998) vol XVIII, 495; Giuseppe Grosso and Giommaria Deiana, *Le servitù prediali*, I, (UTET 1963) 538; Giuseppe Branca, 'Servitù prediali', in *Comm. Scialoja e Branca* (Zanichelli 1967) 274, 267.

specific uses. These uses may consist in the greater convenience of the dominant land or pertain to the industrial destination thereof (Article 1028 c.c.).

Servitudes can be either voluntary or compulsory. A voluntary servitude is established by means of a contract or will (Article 1058 c.c.). The landowners concerned may agree to establish a drone overflight servitude between their respective lands. Conversely, it is unlikely that a compulsory servitude may apply. The owner of the land that will become dominant may demand the establishment of a compulsory servitude, under the conditions set in the law, even against the will of the owner of the land that will become servient. In lack of an agreement between the owners, the landowner that will become dominant can ask the judge for a sentence establishing the servitude (Article 1032 c.c.). For instance, Article 1051 c.c. provides that the owner of a land parcel that is surrounded by someone else's lands and does not have access to the public road is entitled to pass over a neighbouring land parcel for agriculture and the better use of their own land parcel. Likewise, Article 1052 c.c. grants the same right to the owner of a land parcel that does have access to the public road but where such access is unsuitable or insufficient for the needs of the land. This is provided that this fulfils agricultural or industrial needs. In both instances, the owner of the servient land is owed an indemnity (Article 1053 c.c.). Since healthcare facilities typically have viable access to the public road, their owners are unlikely to qualify for compulsory servitudes.

4 The role of Dutch property law in medical uses of drones

Turning now to Dutch property law, Article 5:21, paragraph 2, BW states that third parties may use the space above and under the surface of the land, provided that they make use of it so high above or so deep under the surface that the landowner has no interest in opposing it. Paragraph 3 provides that this does not apply to the right to fly in the airspace.

The parliamentary history offers some useful insights into the content and rationale of paragraph 2.[28] First, it clarifies that the burden of proof rests on the person who wants to use the space.[29] Secondly, it states that the owner's interest does not have to be financial and can be purely aesthetic.[30] Thirdly, it provides that paragraph 2 does not set any fixed

[28] Fokke J Vonck, 'Commentaar op art. 5:21 BW' in *Groene Serie Zakelijke rechten*. Arguing in favour of a tridimensional reinterpretation of traditional property rights see Arie J Mes and others, 'Eigendom van onroerende zaken, met name natrekking (titels 1 en 3), Flexibele eigendomsverhoudingen in het vastgoedrecht', in Leon CA Verstappen (ed), *Boek 5 BW van de toekomst* (preadviezen KNB) (Sdu 2016) 181, 183; Arie J Mes, 'Driedimensionaal eigendom' (2014) Weekblad voor Privaatrecht, Notariaat en Registratie 7043; Aart A van Velten and Fokke J Vonck, 'Appartementsrecht en aanverwante rechtsfiguren voor de privaatrechtelijke vormgeving van bouwwerken (preadvies VBR)' (IBR 2016) 116, 117; Arie J Mes, 'De historische ontwikkeling van natrekking van onroerende zaken in het perspectief van driedimensionaal eigendom' (2020) 3 Rechtsgeleerd Magazijn Themis 109, 122.

[29] T-M, *Parlementaire Geschiedenis BW Boek 5* 126. See also Carel JJM Stolker, 'Commentaar op art. 5:21 BW' in *Tekst & Commentaar Burgerlijk Wetboek*.

[30] T-M, *Parlementaire Geschiedenis BW Boek 5* 126.

height limit. This will depend on the circumstances of the case[31] and will therefore be determined on a case-by-case basis.

In this connection, an important test is whether the use of the space above the surface of the land can prevent the landowner from using such space. This refers not only to practical limits but also to legal limits. For instance, if the zoning plan only allows the land to be used as pasture, the landowner's interest to oppose the use of the air column by others will likely be limited.

Moving on to paragraph 3, this contains a provision regarding flying above one's own or someone else's land. The parliamentary history states that the question of whether flying is permitted should not be answered based on the rules governing the ownership of land.[32] This would create an unjustified difference in legal position between the landowner over whom the aircraft coincidentally flows precisely above and other landowners.[33] Whether a landowner can oppose a certain method of flying is a question that should, rather, be assessed in tort. In addition, attention must be paid to the special legislation in the field of air law, which is partly of a public law nature.[34]

At the same time, according to parliamentary history, flying means moving through the air above someone else's ground, with an airplane, a hot air balloon, a zeppelin, a spacecraft, or a means of flying that may yet be invented in the future. Based on this list of examples, Koops[35] states that the exception in paragraph 3 only refers to manned flying vehicles. Thus, the exception does not extend to unmanned vehicles, such as drones. This means that a landowner has the right to deny the use of the space to drone pilots, unless the drone flies so high that the landowner has no interest in it (paragraph 2).[36] Based on this, Koops reaches the conclusions that the landowner may be entitled to shoot the drone down in self-defence.[37]

Naturally, whether self-defence is actually warranted in a specific case depends on a number of further factors, such as whether or not the self-defence is proportionate. The court of Gelderland,[38] for instance, adjudicated a case where the defendant shot down a drone carrying a camera with an air rifle fearing that their neighbour was spying on them. The neighbour sought compensation from the defendant who had taken down their drone. The court held that the neighbour was indeed infringing on the privacy of the defendant; however, the reaction of this latter was disproportionate. Thus, the court held that the defendant should bear half of the damages. Unfortunately, the court did not take this opportunity to clarify the vertical extent of the right of private property of the landowner.

[31] ibid 128.
[32] ibid.
[33] MvA II, *Parlementaire Geschiedenis BW Boek 5* 127.
[34] ibid.
[35] Egbert Koops, 'Drones, grondeigendom en de luchtkolom van artikel 5:21 BW' (2014) Ars Aequi 610, 613.
[36] Carel JJM Stolker, 'Commentaar op art. 5:21 BW' in *Tekst & Commentaar Burgerlijk Wetboek* (Wolters Kluwer 2023).
[37] Egbert Koops (n 35). See also Mathijs Verbrugge, 'Civiel gebruik van drones' [2018] Verkeersrecht 13.
[38] Rechtbank Gelderland 10 May 2017, ECLI:NL:RBGEL:2017:2663.

At the same time, drone users can rely on justifications to avoid situations where they might end up paying damages to landowners, in accordance with Article 6:162, paragraph 2 BW. In terms of justifications that can rule out civil liability and the obligation to pay damages, Dutch law is quite generous and open to contributions from the case law and the legal scholarship.[39] Among the numerous justifications that can be found in the different legal formants, the one that is most likely to apply to emergency uses of drones is the *noodtoestand* (emergency situation).[40] As a specific instance of force majeure (*overmacht*), *noodtoestand* may be invoked by someone who is forced to choose between two mutually conflicting duties and interests and lets the most compelling (or higher) one to prevail.[41] It is settled case law that infringements on the property rights of someone are justified if necessary to prevent an imminent, serious danger to the life or health of third parties.[42] This means that, in an emergency, drones may be allowed to fly over someone else's land to deliver the needed equipment.

Turning now to a non-emergency situation, if a drone flies close enough to the ground, the landowner is, in principle, entitled to oppose the drone flight and use the reaction tools made available to them by the legal system (injunction, damages, self-defence).

On the other hand, the drone user can find a form of protection in Article 6:168 BW. This Article states that a court may reject an injunction claim if the behaviour that must be tolerated for 'compelling reasons of public interests'[43]. The injured party, nevertheless, remains entitled to claim damages. Furthermore, if a judgment awarding damages is not complied with, the court may still grant the injunction. Thus, in the pursuit of a compelling public interest - and it is hard to argue that the routine supply of medical products to a hospital or a similar facility is not in the public interest - the drone user may be allowed to fly over the landowner's property. However, they would still be required to pay damages to the landowner.

Besides specific contractual arrangements with the landowner concerned (which can raise what in Dutch private law is called *kwalitatieve verplichting*), drone users and landowners may contract to establish more stable supply routes through *erfdienstbaarheden* (servitudes or easements) in accordance with Articles 5:70 - 5:84 BW.

[39] Cees van Dam, *Aansprakelijkheidsrecht* (BJU 2020) No213; Ton Hartlief and others, *Verbintenissen uit de wet en Schadevergoeding* (Kluwer 2018) No 18; Louis Visscher, *Een rechtseconomische analyse van het Nederlandse onrechtmatige daadsrecht* (EUR 2005) 101; Cees van Dam, *Aansprakelijkheidsrecht, een grensoverschrijdend handboek* (BJU 2000) No 815 and 827; Ton Hartlief and Gerrit van Maanen, 'Hoe werkt de onrechtmatige daad?' (1995) 22 Ars Aequi 38.

[40] Kasper J.O. Jansen, 'Art. 6:162 BW', in *Groene Serie Onrechtmatige daad*, section 7.2.1.6.

[41] Hoge Raad 23 July 2011 ECLI:NL:HR:2011:BP5967.

[42] Hoge Raad 3 mei 1934 NJ 1934/1549.

[43] Siewert D Lindenbergh, 'Commentaar op art. 6:168 BW' in *Tekst & Commentaar Burgerlijk Wetboek* (n 36).

5 Comparative socio-economic analysis

Despite their unique characteristics, Italian and Dutch property laws share several features (possibly due to their common roots in Roman law). In particular, both laws tackle potential conflicts of interest between drone users and landowners with a flexible rule referring to the landowner's interest in excluding third parties from using the air column. This is, in turn, based on the extent to which the landowner can actually use the land and how drone overflights might affect this.

This means that neither legal system has a clear-cut rule on this. This is particularly problematic in non-emergency situations. It makes it difficult for drone users to identify the legitimate altitude for drone overflights. This may change significantly from one landowner to another. Thus, it is practically impossible for drone users to plan routine supply routes. In Dutch law, compelling reasons of public interests may be invoked to shield the drone user from injunctions, but damages would still need to be paid.

Relying on servitudes is also unrealistic for drone users in both legal systems. Compulsory servitudes are unlikely to apply, as the law imposes quite restrictive requirements that are typically modelled after agricultural and industrial needs. These will rarely apply to healthcare facilities. Conversely, voluntary servitudes require drone users to contract with each and every landowner between the source and the destination of the supply route. This can contribute to high transaction costs for drone users, making it economically prohibitive for them to establish drone-driven supply routes.

Turning now to landowners, the flexible rule at the core of both Article 840, paragraph 2, c.c. and Article 5:21, paragraph 2, BW can offer them useful reaction tools in exceptional circumstances only, e.g., when a drone flies so close to the ground that it poses an immediate threat to bodily integrity. Otherwise, it is hard for landowners to understand exactly when they are entitled to exclude drone overflights, including through self-defence, and potentially claim damages from drone users. As mentioned above, a drone may threaten not only bodily integrity but also the privacy of landowners, which may reasonably occur even if the drone is flying at a quite high altitude. This may be a frequent occurrence, especially, but not exclusively, in urban contexts. In such cases, *quid juris*? In its ultimate inconclusiveness, the decision by the court of Gelderland mentioned above is quite telling. The drone user was infringing on the landowner's privacy, but the landowner exceeded in shooting the drone down. Failing to offer a clear operational rule for such cases, the court issued a 'Salomonic' decision where the damages are shared equally between the individuals concerned.

From a socio-economic perspective, this lack of clear operational rules in both legal systems seemingly leads to what could be described as a *lose-lose* situation. This is because neither the interests of landowners nor those of drone users are adequately legally protected. This is due to the legal uncertainty stemming from a fundamental

tension between the (traditional) rule over the air column and the (emerging) possibility of low-altitude flights of drones.

In both legal systems, drone users seem to have more leeway in emergencies. However, neither offers a smooth pathway for this. Under Italian law, the drone user would still be entitled to pay an indemnity to the landowner(s) if the drone flew under the (flexible) threshold as per Article 840, paragraph 2, c.c.

6 Conclusions

The considerations above follow a recurring pattern when an emerging technology interferes with established legal solutions devised in a different socio-economic (and technological) context. While pre-modern property law tended to vertically extend property rights over the land *usque ad sidera* (up to the stars), the gradual developments in (manned) flying methods, from balloons to airplanes, challenged the feasibility of that traditional solution and led to devising more flexible approaches. Such a flexible approach, which is well exemplified in the Italian and Dutch Civil Codes, proved effective when flying vehicles operated far from the ground, protecting the latter from legal reactions from landowners. This was intended to favour an activity that was deemed socially and economically desirable.

Nevertheless, this flexible approach proves inadequate for promoting the use of drones and protecting landowners, even if drones are used for important purposes of public interest in the area of public health, such as in medical emergencies and for the (more) routine supply of medical equipment. The letter of the law, which heavily relies on case-by-case assessments, does not seem to offer courts sufficient space to propose clearer operational rules.

Similarly to what happened with the rise of aerial vehicles in the XIX and (early) XX centuries, the emerging use of drones offers the opportunity to update further and refine the rules governing the use of the air column over the land. Just like balloons and airplanes indicated the undesirability of extending property rights up to the stars, the use of drones shows how the test of the interest of the individual landowner to exclude third parties' activities is inadequate to tackle this emerging reality, which promises to deliver important socio-economic benefits.

Other legal systems are exploring ways to better advance the interests of both drone users and landowners. In the US legal literature, a proposal has been put forth to clearly define the navigable airspace by foreseeing a minimum height under which drones cannot fly.[44] The proposal is to set this at around 200 feet (about 60 meters) from the ground.[45] The proponent deems this reasonable in the US context as 200 feet corresponds to five

[44] Lane Page, 'Drone Trespass and the Line Separating the National Airspace and Private Property' (2018) 86 George Washington Law Review 1152, 1173.
[45] ibid 1174.

times the average two-story home and grants owners substantial control over their air columns by excluding anything that flies below it. Whether this or a higher altitude would be more appropriate in the context of a European country should the object of an open and reasoned deliberation of the policymakers or of the competent regulatory authorities, considering national and local specifies and the destination of use (e.g., residential or agricultural) of the land.

