Responsible Design of Drones and Drone Services

Legal Perspective

Synthetic Report

Haomiao Du & Michiel A. Heldeweg
July 2017

Table of Contents

Executive Summary

- The term "drone" is the common language of all types of aircraft without a pilot on board and their ancillary components, such as a control station, if applicable. In addition to the common term "drone", other terms and acronyms, among others, Unmanned Aerial Vehicles (UAV), Unmanned Aircraft (UA), Pilotless Aircraft and Unmanned Aircraft System (UAS) are also widely used in publications.
- In the past 5 years, drones have demonstrated significant growth in civil market as not only a leisure product but also a tool which can provide professional services. Professional uses of drones include, among others, agricultural services, surveillance, search and rescue, monitoring and inspection, parcel delivery and picturing and filming. Compared to conducting those services above by manpower, drones provide services in higher efficiency and accuracy, decrease the cost of actions, and expand the accessibility.
- The deployment of drones has impacts on individuals, the society and the environment. The potential threat to aviation safety as well as the safety of persons and properties on the ground is a central issue. In addition, given that drones are very often equipped with cameras and sensors, the potential violation to personal privacy and data protection by drone users is the major barrier that hinders the public acceptance of drone applications.
- Drone operations are subject to relevant rules under civil aviation laws, because the flying of drone should comply with civil aviation laws in order to ensure aviation safety in a shared airspace with manned aircraft. Also, principles under data protection laws and personal privacy laws are also applicable to drones, as long as any type of drone operation would impact on personal and data privacy. Regulations on drones and drone operations predominantly focus on safety issues, but the implications of drones on the society and individuals are largely overlooked, albeit some general calls on the compliance with existing principles and rules contained in privacy and environmental protection regimes.
- Specific regulations on the design and production of drones and on drone operations are not yet available in many countries, in particular developing countries. In addition, due to the lack of international standards on designing and operating drones or the mutual recognition of national drone regulations, even if one country had its domestic regulation on drones and drone operations, problems would still arise when a drone is designed in accordance with one country's regulation and cannot be operated in another country because of the inconsistent regulations. The lack of specific regulations and the lack of shared standards hinder the increasing market of drone services, and very often result in a prohibition of or highly restricted drone operations.
- Regarding the future regulation on drones, the major objectives of regulating unmanned aircraft are: ensuring the safety of the civil aviation and integrating unmanned aircraft into air traffic regulatory systems; protecting the right of privacy and protecting data, and enabling the development of drone technology and promoting the market of civilian use of drones.
- A topic that has been widely addressed among scholars is how to deal with the dilemma between promoting technological innovation and controlling the adverse impacts arising from the deployment of a new technology on individuals as well as on the society. The challenge lies in how to make proactive and future-proof regulation which can respond to rapid technological development in a more legitimate, effective and efficient manner. The principle-based regulatory approach has the advantages of avoiding regulatory completion and can provides a greater degree of openness and flexibility, allowing for future revisions in the regulatory regimes based on new knowledge. In

addition, the proactive and future-proof regulation can be achieved by decreasing the binding effect of regulation.

- Diverse key players (develops, users, pilots, etc.) in the arena of drone design and services shape their behaviour by complying with current laws and regulations. Key players could meanwhile actively keep communication with regulators and legislators and inform them the problems they encounter during their compliance with current rules and regulations. Also, key players could propose their possible solutions to such problems. The interaction between regulators and key players, in particular developers and operators, should be an iterative process. Also, it is significant to facilitate and promote close collaboration and interaction between engineers and rule-makers.
- The present report proposes a framework consisting of four regulatory approaches for regulators to respond to different types of threats and concerns associated with drone design and operations. The four approaches are: designed-in regulations via technical measures (or called techno-regulations), risk assessment, communication and public participation, and the precautionary approach. Techno-regulations can be widely applied to the threats that can be eliminated from the beginning. Risk assessment is an approach to evaluate risks and find risk mitigation methods, when a threat cannot be prevented from the beginning. Risk assessment covers a series of procedures to deal with complex risks. Communication and public participation are specially applied by public authorities to solve the problem of chilling effect. The precautionary approach refers to a range of regulatory measures which aim to avoid significantly or seriously adverse impact regardless of the availability of decisive evidence. The precautionary approach is applicable when scientific uncertainty is the major concern and a risk of serious or significant harm is compelling.
- The present report recommends, among others, that in order to design and deploy drones in a responsible manner, ethical values should always be embedded into technological innovations. In addition, the notion of precaution should be embedded into designer and developers' mindsets. Moreover, making decisions in a transparent and participatory environment is the key to correct misperception and towards the public's acceptance of a new technology in the society.