Based on a compromise where both sides relinquish some control over the air columns, a clear-cut threshold along these lines, to be adjusted to the economic and practical characteristics of landownership in the respective legal system, has the potential to provide both UAS users and landowners with a clearer legal framework: the former know exactly when they are allowed to fly UASs over someone else's land legitimately; the latter have a clearer idea of when they are entitled to react to drone overflights. Thus, substituting a case-by-case assessment with a clear-cut altitude seems to be able to contribute to a mutually advantageous situation where the legitimate interests of both parties may be more clearly and better protected.[46] The ultimate responsibility for the determination of the conventional minimum altitude for drone overflights should rest on legislators or regulators in an attempt to balance the competing interests of drone users and landowners with a compromise solution; a solution where both interested categories of parties concede a part of their potential sphere of control over the airspace to each other in exchange for a clearer delimitation of their respective spheres. Also, the proposal for a clearer delimitation is not expected to drastically increase the activity level of drone users. This is because the regulatory framework for the authorisation and licensing of drone operations should still continue to apply, thus avoiding that an excessive number of drones fly over the private properties of someone else.

This proposal needs, however, to be qualified. In respect of non-emergency uses of UASs, such a compromise solution seems adequate for operations in the public interest falling in the specific category, such as the delivery of (non-hazardous) medical equipment to public healthcare facilities. Conversely, the proposed solution seems less viable for drone flights that are not in the public interest (eg, commercial deliveries) or that pose substantial risks for third parties (eg, flight operations belonging to the certified categories, such as for the transportation of patients or hazardous materials).

Turning now to emergency medical uses of UASs, flying over private properties above a conventional minimum altitude should be allowed irrespective of the applicable operation category. This would facilitate life-saving operations without triggering indemnification or compensation mechanisms.

Incidentally, in an emergency, drone users should retain the possibility of flying below the normative conventional altitude, if needed. To make it clear to landowners that a

[46] Embracing rather than ignoring owners' rights can actually accelerate the use of drones. See Troy A Rule, 'Drones, Airspace, and the Sharing Economy' (2023) 84 Ohio State Law Journal 157.

drone is flying for an emergency, drones should carry recognisable signs and emit recognisable sounds, also to be determined normatively. This is also to avoid reactions in self-defence from landowners.

Naturally, in order to make the proposed legal arrangement effective, the massive information asymmetries between landowners and drone users should also be addressed. The proposed delimitation would indeed remain ineffectual in a situation where it is disproportionately difficult for the landowners to identify who is actually flying over their properties and at what altitude. As a UAS traffic management system, the U-space[47] can provide a viable information and infrastructural basis for interested persons to obtain such information and use their rights more effectively.

In conclusion, a revised normative arrangement revolving around a clear-cut minimum height for drone flights has the potential to facilitate the development of current initiatives to upscale the use of drones also for medical purposes, both in emergencies and (with some exceptions) non-emergencies, without completely forfeit the interests of landowners in respect of the air columns extending over their properties. By delimiting in a clear and foreseeable way their respective spheres, this normative exercise would also simplify the application of civil or tort lability law rules and privacy law rules to disputes between drone users and landowners.

[47] EASA, 'What is U-space', <https://www.easa.europa.eu/en/what-u-space> accessed 26 June 2024.

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.

*Mitja Kovac**

SPECIAL SECTION

TRAGEDY OF THE COMMONS, CIVIL DRONES AND HYBRID MODES OF TECHNOLOGY REGULATION: A COMPARATIVE LAW AND ECONOMICS PERSPECTIVE

Abstract

This paper provides a multidisciplinary assessment of the growing use and importance of civil drones, evaluates the related problem of the commons, and seeks to assess its impact on the research & development processes in companies that develop or employ civil drones in their daily operations. Recommendations are given to ensure optimal regulatory intervention covering potential, uncontemplated automated civil drone-related hazards. If it evolves in ways not intended by its designers or users, the judgement-proof automated civil drone could create unforeseeable losses wherever current tort and contract law regimes do not ensure optimal risk internalisation and precaution, while also not deterring opportunism. Moreover, it is argued in the paper that the identified shortcomings mean the debate on the different approaches to controlling hazardous activities boils down to the question of efficient ex ante safety regulation and allocation of property rights (resembling those in the aviation industry). Hybrid modes of regulation are also investigated with a focus on the inclusive growth of the AI-drone industry in the EU and a set of economically informed normative suggestions is presented for an improved hybrid regulatory response, which should achieve optimal risk internalisation, precaution, and firm-level innovation.

JEL CLASSIFICATION: C23, C26, C51, K42, O43

SUMMARY

* Professor of civil and commercial law at the University of Ljubljana School of Economics and Business; email: Mitja.kovac@ef.uni-lj.si.

** The author acknowledges financial support from the Slovenian Research Agency (research core funding No. P5-0128).

DOI 10.13135/2785-7867/10741

1 Introduction

Drone use around the world skyrocketed off in recent years, bolstered by rapid technological innovations, business needs, and societal changes. Nowadays, people have become used to seeing small, unmanned aircraft flying above city streets, local fields, touristic harbours, beaches and residential and commercial properties, and very soon autonomous AI-operated drones[1] will be able to automatedly take off, fly, and land virtually anywhere using real-time data. As of February 2024, 375,226 commercial drones and 400,858 recreational drones were registered in the USA alone.[2] The global commercial drone market size was estimated at USD 19.89 billion in 2022 and is expected to grow at a compound annual growth rate (CAGR) of 13.9% from 2023 to 2030.[3] Drones' employability in military, scientific, leisure and commercial uses and their capability to deliver packages and transport goods more efficiently and quickly than ever before are revolutionising our everyday way of life.[4]

Snead and Siebler stress that drones are one of many emerging technologies that can legitimately be both celebrated and feared.[5] Clark reports that there is an increasing regulatory activity and that "several governments have already introduced specific drone regulations" and, for example, "banned drone flights over selected facilities and locations

[1] Autonomous drones are unmanned aerial vehicles (UAVs) that operate using Artificial Intelligence (AI)-powered navigation and operational software, and do not require a human pilot. An autonomous drone is able to conduct a safe flight without the intervention of a pilot. It does so with the help of artificial intelligence, enabling it to cope with all kinds of unforeseen and unpredictable emergency situations. This is different from automatic operations, where the drone flies pre-determined routes defined by the drone operator before starting the flight. For this type of drone, it is essential for the remote pilot to take control of the drone to intervene in unforeseen events for which the drone has not been programmed. See for example Dario Floreano, and Robert Wood, 'Science, Technology and the Future of Small Autonomous Drones' (2015) 521 Nature 460; and Patrick Fabiani, Vincent Fuertes, Alain Piquereau, Roger Mampey and Florent Teichteil-Königsbuch, 'Autonomous Flight and Navigation of VTOL UAVs: from Autonomy Demonstrations to Out-of-sight Flights' (2007) 11 (2-3) Aerospace Science and Technology 183.

[2] Federal Aviation Administration, *Drones by the Numbers* (United States Department of Transportation, 2024). The annual Drone Market Report by Drone Industry Insights, published in August 2023, predicts a global drone market size of USD 54.6 billion by 2030, with the commercial market growing at a 7.7% CAGR. These commercial CAGR figures are 0.1% lower than in the same study in the previous year; Drone Industry Insights, *Global Drone Market Report 2023-2030* (Drone Industry Insights 2023).

[3] Market Analysis Report, *Commercial Drone Market Size, Share & Trends Analysis Report by Product, by Application, by End-use, by Propulsion Type, by Range, by Operating Mode, by Endurance, by Region, and Segment Forecasts, 2023 - 2030* (Grand View research 2023).

[4] See eg, Panagiotis Radoglou-Grammatikis, Panagiotis Sarigiannidis, Thomas Lagkas, and Ioannis Moscholios, 'A Compilation of UAS Applications for Precision Agriculture' (2020) 172 Computer Networks 107148; Jake McRae, Christopher Gay, Brandon Nielsen, and Pieter Hunt, 'Using an Unmanned Aircraft System (Drone) to Conduct a Complex High-Altitude Search and Rescue Operation: A Case Study' (2019) 30(3) Wilderness & Environmental Medicine, 287 and Dante Tezza, and Marvin Andujar, 'The State-of-the-Art of Human–Drone Interaction: A Survey' (2019) 7 IEEE Access 167438.

[5] John Snead and Jonathan Seibler, *The FAA Drone Registry: A Two-Month Crash Course in How to Over-criminalize Innovation* (The Heritage Foundation 2016).

in support of national security and people's safety."[6] It must be noted that drones are today categorised as aircraft and thus fall within the regulatory framework that governs aircraft.[7] Legislators, landowners and businesses are exploring their future roles in the commercialisation of low-altitude airspace. Nevertheless few, if any, theories of airspace rights and economic regulation have generated a viable legal, economic and regulatory framework that balances the often-competing business imperatives of a robust drone economy, the property rights of landowners, safety, and the interests of local governments.

Dor and Hoffman, for example, focus on unsettled questions of airspace property rights and argue that landowners should exclusively own and control the "superadjacent", low-altitude airspace directly above their land, and should be free to commercialise and sell access to their private airspace, or to prohibit drones from entering it.[8] Namely, in the U.S. the Supreme Court in the famous Causby case[9] adopted a middle ground theory where landowners own all the "superadjacent" airspace above their property, and an invasion of that airspace should be treated as if an actual invasion of the surface has occurred.[10] The U.S. Supreme Court did not determine the precise limits of this "superadjacent" airspace—all that was certain was that it fell somewhere between the eighty-three feet (12m) above ground where the Causbys' property had been invaded and the 500-foot (150m) minimum safe altitude of flight where public navigable airspace in the U.S.

[6] See eg, Robert Clarke, 'Understanding the Drone Epidemic' (2014) 30 (3) Computer Law & Security Review 230. See also Benjamin Harber, 'Eyes in the Sky: Constitutional and Regulatory Approaches to Domestic Drone Deployment' (2014) 64(1) Syracuse Law Review; Katharine Suominen, 'The Planet of the Drones: Comparing the Regulation of Commercial Drones in the United States and the United Kingdom' (2016) 29 (2) New York International Law Review 37; and Timothy Ravich, 'A Comparative Global Analysis of Drone Laws: Best Practices and Policies' in Bart Custers (ed), *The Future of Drone Use. Opportunities and Threats from Ethical and Legal Perspectives.* Information Technology and Law Series Vol 27 (T.M.C. Asser Press 2016).

[7] In the addition to all other legislation that governs any product such as contractual and third-party liability rules, insurance, security and environmental laws, GDPR and AI regulation that apply to civil drones as a type of aircraft.

[8] Lavi Ben Dor and Jonathan Hoffmann, 'The Emerging Airspace Economy: A Framework for Airspace Rights in the Age of Drones' (2022) 4 Wisconsin Law Review 953. See also Sarah Kreps, *Drones: What Everyone Needs to Know* (Oxford University Press 2016); and Ella Atkins , Anibal Ollero and Anonios Tsourdos, *Unmanned Aircraft Systems* (Wiley 2016).

[9] *United States v. Causby* [1946] US 60, [1946] 328 U.S. 256.

[10] The Court stated: "We have said that the airspace is a public highway. Yet it is obvious that if the landowner is to have full enjoyment of the land, he must have exclusive control of the immediate reaches of the enveloping atmosphere. Otherwise buildings could not be erected, trees could not be planted, and even fences could not be run. The principle is recognized when the law gives a remedy in case overhanging structures are erected on adjoining land. The landowner owns at least as much of the space above the ground as he can occupy or use in connection with the land. The fact that he does not occupy it in a physical sense—by the erection of buildings and the like—is not material. As we have said, the flight of airplanes, which skim the surface but do not touch it, is as much an appropriation of the use of the land as a more conventional entry upon it. . . . The reason is that there would be an intrusion so immediate and direct as to subtract from the owner's full enjoyment of the property and to limit his exploitation of it. While the owner does not in any physical manner occupy that stratum of airspace or make use of it in the conventional sense, he does use it in somewhat the same sense that airspace left between buildings for the purpose of light and air is used. The superadjacent airspace at this low altitude is so close to the land that continuous invasions of it affect the use of the surface of the land itself. We think that the landowner, as an incident to ownership, has a claim to it and that invasions of it are in the same category as invasions of the surface;" ibid 264, 68.

begins.[11] Several subsequent cases made clear that landowners in the U.S are entitled to the exclusive control and ownership of the low-altitude airspace they seek, or could potentially seek, to use or enjoy above their land, and that they must be compensated fair market value for any overflights in that airspace.[12] More recently, the U.S. Supreme Court held in Cedar Point Nursery case that a California law requiring certain agricultural employers to permit union organisers (who are private entities) onto their property for certain periods of time every year constituted a per se physical taking.[13] The Court reasoned that the regulation "appropriate[d] for the enjoyment of third parties the owners' right to exclude," one of the "most treasured" rights belonging to a property owner.[14] Dor and Hoffmann also predict the emergence of a marketplace for parties to buy, sell and lease valuable airspace to accommodate drone delivery such that companies like Amazon or Walmart will compensate landowners, or even governments that own city streets and highways, for the airspace where drones will one day fly.[15] In addition, they argue that so as to effectuate that marketplace the FAA must redefine the public "navigable airspace" for it to lawfully regulate drone flight paths below 150 metres.[16]

Hodgkinson and Johnston state that one of the key challenges for lawmakers is to regulate drones in a way that allows society to reap the benefits of drones while simultaneously preserving the privacy, safety, and security of individuals.[17] For example, the Australian aviation safety regulator has made progress in establishing a regime that balances safety and usability by introducing a new category of drones below 2 kilograms

[11] The Court expressly confirmed that landowners have a "paramount and exclusive right to exercise the prerogatives of ownership in all of the airspace" that they possess, "or can effectively possess" in the future, and in any further amount of valuable airspace necessary to ensure full enjoyment of the property. "[T]he practical effect . . . [was] to constrict the landowner's rights within the boundaries of reason, or to put it another way, within the boundaries of value;" ibid 263, 65.

[12] See eg *Griggs v. County of Allegheny* [1962] 369 U.S. 84 [1962]; *Branning v. United States* [1986] 654 F.2d 88 Ct. Cl. 1981 [1986]; and *Brown v. United States*, [1996] 73 F.3d 1100 [1996]. See also Lindsey P Gustafson, Arkansas Airspace Ownership and the Challenge of Drones (2017) 39 (2) University of Arkansas at Little Rock Law Review 245, 270, 273.

[13] *Cedar Point Nursery v. Hassid* [2021] 141 S. Ct. 2063 [2021]. See also *Loretto v. Teleprompter* [1928] Manhattan CATV Co., 458 U.S. 419 [1928].

[14] Cedar Point case makes clear that granting UAS operators carte blanche to invade landowners' superadjacent airspace would, absent just compensation to the landowner, constitute an unconstitutional taking; Dor and Hoffman (n 8) 980.

[15] Dor and Hoffmann (n 8) 953. See also Roger Clarke (n 6) and Mostafa Hassanalian and Abdessattar Abdelkefi, 'Classifications, Applications and Design Challenges of Drones: A Review' (2017) 91 Progress in Aerospace Sciences 99, 107.

[16] They also call for the division of airspace into four distinct regions, with different rights and responsibilities for those operating in each domain; ibid.

[17] David Hodgkinson and Rebecca Johnston, *Aviation Law and Drones: Unmanned Aircraft and the Future of Aviation* (Routledge 2017). See also Bart Custers (ed), *The Future of Drone Use: Opportunities and Threats from Ethical and Legal Perspectives* (T.M.C. Asser Press The Hague 2016); Brian F Havel, and John Q Mulligan, "Unmanned Aircraft Systems: A Challenge to Global Regulators" (2016) 65(1) DePaul Law Review 107; and Henry Perritt and Eliot Sprague, *Domesticating Drones: The Technology, Law and Economics of Unmanned Aircraft* (Routledge 2016).

for commercial use that does not require the operator to hold a licence.[18] As to the liability issue, Hodgkinson and Johnston suggest that the drone operator shall be liable for damage sustained by third parties only upon the condition that the damage was caused by a drone in flight.[19] Watson argues that a combination of a state law that clarifies landowners' property rights "by focusing on proxies that measure ever smaller classes of uses", such as the further delineation of landowners' rights based on their location and governance rules through municipal drone zoning ordinances, may increase efficiency by filling in the gaps not currently addressed by the common law aerial trespass doctrine.[20] Most of other scholarly literature focuses on drones' potential impact on privacy rights, tort claims, and criminal evidence gathering.[21]

This paper joins this critical debate and takes a law and economics perspective while focusing on the issue of liability and property rights held by individual property owners and the use of automated civil drones by various stakeholders in the EU.[22] Compared to the mentioned literature on the employment of civil drones and associated issues of property rights, this paper attempts to show that the combined problem of prohibitively high transaction costs and tragedy of the commons phenomena might make the operation of classic property and contract law instruments (eg, trespassing and contracting between the owners of a given space and drone operators) inadequate for addressing the rising use of automated civil drones and for not inhibiting drone-linked R&D processes in companies. While employing the relevant insights from the economic literature on regulatory techniques, in addition to the already mentioned literature this paper also sets out recommendations to ensure improved regulatory intervention covering potential, uncontemplated civil drone-related hazards. The paper also argues that the identified shortcomings mean the debate on the different approaches to controlling hazardous activities in fact boils down to the question of efficient ex ante safety regulation and allocation of property rights (akin to those in the aviation industry). Further, it investigates hybrid modes of regulation with a focus on the inclusive growth of the civil drone industry in the EU and outlines a set of normative suggestions for an improved hybrid regulatory response, which should achieve optimal risk internalisation, precaution, and

[18] Commercially Unmanned Flight – Remotely Piloted Aircraft Under 2 kg (2 November 2017) Civil Aviation Safety Authority https://www.casa.gov.au/standard-page/commercial-unmanned-flight-remotely-piloted-aircraft-under-2kg accessed 10 June 2024.

[19] They also suggest that states should require their drone operators to maintain adequate insurance or guarantee covering their liability; Hodgkinson and Johnston (n 17) 106.

[20] Tyler Watson, 'Maximizing the Value of America's Newest Resource, Low-Altitude Airspace: An Economic Analysis of Aerial Trespass and Drones (2020) 95 (4) Indiana Law Journal 1399, 1434.

[21] See eg Hillary Farber, 'Keep Out! The Efficacy of Trespass, Nuisance and Privacy Torts as Applied to Drones' (2017) 33 Georgia State University Law Review 359; Hillary Farber, 'Eyes in the Sky: Constitutional and Regulatory Approaches to Domestic Drone Deployment' (2014) 64 (1) Syracuse Law Review 13; and Troy Rule, 'Airspace in an Age of Drones' (2015) 95 Boston University Law Review 155, 158.

[22] It focuses merely on civil drones since a comparison with the military sector might due to its specific features (natural security issues, defence policy etc) fall outside the scope of this paper.

firm-level innovation. The regulatory regime should namely help the unmanned civil drone flight industry flourish by adopting an approach that ensures airspace safety while respecting landowners, drone operators, and the public alike and by recognising the value of both EU and local oversight of the skies.

The analysis presented here is both positive and normative. The analytical approach engages in interdisciplinary analysis and enriches it with concepts used in the economic analysis of law. To make the economic analysis accessible to readers not acquainted with sophisticated mathematical reasoning, the law and economics toolkit relied upon follows the traditional comparative law and economics approach.

This paper is structured as follows. The first part presents the general background and recapitulates literature on the main regulatory approaches. The second part provides a set of normative suggestions for an improved hybrid regulatory response which should achieve optimal risk internalisation, precaution, and firm-level innovation. The third part briefly comments on recent EU regulatory approaches. Finally, some conclusions are presented.

2 Conceptual and theoretical framework

This section surveys the crucial debate in law and economics and also in other social sciences concerning the balance between the state and the market. Which activities should be left to markets and which to the purview of the state? The short overview of these concepts also offers a theoretical justification for the drone-specific regulatory intervention recently enacted in the EU that thus needs to be briefly addressed. Classic law and economics textbooks suggest that such intervention is only warranted when 'market failures' materialise.[23] Among others, these include the presence of "negative externalities", which appear when actions by individual actors hold major negative consequences for others that are not mediated via markets, paving the way for an excessive level of certain activities.[24] Economically speaking, the potential hazards and damages caused by the uncontemplated activity of civil drones are a classic example of negative externalities and the asymmetric information problem. Namely, the problem of positive transaction costs and asymmetric information leads to so-called market failures which cause a suboptimal (inefficient) amount of economic activity and inefficient allocation of resources (eg, potential drone congestion in populated areas).[25] The collective-action problem, agency problem, tragedy of the commons, and the game theoretical prisoner's dilemma phenomena are the notorious embodiment of positive

[23] George Akerlof, 'The Market for 'Lemons': Quality Uncertainty and the Market Mechanism' (1970) 84 (3) The Quarterly Journal of Economics 488.
[24] Daron Acemoglu and James Robinson, *The Narrow Corridor: States, Societies, and the Fate of Liberty* (Penguin Press 2019).
[25] Akerlof (n 23) 489.

transaction costs and asymmetric information problems that generate negative externalities. The appearance of these negative externalities accompanied by the 'failure of private law' prima facie also warrants the employment of civil-drone-specific regulatory intervention in the public interest.[26]

Still, it must be emphasised that the mere existence of market failures *per se* is not an adequate basis for regulatory intervention. Regulatory intervention should take place if and only if the costs of the intervention (regulating civil drones) do not exceed its benefits. That is, the efficiency gains arising from such an intervention may be outweighed by market distortions, increased transaction costs and other misallocations in other sectors of the economy fuelled by the intervention.[27] Further, as Tinbergen suggests, in principle N problems require N legal rules — the One Instrument Per Problem Rule, meaning that every source of inefficiency in drone-related activity should be addressed with a separate regulatory policy.[28] In addition, the notorious "tragedy of the commons" concept suggests that individuals and/or firms might not see themselves as responsible for common resources like public safety and might eventually destroy such a common resource.[29]

Where market failures are accompanied by private law failures there is a *prima facie* case for regulatory intervention. However, does the mere existence of any market failures justify corrective government intervention? Many instances of market failures are remediable "by private law and thus by instruments which are compatible with the market system in the sense that collective action is not required".[30] Yet, as Professor Ogus convincingly shows, private law cannot always provide an effective solution.[31] Thus, where the 'market failure' is accompanied with a 'private law failure' there is, at least in theory, a *prima facie* (but not a conclusive) case for regulatory intervention. A series of empirical studies thus reveals that the mere presence of suspected market imperfections does not in itself warrant government corrective action and regulatory intervention.[32] Therefore, once government steps in, it might often exclude private initiative that could, in good entrepreneurial fashion, have invented ways of alleviating the suspected market

[26] Anthony Ogus, *Regulation: Legal Form and Economic Theory* (Hart Publishing 2004).
[27] ibid.
[28] Policymakers generally tend to use a single instrument to solve many problems at once. However, doing so is problematic for two reasons. First, such a single rule will be a compromise rule, which is not very effective at solving all the problems. Second, choosing the right compromise requires information on the relative social importance of all the problems; such information is nearly impossible to obtain, and therefore makes the discussion indeterminate; Jan Tinbergen, *On the Theory of Economic Policy* (North-Holland 1952). See also Mitja Kovac, *Judgement-Proof Robots and Artificial Intelligence*: *A Comparative Law and Economics Approach* (Palgrave MacMillan 2020) 109, 144; and Gerrit De Geest, 'Old Law is Cheap Law' in Michael Faure, Wicher Schreuders and Louis Visscher (eds), *Don't Take it Seriously: Essays in Law and Economics in Honour of Roger Van den Bergh* (Intersentia 2018) 505.
[29] Garret Hardin, 'The Tragedy of the Commons' (1968) 162 Science 1243. See also Scott Gordon, 'The Economic Theory of a Common-Property Resource: The Fishery' (1954) 62 (2) Journal of Political Economy 124.
[30] Ogus (n 26).
[31] ibid.
[32] Steven Cheung, 'The Fable of the Bees: An Economic Investigation' (1973) 16(1) The Journal of Law and Economics 11; and Ronald Coase, 'The Lighthouse in Economics' (1974) 17(2) The Journal of Law and Economics 357.

imperfection.[33] "Government intervention tends to foreclose such demonstration and thereby to become a self-perpetuating process."[34] Literature also suggests that even in instances of repeated market failures, the costs stemming from those imperfections should be weighed against those which the government intervention itself generates.[35] That is, for such optimal governmental intervention one assumes the perfect functioning of public administration that merely maximises social benefits.

However, while seeking to address certain market failure like for example drone-related congestion or different hazards (and maybe to even effectively cure a particular, individual market failure) governmental intervention may unintentionally impose even higher costs on society and its citizens while distorting the rest of the markets.[36] In other words, as a rule of thumb, regulatory intervention is warranted if and only if the costs of the intervention do not exceed its benefits. The argument used here is that either a regulatory solution may be no more successful in correcting the inefficiencies than the market or private law, or that any efficiency gains it gives rise to may be outweighed by the increased transaction costs or misallocations created in other sectors of the economy.[37]

In addition, poor policy may result from inadequate information, failure to anticipate significant side-effects of certain behaviour, phenomena (eg, unmanned drones delivering packages) or regulatory instruments.[38] Poor regulatory intervention along these lines may occur where the government has needed to be seen as respond rapidly to widespread calls for action, following a disaster that captured the public's attention,[39] or when it lacks resources or adapting a passive, compromising approach to contraventions.[40] Public choice theory therefore offers further support for our rule of thumb stating that "state interventions are only justified if they produce less harm than market inefficiencies".[41]

In recent years, the study of regulation has become a multi-disciplinary field featuring substantial contributions to regulatory debates being made by lawyers, political scientists, psychologists, behavioural economists, and others.[42] Regulation has actually become central to the interaction of economic, legal, political, entrepreneurial and innovation

[33] Ejan MacKaay, *Law and Economics for Civil Law Systems* (Edward Elgar 2015).
[34] ibid.
[35] MacKaay (n 33). See also Ogus (n 26) and Richard Posner, *Economic Analysis of Law* (9th edn, Aspen Publishing 2014).
[36] Posner (n 33).
[37] See Ogus (n 26); Kip Viscusi, John M Vernon, and Joseph E. Harrington, *Economics of Regulation and Antitrust* (MIT Press 1992); and Alfred Kahn, *The Economics of Regulation: Principles and Institutions* (MIT Press 1971).
[38] Michael Levine, and Jennifer L Florence, 'Regulatory Capture, Public Interest, and the Public Agenda: Towards a Synthesis' (1990) 6 (4) Journal of Law, Economics and Organization 167.
[39] ibid.
[40] See Ross Cranston, *Regulating Business-Law and Consumer Agencies* (Palgrave MacMillan 1979); and Neil Gunningham, *Pollution, Social Interest and the Law* (M. Robertson 1974).
[41] ibid.
[42] For a synthesis, see Robert Baldwin, Martin Cave and Martin Lodge, *The Oxford Handbook of Regulation* (Oxford University Press 2010). See also Malcom Sparrow, *Fundamentals of Regulatory Design* (Harvard University Press 2020).

spheres. The rise of a better regulation agenda was then designed to ensure consistency between "red-tape" and "regulatory quality" developments.[43] The so-called command-and-control (top-down approach) was the initial starting point of regulators, which later evolved into less-restrictive and incentive-based regulatory policies.[44]

3 Towards an improved regulatory response

The question of what is a 'good' regulation is extensively discussed in the literature[45] and, even though what constitutes a 'good' regulation is difficult to establish, generally five criteria should be met.[46] Literature offers a range of different legal instruments including rules of civil liability, command and control public regulations, market-based instruments, 'suasive' and voluntary instruments, smart regulatory mixes, and hybrid regulatory approaches. This section presents a set of law and economics recommendations for an improved, EU-wide, regulatory intervention which should deter hazards, induce optimal precaution and simultaneously preserve dynamic efficiency – incentives to innovate undistorted.