List of Tables and Figures

List of Acronyms

ATM	Air Traffic Management
CAAC	Civil Aviation Administration of China
CNS	Communication, Navigation and Surveillance
EASA	European Aviation Safety Agency
FAA	Federal Aviation Administration
GALLO	Guidance for an Authorisation for Low Level Operation of RPAS
GDPR	General Data Protection Regulation of the EU
ICAO	International Civil Aviation Organization
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
RPAS	Remotely Piloted Aircraft System
SESARJU	Single European Sky ATM Research Joint Undertaking
SORA	Specific Operational Risk Assessment
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicles
VFR	Visual Flight Rules
VLOS	Visual Line of Sight

This Report

This report is about the legal aspects of responsible drone development and use, to underpin the making of a tool towards such development and use. The report is structured as follows. First, in Section 1, basic scientific aspects of drone technology are introduced. This involves defining drones as object of study (in Section 1.1), and a concise discussion of both drone development and uses (in Section 1.2) and of potential impacts (in Section 1.3). Next, in Section 2, an overview is presented of key types of laws and regulations regarding the design and the operation of drones, across various jurisdictions: international (in Section 2.1), supranational (in Section 2.2), national (in Section 2.3) and transnational (in Section 2.4). Then, Section 3 is about the underlying principles, rules and regulations applicable to the implications of the use of drones on individuals, the society and the environment. Based on Sections 1-3, Section 4 identifies remaining challenges and provides reflections on the current proposals for future regulatory framework. Sections 5 proposes an integrated process for key players in the field of drone design and operation to comply with rules and regulations and to deal with the situation of non-compliance. Section 6 proposes a regulatory framework which includes four major regulatory approaches to responding to different threats or concerns. In the end, Section 7 provides conclusions and recommendations.

1 Background

As a first order of things we will provide a definition of drones and explain this report's focus on one particular type of drone (Section 1.1). Next (in Section 1.2) we will provide an overview of the main developments and uses of this type of drone. Against this backdrop the main concerns, as burdens and threats of drone development and use are listed (in Section 1.3).

1.1 The Definition of "Drone"

The term "drone" is the common language of all types of aircraft[1] which are operated with no pilot on board, and their ancillary components, such as a control station, if applicable. In addition to "drone", other terms and acronyms are also used in a wide range of scientific publications and regulatory documents. The common examples are Unmanned Aerial Vehicles (UAV), Unmanned Aircraft (UA), Pilotless Aircraft and Unmanned Aircraft System (UAS). Although those terms are in principle interchangeable, different aviation authorities have their own preference. For instance, the International Civil Aviation Organization (ICAO) uses the "pilotless aircraft", while the US Federal Aviation Administration (FAA) and the European Aviation Safety Agency (EASA) use the term "UAS". The terms UAV, UA and Pilotless Aircraft refer to *an aircraft* which is operated with no pilot on board. Regarding UAS, the additional word "system" refers to the *ancillary components* (control station, command and control date link, etc.) as opposed to the aircraft component.

Within the scope of drones, there are two major modalities: drones remotely piloted from another place (Remotely Piloted Aircraft System (RPAS)), or programmed and fully autonomous drones.[2] A drone can also be a combination of both modalities. To avoid any

[1] Different types of aircraft include aeroplanes (fixed wing), airships (lighter than air) and helicopters (rotary wing).
[2] ICAO. (2011). Unmanned Aircraft Systems (UAS), Cir. 328, Glossary. Retrieved from http://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf (Accessed on 8 March 2017)

confusion, the present report uses the term "drone" as an overarching concept to cover all relevant modalities and components, and also refers to those abovementioned acronyms insofar as existing laws and regulations use any specific ones.

1.2 An Overview of the Development and the Uses of Non-Military Drones

1.2.1 The Development of Non-Military Drones

Drones have been used for military purposes, such as reconnaissance, intelligence and attacks, for decades. In the recent five years, thanks to the versatility and the affordable price, drones have demonstrated significant growth in civil market as not only a leisure product but also a tool which can provide professional services. It is predicted that, in the EU, drone marketplace will generate the value of more than 5 billion Euro by 2035, and more than 400,000 drones will be used for governmental and commercial missions in 2050.[3]

The increasingly growing demand of drones within the market also stimulates investment into developing drone-related technology, gaining drone-related knowledge and promoting drone-related innovative business. The Netherlands is one of the leading players in the development of drone technology. For instance, Space 53, locating at Twente Airport, is the unique testing area in western Europe that brings together public and private partners both domestically and internationally for testing, training and developing unmanned systems.[4] Twente Airport in Enschede, the Netherlands has been taking initiatives in providing facilities for testing drones and simulating unmanned air traffic systems. In addition, universities, research institutes, governmental departments and entrepreneurs in the Netherlands are cooperating in testing and developing drone technology and dealing with safety and security implications with a view to promoting the responsible design and use of drones.[5]

1.2.2 Non-Military Uses of Drones

The term "non-military" refers to civil uses and state/public uses. Notably, a drone cannot be considered civil aircraft when it is used for police services.[6] According to Art. 3.1 (b) of Chicago Convention, "[a]ircraft used in military, customs and police services shall be deemed to be state aircraft", which is opposite to civil aircraft. Hence, the use of drones described in this Section is phrased as "non-military use".