3.1 Tragedy of the commons, prohibitive transaction costs, and drones

The specific phenomena of interest to us in the investigation of automated drones concern the tragedy of the commons and related external effects or externalities, also known as spillover effects. A negative externality arises when one person's decision affects someone else, but where there is lack of an institutional mechanism to induce the decision-maker to fully account for the spillover effect of their action or inaction.[47] These negative externalities can then also lead to market failures since the generator of the externality does not have to pay for harming others, and so exercises too little self-restraint.[48] In other words, the private cost to the person who creates the negative externality is lower than the social cost, which is the sum of that private cost and the cost incurred by third persons.[49] Corresponding public policies are then one of the most

[43] ibid 7. See also Michael Lodge, and Kai Wegrich, 'High Quality Regulation: Its Popularity, Its Tools and Its Future' (2009) 29(3) Public Money and Management 145.
[44] Baldwin and others (n 42).
[45] See eg Robert Baldwin and Christopher McCrudden, *Regulation and Public Law* (Weidenfeld and Nicolson 1987); and Claudio Radaelli and Fabrizio De Francesco, *Regulatory Quality in Europe: Concepts, Measures and Policy Processes* (Manchester University Press 2011).
[46] Legislative mandate, accountability, due process, expertise, efficiency; Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (2nd edn, Oxford University Press 2012).
[47] See eg Arthur Pigou, *The Economics of Welfare* (Macmillan 1932); Ronald Coase, 'The Federal Communications Commission' (1959) 2 (1) Journal of Law and Economics; and Kip Viscusi, *Fatal Trade-offs: Public and Private Responsibilities for Risk* (Oxford University Press 1992).
[48] See eg Jack Hirshleifer, *Price Theory and Applications* (Cambridge University Press 1984); and Roger Miller, Daniel K Benjamin and Douglas C North, *The Economics of Public Policy Issues* (Pearson 2017).
[49] Pigou (n 47).

effective remedies for correcting this failing. Institutional response and political decision-making should hence aim at the internalisation of these negative externalities, inducing decision-makers (drone operators) to respond to the impacts of their choices on others just as if those impacts were experienced by the decision-maker directly.[50] Inadequate internalisation of such negative externalities might also materialise as the notorious "tragedy of the commons". Coined by Hardin[51] and Gordon,[52] this "tragedy of the commons" concept suggests that individuals might not see themselves as responsible for common resources such as common, public air-space above the streets and by excessively employing drones might eventually destroy such a common resource.[53] For example, the number of commercial drone deliveries rose from 34,000 in 2019 to 482,000 in 2021 and was estimated to reach 1.4 million by the end of 2022 while the overall number of packages delivered by drone increased by over 80 percent from 2021 to 2022, amounting to almost 875,000 deliveries worldwide.[54] The greater employment of civil drones may thus cause a typical materialisation of the tragedy of the commons phenomena such as air congestion in densely populated areas (and at low altitudes), the collapse of current pre-flight air route network planning, the collapse of drone delivery applications, as well as potential accidents and hazards.

Transportation literature also highlights that no currently existing method can directly address the challenge of air route network planning and resulting congestion.[55] Yet, when multiple paths utilise the same airspace, conflicts and interdependencies arise, calling for system-level optimisation.[56] When paths are optimised individually, the allocation of scarce urban airspace is not optimised, which can lead to air traffic conflicts and congestion, potentially causing system failure.[57] Moreover, civil-drone-based delivery services are also limited by several binding factors, such as low battery capacities and short delivery range, which in turn require the simultaneous use of a large fleet for

[50] See eg Leitzel Jim, *Concepts in Law and Economics* (Oxford University Press 2015) 108.
[51] Hardin (n 29).
[52] Scott (n 29).
[53] See eg Harold Demsetz, 'Toward a Theory of Property Rights' (1967) 57(2) American Economic Review 347, 351, 353.
[54] See eg Cornell Andrea, Mahan Sarina and Robin Riedel, *Commercial Drone Deliveries are Demonstrating Continued Momentum in 2023* (McKinsey and Company 2023).
[55] The main challenge lies in achieving a balance between optimising individual paths and optimising the system or infrastructure as a whole. Single-path planning, which aims to minimise factors like path length, energy consumption, and ground impact for a given origin–destination pair, has been extensively studied; Xinyu He, Lishuai Li, Yanfang Mo, Jianxiang Huang, S Joe Qin, 'A Distributed Route Network Planning Method with Congestion Pricing for Drone Delivery Services in Cities' (2024) 160 Transportation Research Part C: Emerging Technologies.
[56] ibid.
[57] Centralised planning can achieve system-level optimisation, but may also result in inefficiencies and inequities in the allocation of valuable urban airspace to individual paths; ibid.

commercial scale operations.[58] In these cases, congestion — the materialisation of tragedy of the commons phenomena — in low-altitude air will inevitably arise.[59]

In addition, Israel and China have recently already been preparing infrastructure for a national airspace network of large drones designed to carry passengers and heavy cargo[60] which will consequently lead to further congestion and, if not regulated, to the manifestation of tragedy of the commons phenomena. As an anecdotal example, one may note that in just the USA there are roughly 870,000 registered drones, which is four times the number of commercial and private planes.[61] Strikingly, about 350,000 of them are used for commercial purposes like inspecting railroad tracks, bridges and pipelines; the rest are recreational drones and within a couple of years urban air mobility companies also will begin testing their electric air taxis in several cities around the globe.[62] In fact, civil drones have often been reported as causing hazards to aircraft, or to people or property on the ground.[63] Safety concerns have been raised due to the potential for an ingested drone to rapidly disable an aircraft engine, and several near-misses and verified collisions have involved hobbyist drone operators flying in violation of aviation safety regulations.[64] Finally, one may also note a famous incident that happened in December 2015 when a civil drone filming a slalom event in Madonna di Campiglio nearly hit Marcel Hirscher.[65] Namely, while the International Ski Federation had agreed to use of the unmanned aerial vehicles (UAS), the pilot was not allowed to fly the drone directly over the race course.[66]

[58] Ruifeng She, Yanfeng Ouyang, 'Efficiency of UAS-based Last-mile Delivery under Congestion in Low-altitude Air' (2021) 122 Transportation Research Part C: Emerging Technologies.

[59] ibid.

[60] Sharon Wrobel, 'Drone Taxis Take First Test Spin in Israel in Bid to Ease Traffic Congestion' *The Times of Israel* (Tel Aviv, 6 June 2023) <https://www.timesofisrael.com/drone-taxis-take-first-test-spin-in-israel-in-bid-to-ease-traffic-congestion/> accessed 10 June 2024.

[61] Joann Mueller, 'Managing Traffic in the Skies is Becoming a Lot Harder' *Axios* (20 September 2021) <https://www.axios.com/2021/09/20/air-traffic-drones-airplanes-skies-crowded> accessed 10 June 2024.

[62] ibid.

[63] See eg John Pyrgies, 'The UASs Threat to Airport Security: Risk Analysis and Mitigation' (2019) 9 (2) Journal of Airline and Airport Management 63; and Dothang Truong and Woojin Choi 'Using Machine Learning Algorithms to Predict the Risk of Small Unmanned Aircraft System Violations in the National Airspace System' (2020) 86 Journal of Air Transport Management.

[64] See eg Julie Tellman 'First-ever recorded drone-hot air balloon collision prompts safety conversation' *Teton Valley News* (Teton Valley, 28 September 2018) <https://www.tetonvalleynews.net/news/drone-balloon-collision-prompts-safety-conversation/article_e08fc158-c269-11e8-904f-8b5d2e21fb4e.html> accessed 10 June 2024; Boise, Idaho, United States: Boise Post-Register, 'After Drone Hits Plane in Canada, New Fears About Air Safety' *The New York Times* (New York, 17 October 2017) <https://www.nytimes.com/2017/10/17/world/canada/canada-drone-plane.html> accessed 10 June 2014.

[65] Eric Willemsen, 'Ski Federation Bans Drones after Camera Nearly Hits Marcel Hirscher' *USA Today Sport* (23 December 2015) <https://eu.usatoday.com/story/sports/olympics/2015/12/23/ski-federation-ban-drones-marcel-hirscher/77838818/> accessed 6 May 2024.

[66] Camera UASs have since been banned from the Federation's World Cup races; ibid.

The lack of excludability in such instances thus creates incentives for the overexploitation of natural resources (air space in densely populated areas) and this leads to a reduction of social welfare as a whole. Extrapolation of these concepts of negative externality and the "tragedy of the commons" to the potential employment of automated civil drones enables us to argue that such unregulated employment might generate systemic negative externalities where the actions of drone operators affect bystanders, other drone operators and all other stakeholders in certain, generally densely populated, areas. The generator of the externality — an individual drone operator — who does not have to pay for harming others namely exercises too little self-restraint (an excessive number of drones in the air). He or she acts as if the cost of employing drones is zero, when in fact there are real costs involved (nuisance, noise, air congestion, potential hazards and harm, overcrowded air space, pollution etc.). The "tragedy of the commons" concept thus forms a prima facie argument for a legal intervention. This intervention may either employ classic ex post private law instruments (ie, property law) or ex ante regulatory intervention.

However, as we will show, the problem of prohibitively high transaction costs means the private law solution may be ineffective, with ex-ante regulatory intervention featuring as the only feasible solution. Namely, in the original formulation by Coase and North transaction costs are defined as "the cost of using the price mechanism" or "the cost of carrying out a transaction by means of an exchange on the open market".[67] Arrow, De Geest, Williamson and Parisi and Posner define transaction costs as the costs of running the economic system of exchange.[68] In the ideal world of zero transactions costs, parties would always efficiently bargain for the optimal allocation of scarce resources and the tragedy of the commons would never materialise. In such a world, the property rights system should namely act as an effective mechanism for mitigating the 'tragedy of the commons' problem and automatically regulating the employment of commercial drones. In the mentioned hypothetical world, landowners exclusively own and control the 'super-adjacent' low-altitude airspace directly above their land, and are free to commercialise and sell access to, or to prohibit drones from entering, their private airspace. As Ben Dor and Hoffmann argue, a marketplace will spontaneously emerge for parties to buy, sell and lease valuable airspace to accommodate drone delivery, such that companies like Amazon or Walmart will compensate landowners, even governments that own city streets and

[67] See Ronald Coase, "The Nature of the Firm" (1937) 4 (16) Econometrica386; Ronald Coase, "The Problem of Social Cost" (1960) 3 The Journal of Law and Economics 1; Ronald Coase R., *The Firm, the Market and the Law* (University of Chicago Press 1988); and Douglas C North, *Institutions, Institutional Change and Economic Performance* (Cambridge University Press 1990).

[68] See Kenneth J Arrow, "The Organization of Economic Activity: Issues Pertinent to the Choice of Market Versus Nonmarket Allocation" in *The Analysis and Evaluation of Public Expenditures: The PBB System, Joint Economic Committee Compendium* (Washington 1969); Gerrit De Geest, *Economische Analyse van het Contracten- en Quasi-contractenrecht* (Maklu 1994); Oliver Williamson, *Markets and Hierarchies* (Free Press 1975); and Francesco Parisi and Richard A Posner (eds), *The Coase Theorem* (Edward Elgar 2013).

highways, for the airspace where drones will one day fly.[69] However, such a solution based on market/property law relies on the assumption that transaction costs are trivial and requires parties to freely bargain.[70] Yet, in reality where for example an individual owner of 'super-adjacent' low-altitude airspace would have to negotiate with thousands of individual drone operators numerous contracts for the use of airspace (and related conditions) such transaction costs might actually be prohibitively high (preventing mutually beneficial transactions from materialising). The problem of non-trivial transaction costs actually renders such a market/property law-based solution ineffective (ie, private law failure) and calls for an ex-ante regulatory intervention.

3.2 Drone technologies and THE judgement-proof problem

A vital aspect of an effective regulatory approach to drones is the problem of automated drone technologies. Automated civil drones namely already have the ability to access and independently utilise their sensory motors to react to external conditions.[71] For example, in 2017 the Swiss start-up company Wingtra launched an autonomous agricultural surveying drone. With a total wingspan of 125 centimetres and total weight of 3.7 kilograms, the drone is incredibly small. It has a payload capacity of 800 grams and is capable of automated vertical take-off and landing. As shown, the property law alone might be inadequate for mitigating potential harms, hazards and other 'tragedy of the commons' linked problems. Here, one may turn to classic tort law mechanisms where

[69] They suggest that rather than sitting empty, the low altitude airspace should be commercialised through a marketplace in which landowners sell their consent to overflights over their properties. Delivery services and other heavy-duty drone operators can aggregate those consents into viable flight paths, and landowners can be compensated for the use of their airspace; Ben Dor and Hoffmann (n 8) 993.

[70] They also suggest that such a marketplace for airspace would only further innovation and commercial development while appropriately balancing the rights and concerns of individuals, businesses, and governments; ibid.

[71] Dario Floreano and Robert J Wood (n 1). See also Hassanalian and Abdelkefi (n 15).

indeed the existing tort law and economics literature[72] seeks to address the role of tort law and related civil liability for damage caused by such automated products.[73]

Nevertheless, automated drones may cause harm to others but their operators may not be unable to make victims whole for the harm incurred and might not have incentives for safety efforts created by standard tort law enforced through monetary sanctions. These phenomena, known in the law and economics literature as a the "judgement-proof problem", is a standard argument in law-making discussions while operationalising policies, doctrines and rules.[74]

A tortfeasor who cannot fully pay for the harms that they have caused and for which they have been found legally liable is namely said to be "judgement proof". Shavell shows that the existence of the judgement-proof problem seriously undermines the deterrence and insurance goals of tort law.[75] He notes that judgement-proof parties also do not have the appropriate incentive to prevent accidents or purchase liability insurance.[76] In other words, the judgement-proof problem is very important since if injurers are unable to pay fully for the harm they may cause, their incentives to engage in risky activities will be greater than otherwise. Summers also shows that the judgement-proof injurers tend to take too little precaution under strict liability because the costs of accidents are only partly internalised.[77] Accordingly, the classic debate on the two different means of controlling hazardous activities – *ex post* liability for harm done and *ex ante* safety regulation – may, due to the shortcomings of classic tort and contract law instruments,

[72] See eg, Alberto Galasso and Hong Luo, "Punishing Robots: Issues in the Economics of Tort Liability and Innovation in Artificial Intelligence" in Ajay Agrawal, Joshua Gans and Avi Goldfarb (eds), *The Economics of Artificial Intelligence: An Agenda* (University of Chicago Press 2019) 493, 504; Hans-Bernd Schaefer and Claus Ott, *The Economic Analysis of Civil Law* (Edward Elgar 2004) 107, 273; Michael Faure, "Toward a Harmonized Tort Law in Europe? An Economic Perspective" (2001) 8 (4) Maastricht Journal of European and Comparative Law 339; Hans-Bernd Schaefer, 'Tort Law: General' in Boudewijn Bouckaert and Gerrit De Geest Gerrit (eds), *Encyclopedia of Law and Economics* (Edward Elgar 2000) 569; Emons Winand and Joel Sobel, 'On the Effectiveness of Liability Rules when Agents are not Identical' (1991) 58 (2) Review of Economic Studies 375; Steven Shavell, *Economic Analysis of Accident Law* (Harvard University Press 1987); Mitchell Polinsky, and William P Rogerson, 'Product Liability, Consumer Misperceptions and Market Power' (1983) 14 (2) Bell Journal of Economics 581; Steven Shavell, "Strict Liability Versus Negligence" (1980) 9 (1) Journal of Legal Studies 1; Kenneth Arrow, 'Optimal Insurance and Generalized Deductibles' (1974) 1 Scandinavian Actuarial Journal 1; Richard Posner, 'A Theory of Negligence' (1972) 1 (1) Journal of Legal Studies 29; Richard Posner, 'Strict Liability: A Comment' (1973) 2 (1) Journal of Legal Studies 205; Guido Calabresi, 'Some Thoughts on Risk Distribution and the Law of Torts' (1961) 70 (4) Yale Law Journal 499; Guido Calabresi, 'The Decision for Accidents: An Approach to Non-fault Allocation of Costs' (1965) 78 (4) Harvard Law Review 713; and Guido Calabresi, *The Costs of Accidents: A Legal and Economic Analysis* (Yale University Press 1970).

[73] Aviation actually has specific rules for contractual and third-party liability as well as compulsory insurance. However, despite this, the main law and economics principles on tort law and economics are analytically applicable and informative also with respect to such specific rules.

[74] Steven Shavell, 'The Judgement Proof Problem' (1986) 6 (1) International Review of Law and Economics 45.

[75] ibid.

[76] John Summers, 'The Case of the Disappearing Defendant: An Economic Analysis' (1983) 132 University of Pennsylvania Law Review 145; and Steven Shavell, 'The Judgement Proof Problem (1986) 6 (1) International Review of Law and Economics 45.

[77] Summers (n 76).

boil down to the question of efficient *ex ante* regulation.[78] The problem is that if you have standing but you cannot represent yourself, society is effectively only left with regulation.

Law and economics literature offers several potential types of policy responses to address the identified judgement-proof problem. The first instrument is the introduction of vicarious liability.[79] Shavell, for example, suggests that if there is another party (principal) who has some control over the behaviour of the party whose assets are limited (agent), then the principal can be held vicariously liable for the losses caused by the agent.[80] Hence, vicarious liability (indirect reduction of risk) and a specific principal–agent relationship between the operator and their automated drone should be introduced. The operator (owner) should be held vicariously liable for the losses caused by the agent (automated drone). If the operator (principal) can observe the drone's (agent's) level of care then the imposition of vicarious liability will induce the principal to compel the agent to exercise optimal care. The extension of liability should in this way lead indirectly to a reduction of risk.

Yet, if the operator (owner) is unable to observe and control the drone's (agent's) level of care then he will generally not be able to induce the agent.[81] If, in contrast, the principal can control the agent's level of activity (and has no observation capacity) then such vicarious liability will induce the principal to reduce the agent's participation in risky activities.

However, what if a drone is indeed automated, self-learning, can develop emergent properties, can adapt its behaviour and actions to the environment? In these circumstances, the imposition of vicarious liability might be completely inadequate due to the extreme judgement-poof problem. Moreover, the product liability regime operates on the assumption that the product does not continue to change in an unpredictable manner once it has left the production line. Still, the new generation of drones may perhaps somewhere in future automatedly learn from their own variable experience and interact with their environment in unique and unforeseeable ways. In addition, companies also might be judgement-proof due to their size. In this scenario, law and economics suggests the introduction of a whole arsenal of economic/legal institutions that might address such an extreme drone operator's judgement-proof problem and continuous product changes.

[78] Patrick W Schmitz, 'On the Joint Use of Liability and Safety Regulation' (2000) 20 (3) International Review of Law and Economics 371.

[79] For a synthesis, see Alan Sykes, 'The Economics of Vicarious Liability' (1984) 93 (1) Yale Law Journal 168; and Reimer Kraakman, 'Vicarious and Corporate Civil Liability' in Gerrit De Geest and Boudewijn Bouckaert (eds), *Encyclopedia of Law and Economics, Volume II. Civil Law and Economics* (Edward Elgar 2000).

[80] Shavell (n 76). See also Steven Shavell, *Economic Analysis of Accident Law* (Harvard University Press 1987).

[81] Steven Shavell, *Foundations of Economic Analysis of Law* (Harvard University Press 2004) 180 *et seq*.

Law and economics scholarship has argued for the need to rethink legal remedies when applying them to AI-related torts.[82] For example, Shavell even claims that AI makes classic product liability law as currently designed is unable to create the optimal incentives for the use, production and adoption of safer AI technologies.[83] AI-related hazards are essentially unknown risks and the law and economics literature has addressed the problem of imposing liability for such unknown and unexpected risks and argues that whether "liability for unknown risks is desirable depends on what is more important: avoiding the marketing of products which are not safe enough, or not hindering the introduction of better new products".[84] Landes and Posner suggest that such liability might actually induce producers to invest in safer technologies.[85]

More recently, in their novel approach Guerra, Parisi and Pi state that AI-generated accidents should be clustered within the realm of "fault-based liability rather than product liability", where negligence-based rules should be blended with strict-liability rules to create precaution incentives for AI operators and their potential victims, and R&D incentives for manufacturers' development of safer AI.[86] They offer a novel liability regime, which they refer to as the "manufacturer residual liability" rule.[87] Under such a "manufacturer residual liability" regime, the primary liability is held by either the civil drone human operator or the victim, and the residual liability – the assignment of the accident cost when neither party is negligent – then falls on the manufacturer.[88] Namely, human operators and victims should bear accident losses attributable to their own negligent behaviour and manufacturers should only be held liable for non-negligent accidents. The negligence of the AI human operator also marks the boundary between a human operator's fault-based liability and the manufacturer's strict residual liability. Further, a manufacturer's liability would arise for two separate sources of accidents

[82] See eg Mark A Lemley and Bryan Casey, 'Remedies for Robots' (2019) 86 (5) The University of Chicago Law Review, 1311; and Eric Talley, 'Automators: How Should Accident Law Adapt to Autonomous Vehicles? Lessons from Law and Economics' [2019] Columbia Law School Working Papers Series No 19002.

[83] Steven Shavell, 'On the Redesign of Accident Liability for the World of Autonomous Vehicles' (2020) 49 (2) The Journal of Legal Studies 243.

[84] Michael Faure, Louis Visscher and Franziska Weber, "Liability for Unknown Risk – A Law and Economics Perspective" (2016) 7 (2) Journal of European Tort Law 198.

[85] William M Landes and Richard A Posner, "A Positive Economic Analysis of Products Liability" (1985) 14 The Journal of Legal Studies 535.

[86] Alice Guerra, Francesco Parisi and Daniel Pi, "Liability for Robots II: An Economic Analysis" (2021) 18 (4) Journal of Institutional Economics 553

[87] ibid 554.

[88] Such a liability regime makes operators and victims liable for accidents due to their negligence – hence, incentivising them to act diligently; and makes manufacturers residually liable for non-negligent accidents – thus incentivising them to make optimal investments in R&D for robots' safety. In turn, as Guerra, Parisi and Pi argue, such a rule would bring down the price of safer robots, driving unsafe technology out of the market and, due to the percolation effect of residual liability, would induce operators to adopt optimal activity levels in AI usage; ibid 554. See also Alice Guerra, Francesco Parisi and Daniel Pi, "Liability for Robots I: Legal Challenges" (2021) 18 (3) Journal of Institutional Economics 331

caused by AI: a) malfunctions;[89] and b) design limitations.[90] Finally, they show that such a liability regime might offer several advantages over simple negligence and strict liability, and might achieve four objectives of an AI tort law regime by inducing: a) efficient human precautionary care; b) efficient activity levels; c) investments in the R&D of safer AI; and d) the adoption of safer technology.[91]

In the author's previous work, several mechanisms were proposed to address such "judgement-proof" characteristics of existing legal persons (ie, manufacturers) and what follows is a brief summary of potential remedies: a) lawmakers could require any principal to have a certain minimum amount of assets in order to be allowed to engage in a completely automated drone-related activity; b) lawmakers could introduce the compulsory purchase of liability insurance coverage in order for any principal to be allowed to engage in an automated drone-related activity; c) lawmakers could directly *ex ante* regulate the drone's risk-creating behaviour (ie, regulatory agencies could *ex ante* set detailed standards for the behaviour, employment, operation and functioning of any automated drone); d) regulatory agencies could establish a detailed set of sector-specific safety standards (similar to those in the air travel or pharmaceutical industries); e) criminal liability for the human operator (ie, the principal) could be introduced to add pressure to optimise the principal's decision on whether to engage with the automated drone activity at all; f) lawmakers could extend liability from the actual injurer (the automated drone) to the company that engages or employs such a 'drone-agent'; g) lawmakers could establish a regime of compulsory compensation or a broad insurance fund for instances of catastrophic losses that is publicly and privately financed; and i) lawmakers could introduce the AI manufacturer's strict liability supplemented by the requirement that an unexcused violation of a statutory safety standard is negligence per se.[92]

[89] Malfunctions should be dealt with by ordinary product liability law already in place where victims may sue manufacturers directly or by allowing operators to sue manufacturers in subrogating when operators face direct liability under conventional tort law; ibid.

[90] Design limitations refer to accidents that occur when AI encounters a new unforeseen circumstance that causes it to behave in an undesired manner; ibid.

[91] ibid. In addition, Cooter and Porat offer a "total liability for excessive harm" rule for instances of multiple tortfeasors where officials can verify the total harm caused by all injurers but not the harm caused by an individual injurer. Under the mentioned rule, each individual injurer should be liable for the total harm that everyone causes in excess of the optimal harm. They suggest that a remarkable consequence of such a rule is that injurers respond to it by causing the optimal harm and their liability to be nil; Robert D Cooter and Ariel Porat, *Getting Incentives Right: Improving Torts, Contracts and Restitution* (Princeton University Press 2014) 74, 89. For example, an AI agency could establish a safety target and announce that each producer of AI systems in a certain area is liable for the damage caused by all producers of AI systems in excess of that target. As Cooter and Porat suggest, the agency gains control over the damages (ie, negative externalities) without having to monitor individual producers, while the producers do not have to pay damages or comply with bureaucratic regulations; ibid 74.

[92] See Mitja Kovac, *Judgement-Proof Robots and Artificial Intelligence: A Comparative Law and Economics Approach* (Palgrave Macmillan Springer Nature 2020); and Mitja Kovac, 'Autonomous Artificial Intelligence and Uncontemplated Hazards: Towards the Optimal Regulatory Framework' (2021) 13 (1) European Journal of Risk Regulation 94.

Further, lawmakers should also introduce corrective *ex ante* taxes that would equal the expected harm of drone usage.[93] The classic recommendation in economic literature for dealing with negative externalities is namely to tax the activity that produces them.[94] In our case, in order to deal with drone-related negative externalities (eg, air congestion), a lawmaker should introduce a tax on drone-related activity. The tax rate for each drone unit should be set equal to the estimated social costs created by such drone activity. By design, the firm (of an individual) operating drones and subject to such taxation will have to compare its tax costs (incurred if one employs a drone) with the costs of employing other, classical, non-flying means of transport, service, delivery and performance, or reducing its output or otherwise trying to reduce its activity level. If a net tax saving were generated by one of these measures, the firm (or individual) will adopt it; otherwise, it will pay the tax and employ the drone.[95]

This paper also suggests that regulation and tort law should be applied simultaneously. *Ex post* liability and *ex ante* regulation (safety standards) are generally viewed as substitutes for correcting externalities, and the usual recommendation is to employ the policy which leads to lower administrative costs. However, Schmitz shows that joint use of liability and regulation can enhance social wealth.[96] That is, regulation removes problems affecting liability, while liability limits the cost of regulation.[97] General regulatory standards should be settled on a lower level of care (lower than optimal) and combined with tort law instruments.[98] Namely, by introducing an *ex ante* regulatory standard, the principal and the agent (AI) might be prevented from taking low levels of precaution and might find the regulatory standard convenient despite the judgement-proof problem.

Moreover, an informed lawmaker should combine strict liability and vicarious liability — strict liability of the manufacturer and vicarious liability of the principal (principal as either a legal or physical person).[99] Nonetheless, since the product liability regime relies

[93] The aim of such Piguvian tax is not to raise revenue but to discourage the taxed activity, in the present instance the drone-related 'tragedy of the commons' phenomena. See eg Alan Barnett, 'The Pigouvian Tax Rule Under Monopoly' (1980) 70 (5) American Economic Review 1037; and Judith Freeman, 'Responsive Regulation, Risk, and Rules: Applying the Theory to Tax Practice' (2011) 44 (3) University of British Columbia Law Review 627.

[94] See eg Lans Bovenberg and Lawrence Goulder, 'Environmental Taxation and Regulation' in Alan Auerbach and Martin Feldstein (eds), *Handbook of Public Economics, Vol 3*. (Elsevier 2002) 1471; John Theeuwes, 'Regulation or Taxation' in Dirk Jan Kraanand Roeland J in 't Veld (eds), *Environmental Protection: Public or Private Choice. Economy & Environment* (Springer 1991); and Peter Salib, 'The Pigouvian Constitution' (2021) 88 (5) The University of Chicago Law Review 1081.

[95] See also Richard Posner, *Economic Analysis of Law* (8th edn Aspen 2011) 502.

[96] Schmitz (n 78).

[97] Susan Rose-Ackerman, 'Regulation and the Law of Torts' (1991) 81 (1) American Economic Review 54.

[98] Gerrit De Geest and Giuseppe Dari-Mattiacci, 'Soft Regulators, Tough Judges' (2007) 15 (1) Supreme Court Economic Review 119.