The advantage of using drones is that they perform certain tasks more efficiently and accurately than human beings and traditional devices. More importantly, drones are able to carry out tasks

---

[3] EASA. (2015). Roadmap for drone operations in the European Union (EU) The roll-out of the EU operation centric approach, retrieved from http://rpas-regulations.com/wp-content/uploads/2016/07/EASA_EU-Roadmap-Operation-Centric-Approach-Drone-Ops-v13_160620.pdf (Accessed on 10 November 2016)

[4] Space 53. Retrieved from http://www.space53.nl/

[5] The University of Twente, Twente Safety and Security, Netherlands Aerospace Centre (NLR), Dutch Brandweer (fire brigade) and Nokia are, for instance, the actors involved in the cooperation. In addition, TU Delft and TU Eindhoven also have their drone research team working on ambulance drones and domestic drones respectively. Retrieved from https://www.tudelft.nl/en/ide/research/research-labs/applied-labs/ambulance-drone/ and https://www.bluejayeindhoven.nl/ (Accessed on 7 July 2017).

[6] Convention on International Civil Aviation, Chicago, adopted 7 December 1944, entered into force 4 April 1947, *United Nations Treaty Series* (1948), vol. 5, no. 102, p.295 (hereafter "Chicago Convention").

at places which are inaccessible to human beings. Specifically, drones are being used increasingly in a wide range of fields, which include but are not limited to[7]:

- Agricultural Services

Drones can be used for a wide variety of agricultural services, ranging from precisely spraying pesticides and fertilizers, monitoring crops growth, estimating yields to detecting and mitigating disease. Compared with conventional airplanes, drones are suitable for all sizes of crop fields and farms and are expected to provide more accurate and efficient services. For instance, in November 2015, DJI, a world-leading company in innovating and producing drones, launched a crop-spraying agriculture drone which can load 10 kilograms of liquid for spraying and can cover between 7 to 10 acres per hours. Such a performance is over 40 times more efficient than manual spraying.[8]

- Inspection and Monitoring

Drones are used for various types of inspections, such as for infrastructures, pipelines and the atmosphere. The main advantages of using drones are they are much less costly and can avoid human beings from undertaking inspections in dangerous places. For instance, a few European Universities have been working on the development of autonomous drones for the inspection and maintenance of wind turbines and incinerators. At the moment, such maintenance and inspection work is still carried out manually, which is costly for farms and sometimes dangerous for workers due to the high altitude, or high temperature and humidity. The autonomous drones designed for inspecting and maintaining mega incinerators are fitted with an arm for removing deposits resulting from incineration as well as abrading the exposed surface beneath.[9]

Drones could play a significant role in monitoring wind turbines, highways, natural resources, wild lives, natural disasters, etc. An interesting example is the so-called "Robirds", which are remotely controlled robotic birds of prey with the realistic appearance of birds and a flight performance comparable to real birds.[10] Robirds are utilised for bird control in airports, crop fields, harbours, etc. Two types of Robirds, falcon and eagle, are available for chasing off birds up to 3 kilograms and birds in any sizes respectively.[11]

- Surveillance

Non-military drones have been widely used for surveillance and law enforcement activities undertaken by governmental authorities, in particular police and intelligence agencies. Such activities include, for instance, monitoring public events, border controls against illegal

---

[7] Regarding an introduction to the types of drone services, see, e.g. Mohammed, F., Idries, A., Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2014). UAVs forsmart cities: Opportunities and challenges. Paper presented at the Unmanned Aircraft Systems (ICUAS), 2014 Conference.
[8] DJI Introduces Company's First Agriculture Drone, retrieved from: https://www.dji.com/newsroom/news/dji-introduces-company-s-first-agriculture-drone
[9] Drone experts gather in Twente AEROWORKS: Drones for inspection and maintenance of wind turbines and incinerators, retrieved from: https://www.utwente.nl/en/news/!/2016/5/5334/drone-experts-gather-in-twente (Accessed on 10 November 2016)
[10] Robirds, retrieved from: http://clearflightsolutions.com/methods/robirds (Accessed on 10 November 2016)
[11] Ibid.

cultivation and investigation of crimes. Surveillance drones are often equipped with cameras and sensors for observation and data collection. In addition to continuously collecting tremendous amount of information in wide areas, surveillance drones may also be able to identify signals, objects and people, and to report the information which is considered abnormal.[12]

- Search and Secure (SAR)

SAR drones are utilised for searching and providing aid to people that are in distress or imminent danger. For instance, SAR drones can provide rapid and highly efficient services after an earthquake. SAR drones are able to search victims in an extensive area within a very short period of time and, depending on the load capability, possibly supply stranded victims with water and medicines, thereby winning time for rescue crew. Another application of drones relating to SAR is that small autonomous drones can be sent prior to SAR crew to an unfamiliar architecture for exploring and memorising the structure of the architecture, and then fly back to the entrance to guide SAR crew in the architecture.