[99] Insightfully, similar shifts and balancing of liability can be observed in manned aviation where such a balancing of liability between contractual and non-contractual liability has been discussed. For example, in 1929 the Warsaw

on the assumption that the product does not continue to change in an unpredictable manner once it has left the production line, such a combination might not be adequate. Drone companies might also be judgement-proof due to their size. If one then employs the 'let the machine learn' concept, the argument that the designer should have foreseen the risk becomes harder to sustain. The classic debate on the two different means of controlling hazardous activities, namely *ex post* liability for harm done and *ex ante* safety regulation may, due to the identified shortcomings boil down to the question of efficient regulatory timing and *ex ante* regulation. A specific EU regulatory intervention might thus be considered that encompasses the following: a) the principal's minimum asset requirement needed to engage in an activity; b) compulsory purchase of liability insurance coverage (for the principal); c) direct ex ante regulation of drones' risk-creating behaviour — an EU regulatory agency setting behaviour-employment-operating-functioning standards; d) safety standards (albeit alone these are inadequate); and registration (for both principal and agent); e) the principal's criminal liability; f) extension of liability from the actual injurer (AI) to the company — piercing the veil of incorporation; g) corrective taxes equal to the expected harm; and h) establishment of an EU-wide publicly-privately-financed insurance fund.

3.3 Regulatory strategies and the economics of federalism

Sparrow suggests that for some risks responsibilities (regulatory advantages) might be held close by the regulator (the classic top-down approach) whereas for others where regulated entities have appropriate motivations and competences the regulator may delegate certain aspects of the control task to industry (information advantage and accountability).[100] For example, changes in regulatory strategy around the world have led to new forms of regulation: responsive regulation, self-regulation, performance-based regulation, command-and-control regulation, right-touch regulation, outcome-based regulation, light-touch regulation, really-responsive-regulation, co-regulation, incentive-based regulation, market-harnessing control regulation, regulation by contract, disclosure regulation (eg, by naming and shaming), direct action regulation, nudge-based regulation, rights and liabilities regulation, public compensation & social insurance model regulation etc.[101]

Convention was drafted to govern passenger liability in the case of death or bodily injury and a balance between protecting airlines from absolute liability (incentives to innovate) vs. ensuring passengers to be compensated was discussed.

[100] Of course, regulators have to know which parts of the task they may safely delegate, for which types of risk and in what conditions; Sparrow (n 42) 100.

[101] See Sparrow (n 42), and Baldwin and others (n 46).

Literature emphasises that the best regulatory outcomes will generally involve mixtures of institutions and instruments (hybrid types of regulation).[102] The problem of how to design the optimal mixes or to state in advance which institutions and instruments will work together effectively can nevertheless hardly be overstated.[103] Sparrow, for example, suggests that risk-based regulation (problem-solving) should be placed at the centre of regulatory policymaking and stresses the need to define problems precisely, to monitor and measure performance, and to adjust strategy based on performance assessment.[104] The 'really-responsive' regulatory approach requires that while designing and developing regulatory systems attention must be paid to five core matters: the behaviour, attitudes, and cultures of regulatory actors; the institutional settings of the different regulators; the different logics of regulatory tools and strategies (and their interaction); the regime's own performance over time; and changes in each of these elements.[105]

In addition, one may invoke the "economics of federalism" literature that discusses the optimal allocation of regulatory competence among national and supra-national regulators. All regulatory systems namely require a number of tasks to be performed and while performing all of these different tasks important structural issues arise in determining how these tasks are to be allocated to different institutions. The law and economics of federalism[106] actually inform us with respect to which institutional arrangements can assist the implementation of the public interest goals of regulation and the extent to which they offer protection against the subversion (politicisation) of the law to meet the demands of private interests. Further, the law and economics of federalism offer guidance on the question of whether the appropriate source of regulatory rule-making should be at Brussels or in Rome.[107]

Literature also suggests that the primary reasons in support of decentralisation are: the diverging preferences of citizens, information advantages on lower levels of government, accountability (ie, regulators should be answerable for the manner in which they exercise

[102] See eg Andy Murray and Colin Scott, 'Controlling the New Media: Hybrid Responses to New Forms of Power' (2002) 65 (4) Modern Law Review 491.

[103] See eg Neil Gunningham and Peter Grabosky, *Smart Regulation: Designing Environmental Policy* (Clarendon Press 1998) 422, 53.

[104] Sparrow also advocates the dynamic nature of the risk control game and targeting key problems and solve these by developing interventions; Malcolm Sparrow, *The Regulatory Craft: Controlling Risks, Solving Problems, and Managing Compliance* (Brookings Institution Press 2003).

[105] Moreover, regulatory design should take account of the detection of undesirable or non-compliant behaviour, developing tools and strategies for responding to that behaviour, enforcing those tools and strategies on the ground, assessing their success or failure, and modifying them accordingly; Baldwin and others (n 46) 159. See also Julia Black, 'Decentring Regulation: The Role of Regulation and Self-Regulation in a Post-Regulatory World' (2001) 54 (1) Current Legal Problems 103.

[106] See eg Ogus (n 26); and Jacques Pelkmans, 'The Assignment of Public Functions in Economics Integration' (1982) 21 (2) Journal of Common Market Studies 97.

[107] Robert Inman and Daniel Rubinfeld, 'Economics of Federalism' in Francesco Parisi (ed), *The Oxford Handbook of Law and Economics, Volume 3: Public Law and Legal Institutions* (Oxford University Press 2017) 84.

their powers), monopoly problems on the side of central government[108] and the importance of the learning process.[109] In relation to the optimal government levels, one may argue that local governments will possess better information than distant central government about local conditions and preferences and also greater incentives to satisfy them. Zoning should hence be typically left to local government (ie, Member States), while defence should be left to the central government (ie, EU Commission).

These findings may however also be implemented in the optimal regulatory design for civil drones. A combination of a local (EU Member State) law that clarifies landowners' property rights "by focusing on proxies that measure ever smaller classes of uses",[110] such as the further delineation of landowners' rights based on their location and local governance rules through municipal drone-zoning ordinances, may, as Watson suggest, therefore increase efficiency by filling in the gaps not currently addressed by the current EU MS property law aerial trespass doctrines.[111] For example, a certain MS or local municipality may find that drones should generally be excluded below 30 or 50 metres in urban areas, where parcel sizes tend to be relatively small and closer together, because the ability of drones to capture detailed images adds to the likelihood of invasions of privacy by drones or completely banned in natural resorts and parks due to their harmful effects on local flora and fauna. The statute would be efficient provided that it also gives local municipalities 'broad regulatory authority' to regulate drones below this level through its zoning powers.[112] Watson adds that this might be done by creating a cause of action in trespass for landowners, subject to the local drone-zoning ordinances that may allow certain uses of that space by drones — for example, an ordinance may distinguish between commercial and recreation drone uses and allow commercial drones to operate only during business hours on weekdays but limit recreational drone activity by prohibiting it altogether or to a narrower set of places and times.[113] As proposed by Watson, such a combination of exclusion rules on the state level and governance rules on the local level would reduce drone delivery activity in communities by restricting drone operations in certain locations and at certain times where drones have the potential to cause a nuisance or anxiety over the intrusion of privacy.[114]

[108] Donald Wittman, *Economic Foundation of Law and Organization* (Cambridge University Press 2006).
[109] See eg Wallace Oates, 'An Essay on Fiscal Federalism' (1999) 37 (3) Journal of Economic Literature 1120; Friederick A von Hayek, 'Competition as a Discovery Procedure' in Friederick von Hayek, *New Studies in Philosophy, Politics, Economics and the History of Idea* (University of Chicago Press 1978); and Charles M Tiebout, 'A Pure Theory of Local Expenditures' (1956) 64 (5) Journal of Political Economy 416.
[110] Henry E Smith, 'Exclusion Versus Governance: Two Strategies for Delineating Property Rights' (2002) 31 (S2) Journal of Legal Studies S453, S462, S463.
[111] Watson (n 20) 1434.
[112] ibid. See also William Fischel, *The Economics of Zoning Laws: A Property Rights Approach to American Land Use Controls* (Johns Hopkins University Press 1985) 22.
[113] ibid.
[114] Yet it would still allow companies and individuals to exploit the rising value of the airspace by implementing its drone delivery services in that community, which would benefit the community as well as companies and individuals; ibid.

Still, on the other hand, such a regulatory combination of different rules on the state level and on the local level might also entail considerable enforcement costs (i.e., transaction costs) for local communities that will have to enforce and monitor the application of different regulatory regimes and hence involve a very robust regulatory environment on both local and state levels. The estimation of such administrative and enforcement costs depends on the institutional quality and capacity and of course varies among different countries. One may even argue that such costs may in some countries even be prohibitively high since the employment of additional policing and administrative force is entailed, making the enforcement of such laws unfeasible in the short run. A potential way to overcome this problem, essentially one of transaction costs, is to introduce novel technical regulatory innovation such as an AI-run novel distributed route planning method to support UAS operations in a high-density urban environment.[115] This method for minimising transaction costs would for instance allow each origin–destination (OD) pair to compete against other OD pairs for an optimised route (e.g., shortest distance), coordinated by a system-level evaluation, leading to a network design that maximises the performance of not only the individual routes but also the entire system and in turn also addresses any tragedy of the commons problem.

hus, as shown, economic arguments do not always offer a clear-cut answer but offer an insightful tool-kit for finding economically informed set of suggestions that may improve the current regulatory mix of national and local regulatory competences. For example, law and economics principles suggest decentralisation (allocating regulatory competences for regulating drone activity) in instances where one is dealing with a larger number of states, increased diverging preferences across regions, information benefits at decentralisation decision levels, increased scope for innovation through regulatory competition and accountability issues. In other words, an ill-designed vertical division of powers undermines the conditions for economic growth, prosperity and peaceful coexistence.[116]

Ultimately, Ilman and Rubinfeld argue that the choice of an "optimal" level of decentralisation depends on the relative importance one ascribes to economic efficiency and the potentially competing values of political participation, economic fairness, and personal rights and liberties.[117]

[115] Xinyu He, Lishuai Li and others (n 55). See also Xinyu He, Fang He, Lishuai Li, Lei Zhang, Gang Xiao, "A Route Network Planning Method for Urban Air Delivery" (2022) 166 Transportation Research Part E: Logistics and Transportation Review; and Jacco M Hoekstra, Ronaldvan van Gent, Rob CJ Ruigrok, "Designing for Safety: the 'free flight' Air Traffic Management Concept" (2002) 75 (2) Reliability Engineering & System Safety 215.

[116] Roger Van den Bergh, 'The Subsidiarity Principle in European Community Law. Some Insights from Law and Economics' (1994) 1 (4) Maastricht Journal of European and Comparative Law 337; and Roger Van den Bergh, 'Economic Criteria for Applying the Subsidiarity Principle in the European Community: The Case of Competition Policy' (1996) 16 (3) International Review of Law and Economics 363.

[117] See Robert Inman and Daniel Rubinfeld, 'Rethinking Federalism' (1997) 11 (4) Journal of Economic Perspectives 43; and Inman and Rubinfeld (n 107).

4 Comment on the current EU and US legal frameworks

As described, to promote the widespread adoption of drones in the commercial space technological advancements and new regulatory frameworks are critical and solving the technical, regulatory and societal hurdles is essential to facilitate the advancement of commercial drone adoption. Moreover, ensuring that a regulatory framework is in place to support the nascent technology remains crucial for all who will be affected by the coming drone revolution.

All civil drones are presently defined as aircraft and fall within the general regulatory framework that governs aircraft. It must also be noted that alongside the general regulatory framework that governs aircraft there are currently also specific non-safety rules like contractual and third-party liability, insurance, security and environmental laws that also apply to civil drones as a special type of aircraft.[118] Today, the International Civil Aviation Organization (ICAO) classifies airspace into controlled and uncontrolled airspace using seven classes (A, B, C, D, E, F, G), depending on the air traffic services provided and flight requirements.[119] Controlled airspace covers classes A, B, C, D and E, while uncontrolled airspace covers classes F and G.[120] Each airspace class contains a set of rules indicating exactly how aircraft should fly and in which way ATC must interact with such aircraft.[121] Therefore, the ICAO defines each airspace class by the type of flight it services (instrument flight rules (IFR), visual flight rules (VFR)), provided separations (all aircraft, IFR flown aircraft from VFR flown aircraft, no separation), the type of air traffic service (ATC, traffic information about VFR flights, flight information service), speed limitation and altitude, radio communication requirements (continuous two-way, no communication) and ATC clearances.[122] As a regulatory body, the ICAO allows its member states to select airspace classes that fit their requirements.[123]

[118] In addition, all general rules such as the GDPR, human rights, product liability and AI Act also apply to drones.

[119] ICAO Annex 11 – Air Traffic Services, International Standards, Annex 11 to the Convention on International Civil Aviation (15th edn, Montréal Canada 2018).

[120] ibid.

[121] ibid.

[122] ibid.

[123] For example, in the United States (Fig. 1), controlled airspace consists of Class A and B airspace (where clearance from air traffic control is mandatory), Class C and D airspace (where two-way ATC communications are mandatory), and Class E airspace (where it is not mandatory to contact the ATC or obtain clearance to enter). These five classes are further divided by altitudes: Class A, between altitudes 18,000 and 60,000 ft above sea level; Class B, around the nation's busiest airports; Class C, around medium-sized airports; Class D, around smaller airports with air traffic control towers; and Class E, around smaller airports without air traffic control towers. Uncontrolled airspace, defined as Class G, is airspace below 1200 ft, not equipped with any air traffic management service, where pilots rely on visual flight rules (VFR). Class F airspace is not used. Within the classes of airspace, safety is preserved by maintaining a required separation between two aircraft; Federal Aviation Administration Pilot's Handbook of Aeronautical Knowledge FAA-H-8083-25B, Chapter 15: Airspace, Washington DC (2016). See also Alexasandar Bauranov and Jasenka Rakas, 'Designing Airspace for Urban Air Mobility: A Review of Concepts and Approaches' (2021) 125 (1) Progress in Aerospace Sciences.