- Picturing and Filming

Installed cameras enable drones to take pictures and films for construction planning, geo-mapping and entertainment industry. Drones are used in construction and infrastructure asset management to capture images and to collect data. Until now, manual planning and documenting can only be done on the ground, and hiring helicopters to take images is to costly or logistically impossible due to airspace restrictions. In comparison, small drones can fly lower and closer to objects than helicopters and are able to take very detailed pictures, though they are also required to abide by relevant rules and regulation.[13] Regarding geo-mapping, the advantages of using drones are similar with the case of construction planning and documenting. Without doubt, the use of drones greatly expands the creativity of photo-shooting and filming.

- Parcel Delivery

The idea of using drones for delivering parcels was initiated by Amazon, a U.S. e-commerce giant, with an aim to largely saving delivery cost and increasing working efficiency. In December 2016, Amazon air delivery, for the first time, has been completed in the UK. In China, parcel delivery by drones is expected to largely improve the efficiency and decrease the cost of delivery in rural areas, in particular mountainous and hilly areas. Instead of transporting parcels manually through hundreds of kilometres, postmen merely wait at the drop-off points to collect parcels and then deliver them to individuals.

1.3 Potential Impacts of the Use of Drones

1.3.1 Safety and Security Issues

[12] Security and surveillance, retrieved from http://www.droneconvention.eu/security-and-surveillance.html (Accessed on 10 November 2016)

[13] Rules and regulations related to small drones will be further discussed in Section 3.

Safety concerns refer to the safety of airspace as well as the safety of persons and properties on the ground.[14] First, the flying of drones creates the risk of collision with other drones or manned aircraft. In particular, when a drone flies to the vicinity of aerodromes, the likelihood of collision with other aircraft greatly increases. Second, the flying of drones at a low altitude or the accidental crashes of drones create a risk of damaging static objects, such as buildings, as well as injuries to people.

The flying of drones arises safety concerns due to various reasons: pilot's mistake, technical malfunction (low battery), extreme weather, etc. As drones, in particular small drones have very limited capabilities to maintain the stability and function during extreme weather, such as strong wind and heavy rain, crashes and other damaging consequences would be inevitable. Notably, safety concerns arising from different reasons above may be treated differently by laws and regulations.[15]

The use of drones also challenges the existing air traffic management (ATM) system. Considering the fact that an UAS traffic management system or an integrated ATM system for both manned and unmanned aerial vehicles are still under development,[16] the concern about the safe management of diverse utilisation of drones in the low-altitude airspace will still last. The future system would require, among others, the improvement of communication, navigation and surveillance (CNS), which are essential components of the ATM system for both pilots and air traffic controllers on the ground.[17] In the EU, the Single European Sky ATM Research Joint Undertaking (SESARJU) is a public-private partnership established responsible for the modernisation of the European air traffic management (ATM) system by coordinating and concentrating all ATM relevant research and innovation efforts in the EU.[18] In July 2016, SESARJU launched a call for exploratory research projects on the integration of drones into civil airspace.

Security concerns refer to, among others, the risk of losing the information captured by drones, and the panic of people on the ground. The security concerns in this Section are cross-cutting issues with privacy and data protection, and will be elaborated in corresponding Sections later.

1.3.2 Privacy Issues

Although surveillance drones ought to be utilised for safeguarding the public, it is often criticized that such drones pose a risk of violating the right of privacy. Despite the fact that surveillance by drones shares commonality with CCTV surveillance or police helicopter, drones

---

[14] TNO (2016), Final Report: Technical Aspects Concerning the Safe and Secure Use of Drones. Retrieved from https://www.thehaguesecuritydelta.com/uavs-drones (Accessed on 10 November 2016)
[15] It will be addressed in Section 6. Possible approaches include embedding restriction into the design of drones (techno-regulations) and eduating pilots and operators.
[16] For instance, NASA is leading the research on developing a possible future unmanned traffic system that could safely enable low-altitude airspace and UAS operations. Retrieved from https://utm.arc.nasa.gov/ (Accessed on 5 March 2017)
[17] Communication, navigation and surveillance. Retrieved from http://www.eurocontrol.int/dossiers/communications-navigation-and-surveillance (Accessed on 5 March 2017)
[18] SESAR. (2016). Call launched for exploratory research projects on the integration of drones into civil airspace. Retrieved from http://www.sesarju.eu/newsroom/all-news/call-launched-exploratory-research-projects-drone-integration-civil-airspace (Accessed on 5 March 2017)