To safely incorporate civil drones into the national airspace, many countries and regions around the world task agencies to issue aviation laws.[124] Examples include the FAA for the USA or the European Union Aviation Safety Agency (EASA) for the European Union (EU). Herman provides a national review and comparison of UAS regulations between the USA and Europe and find that, although civil drones regulations are categorised differently in each framework, eg, based on weight, maximum flight height, or operator experience and certification, both frameworks limit the weight of the UAS to approximately 55 pounds (25 kg) and prohibit the use of civil drones around people not involved in its operation.[125] For example Stöcker and others review different national drone regulations from the perspectives of past, present and future along with criteria such as applicability (scope), technical prerequisites[126] and find that almost all countries incorporate a maximum take-off mass, whereas only two countries introduce a minimum threshold in their regulations.[127] They also suggest that UASs heavier than "150 kg are not usually regulated by national aviation authorities but by international bodies like the EASA in Europe and tend to be regulated similarly as manned aircraft."[128] Mandourah and Hochmair also note that despite certain commonalities, such as mandatory portal registration, obligatory insurance coverage and pilot licensing procedures, there are considerable differences among national regulation, e.g., in terms of minimum distance requirements around people or airports, privacy policies, and insurance coverage.[129] In addition, Lee et al. in their comparative analysis establish that safety is a much more salient concern than privacy.[130] Further, safety is focused on the technical features of UASs, registration and certification, and differentiation by use case.[131]

The US congress legislated the recreational use of drones first in 2012 and then in 2015, where the Federal Aviation Administration (FAA) was mandated to register drones, including those for recreational use, due to the increasing number of drones and inherent threat of incidents and lack of collision insurance.[132] The FAA manages most of the

[124] Ammar Mandourah and Hartwig Hochmair, 'Analysing the Violation of Drone Regulations in Three VGI Drone Portals Across the US, the UK, and France' (2024) 27 (2) Geo-Spatial Information Science 364.

[125] Michele Herrmann, A Comparison of Unmanned Aerial Vehicle Regulations in the United States and Europe in *53rd ASC Annual International Conference* (Associated Schools of Construction 2017).

[126] For example, mandatory instruments, operational limitations (restrictions), application procedure, qualification of the pilot, and ethical constraints (eg, privacy and data protection regulations).

[127] Claudia Stöcker, Rohan Bennett, Francesco Nex, Markus Gerke, and Jaap Zevenbergen, 'Review of the Current State of UAS Regulations' (2017) 9 (5) Remote Sensing 459. See also Clarke (n 6), Harber (n 6), Suominen (n 6), and Ravich (n 6).

[128] All analysed countries except for China and Nigeria allow only low-altitude flights in the range between 90 m (Canada) and 152 m (Colombia) above ground level; Mandourah and Hochmair (n 124) 373.

[129] ibid.

[130] Lee Dasom, David J Hess, and Michiel A Heldeweg, 'Safety and Privacy Regulations for Unmanned Aerial Vehicles: A multiple Comparative Analysis' (2022) 71 Technology in Society.

[131] Whereas privacy regulations tend to follow broader digital privacy guidelines. Although there are some privacy rules that are UAS-specific, many of them do not yet directly address privacy challenges that are specific to UASs; ibid.

[132] Mandourah and Hochmair (n 124).

airspace in the United States and has recently outlined detailed regulations that every drone pilot operator in the USA must comply with. In short, the following regulations apply to both commercial and non-commercial (recreational) drone pilots: a) civil drones must fly at or below 400 feet (122m); b) all drones must be registered and should not weigh more than 55 pounds (25 kg); c) compulsory use of the B4UFLY Mobile App, a safety app from the FAA that uses a drone's GPS location to provide real-time information about airspace restrictions and other flying requirements; d) there are 'No Drone Zones' where civil drones are banned from the airspace;[133] e) civil drones may fly within the visual line of sight so that operator/observer can see the drone at all times; f) the drone operator must learn about airspace restrictions, especially around airports, so that the civil drone avoids potentially endangering people or other aircraft; g) civil drones can be flown without remote ID equipment within FAA-Recognised Identification Areas (FRIAs); and h) civil drones must give way to other aircraft and not interfere with other aircraft.[134]

On top of the general regulatory framework that governs aircraft and also applies to civil drones (alongside all other applicable legislation), following an informal agreement between the Council, the European Commission and the European Parliament in 2017 a new regulation (referred to as the "Basic Regulation") was adopted in 2018.[135] It extends the scope of the European aviation safety rules to all unmanned aircraft systems, regardless of weight. This regulation[136] sets the essential requirements applicable to unmanned aircraft and their engines, propellers, parts and non-installed equipment which should also cover matters relating to electromagnetic compatibility and the radio spectrum, in order to ensure that they do not cause harmful interference, that they use the radio spectrum effectively and that they support the efficient use of the radio spectrum. However, many types of aviation equipment are not necessarily intended

[133] The No Drone Zone includes: a) Restricted Airspace: The FAA prohibits drone flight over certain areas of airspace; b) Local Restrictions: In some locations, drone take-offs and landings are restricted by state, local, territorial, or tribal government agencies. The FAA has provided a No Drone Zone sign that can be used by these governments to identify areas where there are local flight restrictions. It is important to note that these No Drone Zones only restrict taking off or landing and do not restrict flight in the airspace above the identified area; and c) Temporary Flight Restrictions (TFRs) define a certain area of airspace where air travel is limited for a period and may be in place for different reasons. The FAA may use the term "No Drone Zone" to identify an area where there is a TFR. Examples include: major sporting events, space launch and re-entry operations, presidential movements, or in security-sensitive areas designated by federal agencies; Federal Aviation Administration, *Unmanned Aircraft Systems (UAS*), United States Department of Transportation 2024.

[134] ibid. See also Ravich (n 6).

[135] 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 996/2010, (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; OJ L 212 22.8.2018.

[136] Amended by EU Commission Delegated Regulation (EU) 2021/1087 of 7 April 2021 amending Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards updating the references to the provisions of the Chicago Convention.

specifically for use in either unmanned aircraft or in manned aircraft but could rather be used in both. Therefore, those requirements relating to electromagnetic compatibility and the radio spectrum should only apply from the moment that, and in as far as, the design of the unmanned aircraft and of their engines, propellers, parts and non-installed equipment are subject to certification in accordance with this Regulation. The reason for this is to ensure that the regime applicable to such aviation equipment is aligned with the regime applicable to other aircraft and their engines, propellers, parts and non-installed equipment in respect of which such certification is also required under this Regulation. Provisions on the design, production, maintenance and operation of drones and their engines, propellers, parts, non-installed equipment and equipment to control them remotely, as well as the personnel, including the remote pilots, security and organisations involved in those activities are in line with law and economics recommendations and hence fit into previously discussed framework. The establishment of the EU aviation safety agency and its certification, enforcement, control, monitoring and standardisation functions is also a very important step towards regulatory compliance and control of the employment and industry of drones.

In 2019, the Commission adopted two regulations on drone operations. Implementing Regulation (EU) 2019/947[137] on the rules and procedures for the operation of unmanned aircraft classifies drones in three categories: open, specific and certified. The open category includes drones up to 25 kg to be used mostly for leisure purposes, not needing prior authorisation. The specific and certified categories largely concern the professional use of drones, requiring due authorisation from the competent authorities. The regulation also covers conditions for maximum flight distance from the surface, and training and competency requirements for remote pilots. All of these provisions are in line with previously emphasised economic suggestions and thus fit into the optimal regulatory framework.

Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems includes the technical requirements for drones to be operated in the open category. According to the EASA, these regulations make Europe "the first region in the world to have a comprehensive set of rules ensuring safe, secure and sustainable operations of drones".[138] The Regulation also prescribes the requirements for the design and manufacture of unmanned aircraft systems (drones) intended to be operated under the rules and conditions defined in Implementing Regulation (EU) 2019/947 and of remote identification add-ons. It also defines the type of UAS whose design, production and maintenance is subject to

[137] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

[138] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems.

certification.[139] Further, Article 6 of this Regulation on the obligations of drone manufacturers provides that when placing their products on the EU market manufacturers shall ensure that it has been designed and manufactured in compliance with the requirements provided for in EU legislation, which in itself represents the highest standards of safety and strict product liability.[140] Article 40 also introduces special requirements — compulsory ex-ante certification — for drones operated in the "certified" and "specific" categories.[141] Such ex-ante requirements for compulsory certification, quality, design, security and maintenance control are all in line with law and economics recommendations and thus should be welcomed.

Finally, to ensure the safety of drone operations in airspace and their integration with manned aviation, in 2021 the Commission adopted a package of implementing regulations on U-space.[142] Implementing Regulation (EU) 2021/664 on a regulatory framework for U-space,[143] which lays down the technical and operational requirements for the U-space system. Implementing Regulation (EU) 2021/665 sets out common requirements for air traffic management and air navigation service providers to establish specific coordination procedures and communication facilities between air traffic service (ATS) units, U-space service providers and UAS operators.[144] Implementing Regulation (EU) 2021/666 establishes common rules for making the presence of manned aircraft operating in U-space airspace electronically visible. These provisions have applied since 26 January 2023.[145] From the law and economics perspective, all three of these regulations form a trajectory

[139] Moreover, it also establishes rules on making UAS intended for use in the "open" category and remote identification add-ons available on the market and on their free movement in the EU.

[140] For example, Article 38 of the Regulation states that, upon carrying out an evaluation of a drone, a Member State finds that, although the product is in compliance with this Regulation it presents a risk to the health or safety of persons or to other aspects of public interest protection covered by this Regulation, it shall require the relevant economic operator to take all appropriate measures to ensure that the product concerned, when placed on the market, no longer presents that risk, to withdraw the product from the market or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.

[141] The design, production and maintenance of drones shall be certified if the drones meets any of the following conditions: a) it has a characteristic dimension of 3 m or more, and is designed to be operated over assemblies of people; (b) it is designed for transporting people; (c) it is designed for the purpose of transporting dangerous goods and requiring a high level of robustness to mitigate the risks for third parties in the case of an accident; (d) it is used in the 'specific' category of operations defined in Article 5 of Implementing Regulation (EU) 2019/947 and the operational authorisation issued by the competent authority, following a risk assessment provided for in Article 11 of Implementing Regulation (EU) 2019/947, considers that the risk of the operation cannot be adequately mitigated without the certification of the UAS.

[142]The U-space is UAS geographical area designated by the EU Member States where only UAS operations supported by U-space services are permitted.

[143] Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space.

[144] Commission Implementing Regulation (EU) 2021/665 of 22 April 2021 amending Implementing Regulation (EU) 2017/373 as regards requirements for providers of air traffic management/air navigation services and other air traffic management network functions in the U-space airspace designated in controlled airspace.

[145] Commission Implementing Regulation (EU) 2021/666 of 22 April 2021 amending Regulation (EU) No 923/2012 as regards requirements for manned aviation operating in U-space airspace (Text with EEA relevance).

that leads toward an optimal regulatory framework and are in line with the previously mentioned law and economics insights.

In addition, one must mention the US FAA's Notice of Proposed Rulemaking on Remote Identification (remote ID) of Unmanned Aircraft Systems published on 31 December 2019.[146] This remote ID concept is a novel approach that facilitates drone integration into US airspace following the consideration of concerns related to safety, national security, and law enforcement by sharing drone information, such as drone identification, geographic coordinates, and altitudes for both the vehicle and its control station. A Standard Remote ID drone is produced with built-in remote ID broadcast capability in accordance with the remote ID rule's requirements. The final rule became effective in the USA on 16 March 2021, and in the EU on 1 July 2020.[147]

A brief comparison of US and EU regulatory approaches reveals that the EU regulations are very similar to the recently enacted FAA rules and should also provide a similar level of certainty to UAS operators. However, despite all of this economically enlightened (and highly welcomed) EU regulatory activity, which is as stated generally in line with the previously discussed economic insights, some additional improvements could be made on the EU level. First, as suggested by Guerra, Parisi and Pi, AI-operated-drone-generated accidents should be clustered within the realm of "fault-based liability rather than product liability", where negligence-based rules should be blended with strict-liability rules to create precaution incentives for drone operators and their potential victims, and R&D incentives for manufacturers' development of safer drone technologies – drone manufacturer residual liability.[148]

Moreover, alongside the previously surveyed regulatory requirements lawmakers could also introduce: a) the principal's minimum asset requirement needed to engage in a drone-related activity; b) compulsory purchase of liability insurance coverage (for the principal); c) the drone operator's (principal's) criminal liability; d) an extension of liability from the actual injurer (automated drone) to the company – piercing the veil of incorporation; and d) establishment of an EU-wide publicly-privately-financed insurance fund. All these policy measures are actually already implemented in other areas of current regulatory

[146] "Federal Aviation Administration – UAS Remote Identification Overview" <https://www.faa.gov/uas/getting_started/remote_id/> accessed 10 June 2024; and Yulei Wu, HongNing Dai, Hao Wang and Kim Kwang Raymond Choo, "Blockchain-Based Privacy Preservation for 5G-Enabled Drone Communications" (2021) 35 (1) IEEE Network 50.

[147] EASA. 2019a. "European Union Aviation Safety Agency – Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on Unmanned Aircraft Systems and on Third-Country Operators of Unmanned Aircraft Systems" Official Journal of the European Union 152 (June): 1–40. C/2019/1821, L; Dronesafe. 2019b. "European Union Aviation Safety Agency – Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the Rules and Procedures for the Operation of Unmanned Aircraft (Text with EEA Relevance)." Official Journal of the European Union 152 (June): 45–71. C/2019/3824, L.; "Federal Aviation Administration – Remote Identification of Unmanned Aircraft" Federal Register <https://www.federalregister.gov/documents/2021/01/15/2020-28948/remote-identification-of-unmanned-aircraft> accessed 10 June 2024.

[148] Guerra and others (n 88).

activity, since cargo carriage by air is a highly regulated industry with a specialized body of law and hence are in line with previously discussed economic suggestions. For example, current aviation liability rules are applicable also to drones, since drones are aircraft and are regulated as such. Namely, The Montreal Convention[149] governs contractual liability for international transport and in its Article 18 imposes liability on air cargo carriers (including drone operators) for the destruction, loss, or damage to cargo during international flight unless the destruction, loss, or damage is caused by something or someone else. Moreover, the Rome Convention[150] on third-party liability, is relevant also for drones and drone operators and imposes strict (but limited in accordance with Article 4 of the Rome Convention) liability to the drone operator which is according to Article 3 of the Rome Convention strictly liable for damage sustained by third parties upon condition only that the damage was caused by an aircraft (drone) in flight.[151] In addition, in line with economic suggestions international and EU law provisions already require compulsory insurance, which also covers drones and drone operators.[152] Hence, current international instruments and EU legislation already provides a sound legal environment

[149] The Montreal Convention also provides for additional limits on carrier liability, establishes formulas for calculating damages, and prevents carriers from limiting liability through contract. Additionally, and significantly, Article 29 bars all other claims, including state-law claims, when an action for damages falls within the substantive scope of one of three liability-creating provisions. So if Article 18 were to apply, for example, the Montreal Convention would be the exclusive instrument by which a claimant could seek redress for his or her damages; Convention for the Unification of Certain Rules for International Carriage by Air (the Montreal Convention) (OJ L 194, 18.7.2001).