still have their distinct features. First, the relative invisibility of drones makes individuals unable to know when and where they are monitored. Under this circumstance, individuals assume that they are all the time monitored and thus would change their behaviour in order to avoid any legal repercussions, which is described as the "chilling effect". The chilling entails the inhibition or discouragement of legitimate exercise of civil liberties and rights, because of the threat of lawsuit, prosecution or sanction.[19] Such a chilling effect would also impede the acceptance of surveillance drones by the society. Second, drones can observe much wider areas than CCTV cameras, even amounting to an entire city (with special cameras equipped). Moreover, it is also possible for drones to obverse much more in detail than CCTV, even a private garden or the interior of a house. Third, a variety of advanced sensors, such as GPA tracker and biometric sensors, available to be equipped on drones largely proliferate the capabilities of drones. Those sensors enable drones to undertake tracking observation of a certain person covertly, and to further collect information about the group membership and affiliation of this person.[20]

The use of drones for business, journalism and other non-surveillance purposes also generates privacy concern. For instance, filming and photographing activities undertaken by companies and journalists for the purposes of monitoring a business competitor or observing celebrities. It has even been argued that, compared to public surveillance, the use of drones in private sectors and citizens will likely pose the greatest threat to privacy.[21]

In sum, for both surveillance or non-surveillance purposes, the use of drones generates unprecedented privacy problems which is not analogous with the privacy problems generated by CCTV systems. Depending on the equipment outfitted on a drone, privacy concerns may include personal data and image, people's location and their tracks, the group membership and affiliation of a person, etc.[22]

1.3.3 Data Protection Issues

Data protection is a cross-cutting topic which has overlaps with security issue (as addressed in Section 1.3.1) and privacy issues (as addressed in Section 1.3.2). Nevertheless, for the sake of addressing both parts in a more systematic manner, data security and data privacy issues associated with the use of drones are presented together under the framework of data protection. Another important reason to address data protection and privacy issues in the present and the following sections separately is that the right of privacy concerns the protection of a fundamental human right, whereas data protection is the response to technological development and the data subject can be either a natural persons or a company.[23] In addition, the processing of data should be subject to data protection rules, which have connections with but are still independent from privacy rules.

---

[19] Retrieved from http://dronelaw.blogspot.nl/2015/06/the-chilling-effect-of-drones-article.html (Accessed on 5 March 2017)
[20] Finn, R., Wright, D., Jacques, L., & De Hert, P. (2014). Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations. Final Report, Luxembourg: Publications Office of the European Union, 39.
[21] Supra note 20, 27.
[22] Finn, Rachel L., David Wright, and Michael Friedewald, "Seven types of Privacy" in Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (Eds.), *European Data Protection: Coming of Age,* Springer, Dordrecht, 2013, 16.
[23] Supra note 20, 42.

Data protection risks associated with the use of drones for processing all types of data: images, biometric data, sounds, location data, etc. As addressed by Working Party Article 29, "the increasingly powerful techniques drones may be equipped with would allow collecting personal data through high resolution image and video recordings as well as storing and, if necessary, transferring such data to the relevant ground station".[24] In addition, same as stated in the previous Section on privacy issues, data are collected in a covert manner, which means "data subjects would hardly be aware of this kind of processing as it is difficult to notice RPAS, because of their small size and the altitude of operation".[25] Another risk to data privacy associated with the use of drones is the likely massive and indiscriminate collection of data, which goes beyond the original purpose of collecting a specific type and amount of data.

The risk of data security arises from the improper capture and the likely hijacking of contents captured by drones.[26] For instance, through Wi-Fi connection, data on cell phones can be stolen by the drones which are operated by improper users, and drones in normal operations can be hijacked by hackers for illegal uses.[27]

1.3.4 Environmental Interference

Environmental inference would not be the major concern in the use of drones, mainly because most drones are powered by electrical engines. Main environmental interferences are noise nuisance, especially the noise caused by small drones flying over residential areas.[28] The buzz sound in drones could amount to noise emission if a drones with a big engine flies at a low altitude above buildings. Another potential environmental pollution concerns the imprecise injection of particles, in particular pesticides, in agricultural use of drones.

1.4 Economic Issues

Economic concerns relate to both positive and negative aspects. The positive refer to the increased market of designing and producing drones as well as the business of providing professional operator services. For instance, it has been predicted that, once the civilian use of RPAS is integrated into civil aviation market, the growing RPAS activities will create a substantial number of jobs and economic benefit.[29] The negative aspects encompasses two dimensions, which are direct economic loss due to the crashes or the loss of expensive drones

---

[24] The Working Party Article 29 was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Retrieved from: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131216_reply_to_rpas_questionnaire.pdf (Accessed on 5 March 2017)
[25] Ibid.
[26] Supra note 20, 45.
[27] How a Drone Could Spoof Wi-Fi, Steal Your Data. Retrieved from: http://www.nbcchicago.com/investigations/drone-public-wi-fi-302649331.html (Accessed on 5 January 2017)
[28] European Commission. Commission Staff Working Document Impact Assessment, Accompanying the Document, Proposal for a Regulation of the European Parliament and of the Council on Common Rules in the Field of Civil Aviation and Establishing a European Union Aviation Safety Agency, and repealing Regulation (EC) No 216/2008 of the European Parliament and of the Council, SWD (2015) 262, 15.
[29] Communication from the Commission to the European Parliament and the Council. COM (2014) 207. A new era for aviation, Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner, 4.

and indirect economic loss due to the diminishing job opportunities because of, for instance, the replacement of postmen with delivery drones.

2 Laws and Regulations Regarding the Design and the Operation of Drones

2.1 International Level

At the international level, the Convention on International Civil Aviation (Chicago Convention) is the major treaty relevant to unmanned aircraft. In principle, existing rights and obligations apply equally to manned and unmanned civil aircraft. Article 8 of Chicago Convention regulates conditions for operating a "pilotless aircraft":

> aircraft capable of being flown without a pilot shall be flown without a pilot over the territory of a contracting State without special authorization by that State and in accordance with the terms of such authorization. Each contracting State undertakes to insure that the flight of such aircraft without a pilot in regions open to civil aircraft shall be so controlled as to obviate danger to civil aircraft.

In addition, Articles 12 and Annex 2 (rules of the air), 15 (airport and similar charges), 29 (documents carried in aircraft), 31 (certificates of airworthiness), 32 (personnel licensing) and 33 (recognition of certificates and licenses) are also applicable to UAS.

Note that "model aircraft", generally recognized as for recreational purposes only, fall outside the provisions of the Chicago Convention, being exclusively subject to national regulations.

The International Civil Aviation Organization (ICAO), an UN specialized agency managing the administration and governance of Chicago Convention, published a circular in 2011 to address UAS. This circular submits that only the remotely-piloted aircraft (RPA) will be able to integrate into the international civil aviation system in the foreseeable future, because the functions and responsibilities of the remote pilot are essential to the safe and predictable operation of the aircraft. "[U]nder no circumstances will the pilot responsibility be replaced by technologies in the foreseeable future."[30]

2.2 EU Level

At the EU level, the European Aviation Safety Agency (EASA) is the European authoritative body that regulates and administrates the operation of UAS.[31] The EASA has been following the Riga Declaration to develop a regulatory framework for drone operations.[32] The Riga Declaration suggests that "drones need to be treated as new types of aircraft with proportionate rules based on the risk of each operation", and the rules should be "simple and performance based, to allow a small start-up company or individuals to start low-risk, low-altitude operations under minimal rules and to develop, with light-touch risk-based regulation".[33] In August 2016, the EASA adopted a "prototype" Regulation which is aimed to regulate UAS in an operation-centric,

---

[30] Supra note 2, para. 3.1.

[31] Earlier documents as regards the regulation on UAS, see, e.g., EASA. (2009). Policy Statement on the Airworthiness Certification Policy of Unmanned Aircraft Systems. Retrieved from https://www.easa.europa.eu/system/files/dfu/E.Y013-01_%20UAS_%20Policy.pdf; EASA. (2015). Concept of Operations for Drones - A risk based approach to regulation of unmanned aircraft. Retrieved from https://www.easa.europa.eu/system/files/dfu/204696_EASA_concept_drone_brochure_web.pdf

[32] Riga Declaration on Remotely Piloted Aircraft (drones) - "Framing the Future of Aviation", Riga, 6 March 2015.

[33] Ibid, Principle 1.

progressive and risk- and performance- based manner.[34] A new and unified EU drone regulation is expected to replace Member States' current regulations in a few years.

2.3 National Level[35]

2.3.1 The Netherlands

The regulations on the operation of unmanned aircraft in the Netherlands differentiate model aircraft (modelvliegen) from RPA (afstand bestuurde luchtvaartuigen). A model aircraft is defined as an unmanned aircraft used exclusively for aviation display, recreation or sports,[36] while the operation of RPA is for professional purposes. To date, a flight with a RPA is not allowed without a general or special permit. The operation of fully autonomous aircraft remains prohibited.

The Regulation on RPAs is the major legal instrument in the Netherlands that stipulates specific requirements for and restrictions of RPA operations.[37] Provisions on RPA contain specific obligations for RPA operators, airworthiness requirements for RPA, requirements for the operation of RPA and provisions on the participation of RPA in the air traffic.

In general, the total mass of a RPA should not exceed 150 kg. Flights with an RPA should not be above crowds, congested areas, artwork, industrial areas and harbours, railways or roads that are open for motorized vehicles.