[150] The Rome Convention was developed to provide internationally harmonious arrangements to ensure adequate compensation for persons who suffer damage caused on the ground by foreign aircraft, while limiting the extent of the liabilities incurred for such damage in order not to hinder the development of international civil air transport; Convention on Damage caused by Foreign Aircraft to Third Parties on the Surface, done at Rome on 7 October 1952.

[151] Article 6 of the Rome Convention also states that where two or more aircraft (drones) have been involved in an event causing damage to which the Rome Convention applies, the operators of those aircraft (drones) are jointly and severally liable for any damage suffered by a third party. If two or more drone operators are so liable, the recourse between them shall depend on their respective limits of liability and their contribution to the damage. Finally, according to Rome Convention no drone operator shall be liable for a sum in excess of the limit, if any, applicable to its liability.

[152] Compulsory insurance is for example introduced by Montreal Convention for the Unification of Certain Rules for International Carriage by Air and by specific EU regulations where air carriers (including drone operators) must be insured up to a sufficient level that is adequate for all persons entitled to compensation to receive the full amount to which they are entitled under the regulation; ensure that a summary of the main provisions governing liability for passengers and their baggage is available to passengers at all points of sale, including by telephone and via the internet. Montreal Convention in its Article 50 states that States Parties shall require their carriers to maintain adequate insurance covering their liability under the Montreal Convention. A carrier may be also required by the State Party into which it operates to furnish evidence that it maintains adequate insurance covering its liability under this Convention. Moreover, in 1997, the EU adopted Regulation (EC) No 2027/97 (on air carrier liability in the event of accidents) which imposes unlimited liability on EU air carriers in the event of death or injury to passengers. Regulation (EC) No 889/2002 amends Regulation (EC) No 2027/97 and applies the rules of the Montreal Convention (including compulsory insurance) to all flights, whether domestic or international, operated by EU air carriers. This new Regulation (EC) No 889/2002 of the European Parliament and of the Council of 13 May 2002 amending Council Regulation (EC) No 2027/97 on air carrier liability in the event of accidents in its Article 3 provides that the obligation of insurance set out in Article 7 of Regulation (EEC) No 2407/92 as far as it relates to liability for passengers shall be understood as requiring that a Community air carrier shall be insured up to a level that is adequate to ensure that all persons entitled to compensation receive the full amount to which they are entitled in accordance with this Regulation.

in relation to various liability issues, regulatory operational requirements and insurance mechanisms that are also in line with previously emphasized law and economics suggestions. Hence, one has to note that the economic discussion and application of general liability rules is greatly limited and emphasized shortcomings of general liability rules are already adequately addressed (mitigated) by these specific international instruments and EU rules.[153] In addition, also other general rules, such as GDPR,[154] and recently implemented EU AI Act,[155] also apply to drones.[156]

In order to tackle the problem of potential congestion, lawmakers could in addition to previously discussed legal instruments and technical solutions[157] also introduce corrective (Piguvian) *ex ante* taxes that would equal the expected harm of drone usage.[158] As discussed, in order to deal with drone-related negative externalities (e.g., air congestion) lawmakers should introduce a tax on drone-related activity. The tax rate for each drone unit should be set equal to the estimated social costs created by such drone activity (and aim to prevent the race to the bottom set at the EU level). By design, the firm (of an individual) operating drones and subject to such taxation will then have to compare its tax costs (incurred by employing a drone) with the costs of employing other, classical, non-flying means of transport, service, delivery and performance, or reducing its output or otherwise trying to reduce its activity level. If a net tax saving were generated by one

[153] Moreover, EU Commission published a proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence (the 'AI liability directive') in September 2022 which will, among other things, bring all types of software under the scope of the directive, both stand-alone and embedded, as well as digital services that affect the functionality of a product. This means that products such as drones, robots, navigation systems in cars and software in medical devices will be under Article 1 covered by this new Directive (COM(2022) 496 final, 28.9.2022). The Commission in this directive proposes to complement and modernise the EU liability framework to introduce new rules specific to damages caused by AI systems. The new rules intend to ensure that persons harmed by AI systems enjoy the same level of protection as persons harmed by other technologies in the EU. The AI liability directive would create a rebuttable 'presumption of causality', to ease the burden of proof for victims to establish damage caused by an AI system. It would furthermore give national courts in the EU the power to order disclosure of evidence about high-risk AI systems suspected of having caused damage. Stakeholders and academics are questioning, inter alia, the adequacy and effectiveness of the proposed liability regime, its coherence with the artificial intelligence act currently under negotiation, its potential detrimental impact on innovation, and the interplay between EU and national rules.

[154] 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).

[155] Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending certain Union Legislative Acts, COM/2021/206 final.

[156] All these rules complement our previous economic discussion and are adequately addressing other drone related issues (eg privacy and data protection, risks related issues).

[157] Technical solutions might restrict and govern the interactions between drones, objects, places and third parties. For example, low-risk drones may not be able to fly close to people and will be kept VLOS, whereas medium-risk drones might need to be authorised. Such authorisation will enable to precent drones flying close to people and property or will be restricted whereby nuisance will be considered.

[158] The aim of such Piguvian tax is not to raise revenue but to discourage the taxed activity, in the present instance the drone-related 'tragedy of the commons' phenomena. See eg Andy Barnett (n 93); and Judith Freeman (n 93).

of these measures, the firm (or individual) will adopt it; otherwise, it will pay the tax and employ the drone.[159]

Finally, a combination of a local (EU Member State) law that clarifies landowners' property rights "by focusing on proxies that measure ever smaller classes of uses", such as a further delineation of landowners' rights based on their location and local governance rules through municipal drone-zoning ordinances, may as shown, increase efficiency by filling in the gaps not addressed by the current MS property law aerial trespass doctrines.

In addition, the local municipalities should be given 'broad regulatory authority' to regulate drones below a certain level (e.g., 50 metres) through its zoning powers. As discussed, such a combination of exclusion rules on the state level and governance rules on the local level may then reduce drone delivery activity in communities by restricting drone operations in certain locations and at certain times where drones may potentially cause a nuisance or anxiety over the intrusion of privacy, protection of the environment, protection of cultural monuments and other broad social goals.

However, one should also note that the implementation of such a complex mix of regulatory policies and introduction of a complex hybrid regulatory system may entail considerable transaction costs (administrative, monitoring and enforcement costs) that may be even prohibitive and counterproductive. In other words, the proposed hybrid regulatory system requires a well-founded, human-capital intensive and very sophisticated institutional environment with highly skilled regulatory authorities and enforcement agencies capable of enforcing and implementing such a complex regulatory regime. In the absence of such a high-quality institutional environment, the implementation of complex hybrid regulatory system might actually induce uncertainty, increase transaction costs, consume a significant amount of resources (otherwise badly needed in other enforcement policies), overstretch the institutional capacity of regulatory agencies and end in a regulatory disaster (amplifying the tragedy of the commons and transaction costs problems).

To address these shortcomings, several potential remedies could be introduced. One potential remedy for such institutional restraints is for example the standardisation and simplification of certain regulatory approaches. For example, one could employ the previously mentioned concept of introducing a simple general rule that certain civil drones should be excluded below 30 or 50 metres in urban areas,[160] where parcel sizes tend to

[159] See also Richard Posner, *Economic Analysis of Law* (8th edn, Kluwer 2011) 502.

[160] For example, Amazon proposes that airspace below 500 feet be segregated into layers: a) Low-Speed, Localised Traffic – the area below 200 feet is reserved for applications such as recreation, surveying, inspection, surveillance, and videography, as well as low-tech aircraft without detect-and-avoid technology; b) High-speed transit – includes levels between 200 and 400 feet, and is reserved for well-equipped autonomous aircraft vehicles that operate beyond the line of sight. Technological capabilities required for this layer include detect-and-avoid capabilities, vehicle-to-vehicle (V2V) communication, and collision avoidance; c) No Fly Zone – is the area between 400 and 500 feet; and, d) predefined Low-Risk Locations – an area established by aviation authorities; Air, Amazon Prime. "Revising the airspace model for the safe integration of small unmanned aircraft systems." Amazon Prime Air 5 (2015): 36.

be relatively small and closer together, because flying in such low air space is simply too hazardous, often entails immediate congestion, and to capture detailed images adds to the likelihood of invasions of privacy by drones or completely banned around culture monuments, natural resorts and parks due to their harmful effects on local cultural heritage, flora and fauna. Yet, such a regulatory approach would be efficient provided that it also gives local municipalities 'broad regulatory authority' to regulate drones below this level through its zoning powers.[161] Some of the proposed solutions may also be implemented via existing regulatory mechanisms already employed to govern other social activities (e.g., taxation, education, private law enforcement). One may also argue that some regulatory enforcement can be done centrally at the EU level and that such regulatory proposals indeed also need serious improvements and capacity of the current institutional framework. Evidently, jurisdictions that will declare more no-fly zones will also need more code compliance officers or information campaigns to assure compliance with these restrictions.

Finally, one could introduce novel technical regulatory innovation[162] such as AI-run automatic enforcement and monitoring systems that would for example coordinate all civil drones in a certain area (preventing congestion and potential hazards from occurring) such as a novel distributed route planning method to support UAS operations in a high-density urban environment.[163] Namely, one may introduce automated AI air traffic management and control systems that should then be centralised and technologically able to accommodate, coordinate, monitor (and if needed enforce certain rules) all aircraft and all civil drones across a particular area on all levels of performance.[164]

The enforcement and compliance costs may be decreased further with the implementation of smart compliance and control mechanisms. For example, one may assess (and enforce) the compliance of the contribution to three drone image/video sharing portals (SkyPixel, DroneSpot, Flickr) with nationally and regionally issued restrictions. Mandourah and Hochmair suggest that using drone positions shared on crowd-

[161] As stated, this might be a done by creating a cause of action in trespass for landowners, subject to the local drone zoning ordinances that may allow certain uses of that space by drones – for example, an ordinance may distinguish between commercial and recreation drone uses and allow commercial drones to operate only during business hours on weekdays but limit recreational drone activity by prohibiting it altogether or to a narrower set of places and times.

[162] Namely, the inability of the current air traffic management (ATM) system to manage urban airspace is seen in the transportation literature as the primary inhibitor of the development of urban air transportation. Several challenges impede the integration of the existing NAS operations and urban operations: 1) higher number of operations, 2) greater density of operations, 3) lower altitudes of operations, and 4) varying performance of different operators and air vehicles; Bauranov and Rakas (n 123).

[163] Xinyu He and others (n 55), Xinyu He and others (n 115); and Hoekstra and others (n 115).

[164] Alternatively, one could also envisage autonomous civil drones technically equipped and having capacity to select their preferred routes while maintaining safety with onboard technology, such as sense-and-avoid, avoiding congestion etc. See eg Euclides Carlos Pinto Neto, Derick Moreira Baum, Jorge Rady de Almeida Júnior, João Battista Camargo Junior and Paulo Sérgio Cugnasca, "Trajectory-Based Urban Air Mobility (UAM) Operations Simulator (TUS)" (2019) abs/1908.08651 ArXiv.

sourced photo portals gives access to a new source of spatio-temporal data, which can be used to analyse violations of drone regulations even before any incidents occur.[165] Crowd-sourcing portals are only one source of geotagged data that is actively shared by the Web community, which is often referred to as Volunteered Geographic Information (VGI).[166]

5 Conclusions

The drone's applicability for military, scientific, leisure and commercial uses and its capability to deliver packages and transport goods more efficiently and quickly than ever before is revolutionising our everyday way of life. Legislators, landowners and businesses are exploring their future roles in the commercialisation of low-altitude airspace whereas European legislature has already produced an impressive number of regulatory interventions.

This paper seeks to show that the combined problem of prohibitively high transaction costs and tragedy of the commons phenomena might make the operation of classic property and contract law instruments (eg, trespassing and contracting between the space owners and drone operators) inadequate for addressing the growing use of automated civil drones and not to inhibit the related technological innovation and progress brought by drones. While recognising the merits of the novel European regulatory activity, the paper lists additional recommendations to ensure an improved regulatory intervention covering potential, uncontemplated civil drones-related hazards.

As highlighted in addition to discussed international legal instruments, different EU and national law provisions lawmakers may introduce also corrective ex-ante taxation that would equal the expected negative externalities (nuisance, congestion, cultural & environmental hazards etc.) of drone employment, the principal's minimum asset requirement needed to engage in a drone-related activity, extension of liability from the actual injurer (automated drone) to the company — piercing the veil of incorporation; establishment of an EU-wide publicly-privately-financed insurance fund; and of specific drone manufacturer residual liability. Local governments (municipalities) may also be given specific 'broad regulatory authority' that would clarify landowners' property rights to regulate the use of drones below a certain level (eg, 50 metres) through their zoning powers so as to mitigate the high-transaction-cost and tragedy of the commons problems. An improved regulatory regime should namely help the unmanned flight industry flourish by adopting an approach that ensures airspace safety while respecting landowners, drone operators, and the public alike and by recognising the value of both EU and local oversight of the skies.

[165] Mandourah and Hochmair (n 124).

[166] Michael F Goodchild, 'Citizens as Voluntary Sensors: Spatial Data Infrastructure in the World of Web 2.0' (2007) 2 International Journal of Spatial Data Infrastructures Research 24.

Journal of Law, Market & Innovation

ISSN: 2785-7867

https://www.ojs.unito.it/index.php/JLMI
email: editors.jlmi@iuse.it

The JLMI is edited as part of the
Open Access online scientific journals of
the University of Turin
Via Verdi 8, 10124
Turin, Italy

Vol. 3 - 2/2024