RPA operators are required to demonstrate that their knowledge, skill and experience meet the requirement for issuing them a certain type of competence certificate (Operator Certificate, ROC). Regarding airworthiness requirements, the holder of a RPA is required to apply for a special airworthiness certificate (Speciaal Bewijs van Luchtwaardigheid, S-BVL). With respect to the operation of RPAs, an organization who wishes to operate RPAs is required to provide the manual (describing, among others, the detailed information about the operation of an RPA), the S-BVL, the ROC and the insurance against civil liability for the death, injury or other damage to third parties.[38]

In terms of the integration of RPAs into the air traffic system, RPAs must give way to airplane, helicopters, gliders, free balloons and airships.[39] The Regulation prohibits a VFR (Visual Flight Rules) flight with a RPA out of sight from the operator, with a maximum distance of 500 metres.[40] Generally, it is also prohibited to operate a RPA higher than 120 metres above the

---

[34] EASA. (2016). "Prototype" Commission Regulation on Unmanned Aircraft Operations. Retrieved from https://www.easa.europa.eu/system/files/dfu/UAS%20Prototype%20Regulation%20final.pdf (Accessed on 5 January 2017)

[35] Section 3.3 merely provides the prominent examples of national regulations regarding the operation of drones. For a comprehensive list of national regulations in EU countries, see www.dronerules.eu; For a comprehensive list of national regulations, see, e. g. Global Drone Regulation Database available at www.droneregulations.info

[36] Regeling modelvliegen. Retrieved from http://wetten.overheid.nl/BWBR0019147/2015-11-07

[37] Regeling op afstand bestuurde luchtvaartuigen. Retrieved from http://wetten.overheid.nl/BWBR0036568/2016-07-01 (All websites accessed on 18 October 2016)

[38] Supra note 37, Art. 10.1.

[39] Supra note 37, Art. 15 a.

[40] Supra note 37, Art. 13.2.

ground or water.[41] It is prohibited to operate a flight with a RPA higher than 45 metres above ground or water within aerodromes.[42] In the case that a VFR flight with a RPA flying above crowds, buildings, railways or high-speed roads, it is prohibited to operate such a RPA within 150 metres horizontally above them.[43] It is also prohibited to operate a VFR flight with a RPA within 50 metres horizontally above vessels, vehicles, artwork and railways. However, it is allowed to operate a FVP flight with a RPA within 50 meter horizontally above industrial and harbours.[44]

Notably, flights with RPAs less than 4 kg may be exempted from some standard restrictions. A flight with such a RPA is allowed when it meets the following requirements (Art. 10 a):

a) The flight is conducted within the distance of 100 metres from the operator;
b) The flight is conducted below 40 metres above the ground or water in an area in which civil or military aircraft may fly at a low altitude;
c) The flight is conducted below 50 metres in areas other than those areas mentioned in paragraph b);
d) The flight is conducted in airspace class G under the applicable regulations on air traffic.

It is lawful under the Regulation to operate a RPA less than 4 kg higher than 50 metres horizontally above crowds, buildings, railways or high-speed roads.

RPAS operators outside the Netherlands can apply for exemption.

2.3.2 Germany

The German Air Traffic Act (Luftverkehrsgesetz (LuftVG)) and the Air Traffic Regulation (Luftverkehrs-Ordnung (LuftVO)) apply to the operation of UAS.[45] Regarding the harmonious regulatory regime for the operation of UAS between the Federation and the German States, the Common Principles of the Federation and the States for Granting a Permission to Fly for Unmanned Aerial Systems apply.[46]

LuftVO defines that unmanned aerial vehicles used for sports or recreational purposes is qualified as "model aircraft" (Flugmodelle) instead of a UAS.[47] In general, the operation of a model aircraft less than 5 kg does not need an authorization.[48] The weight of a UAS is not allowed to be more than 25 kg.

---

[41] Supra note 37, Art. 14.1.
[42] Art. 16.
[43] Supra note 37, Art. 15.1.
[44] Supra note 37, Art. 15.2-15.3.
[45] An English overview of German regulations on UAS is available at: https://www.loc.gov/law/help/regulation-of-drones/germany.php#_ftn1 (Accessed on 5 November 2016)
[46] Gemeinsame Grundsätze des Bundes und der Länder für die Erteilung der Erlaubnis zum Aufstieg von unbemannten Luftfahrtsystemen gemäß § 16 Absatz 1 Nummer 7 Luftverkehrs-Ordnung (LuftVO). Retrieved from https://www.uavdach.org/aktuell/NFL-1-281-13.pdf
[47] LuftVG § 1, para. 2, no.11.
[48] LuftVO § 20, para. 1, no. 1a.

There are two types of authorization for the operation of UAS: a general authorization (Allgemeinerlaubnis) and a specific, case-by-case authorization (Einzelerlaubnis).[49] For a UAS that weighs less than 5 kg requires a general authorization from the aviation authority from German states. For a UAS that weighs between 5 and 25 kg, a specific authorization from German states is required. The general requirement for such an authorization is that the operation of a UAS does not present a risk to air safety or public safety or order, and does not violate the rules on data protection. As regulated in Section 16.4 of the German Air Traffic Act, a permission shall be granted if the intended uses do not result in any risk to aviation safety or to public security or order, and do not infringe the provisions governing data privacy.

The development of the regulations as regards remote pilot certification is ongoing.

2.3.3 France

France was one of the earliest country that started to regulate the commercial use of drones. In 2012, Directorate General of Civil Aviation issued the Order on the Use of Airspace by Unmanned Aircraft ("Airspace Order" below)[50] and the Order on the design of unmanned civil aircraft, the conditions of use and required capabilities of the people who use them ('Design and Use Order" below).[51] On 17 December 2015, both Orders were developed on the basis of the 2012 Orders, which are considered obsolete now.[52]

The 2015 Design and Use Order regulate drones via a categorized approach, which takes into account several variables: the weight of a drone, the purposes of operation and the scenarios of operation (only applicable to "particular activities"). In terms of the weight, the 2015 Design and Use Order defines two categories of model aircraft on the basis of weight and the type of propulsion.[53] Table 2-1 below briefly indicate the categorization:

---

[49] Supra note 46, Sections 2.1 and 2.2.

[50] Arrêté du 11 avril 2012 relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord (Order on the use of airspace by unmanned aircraft), 10 May 2012. Retrieved from https://www.legifrance.gouv.fr/jo_pdf.do?numJO=0&dateJO=20120510&numTexte=9&pageDebut=08655&pageFin=08657 (Accessed on 5 November 2016)

[51] Arrêté du 11 avril 2012 relatif à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent (Order on the design of unmanned civil aircraft, the conditions of use and required capabilities of the people who use them). Retrieved from https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025834953 (Accessed on 5 November 2016). An English translated version can be found at http://jarus-rpas.org/sites/jarus-rpas.org/files/french_decree_11_04_2012_uas_operations.pdf (Accessed on 5 November 2016)

[52] Arrêté du 17 décembre 2015, Relatif à la conception des aéronefs civils qui circulent sans personne à bord, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent (Order on the design of unmanned civil aircraft, the conditions of use and required capabilities of the people who use them). Retrieved from http://www.flyingeye.fr/wp-content/uploads/2015/01/DEVA1528542A-propre.pdf (Accessed on 5 November 2016); Arrêté du 17 décembre 2015, Relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord (Order on the use of airspace by unmanned aircraft). Retrieved from http://www.flyingeye.fr/wpcontent/uploads/2014/09/DEVA1528469A-propre.pdf (Accessed on 5 November 2016).

[53] 2015 Design and Use Order, Annex I. The types of propulsion include engine, electricity, turboprop, reactor and hot air.

Category	Description
A	• Model aircraft with a mass of no more than 25 kg, consisting of a single propulsion and subjecting to different limitations • Tethered model aircraft with a take-off weight of no more than 150 kg
B	Any model aircraft which does not belong to category A (requiring case-by-case authorization from the competent authority)

Table 2-1 Categorization of Model Aircraft in France

In addition to the explicit categorization of model aircraft, the Design and Use of Order also uses the take-off weight of 2 kg, 25 kg or 150 kg and the type of tethered or non-tethered as decisive parameters for non-model aircraft throughout the document. For instance, drones with a take-off weight of more than 150 kg requires case-by-case authorization from the competent authority.[54]

In terms of the purposes of operation, Article 3 of the Design and Use Order divides the civilian use of drones into three categories: recreational practices, experimental flights and "particular activities" (activité particulière) which includes all commercial operations. The three categories are separately regulated under the Design and Use Order. As specified in Table 2-1 above, Category A and Category B represent model aircraft. A model aircraft belonging to category A can be operated by anyone without any authorization, whereas an authorization from the competent authority is required for a model aircraft belonging to category B. In addition, restrictions are placed on the weight of model aircraft, the flying distance from the pilot and the altitude of flight.[55]

Annex II of the Design and Use order applies to drones utilized for experimental purposes. Basically, such an operation requires a special permit by the competent authority. Annex II also places restrictions on the weight of drones, the horizontal distance from the pilot as well as the altitude of flight.

Annex III of the Design and Use Order identifies four scenarios of "particular activities" (S-1 – S-4) in light of the operation area (in/outside populated areas) and the horizontal distance from the pilot (100/200/1000 metres).[56] S-2, S-3 and S-4 scenarios are subject to further restrictions. In S-2 scenario, restrictions are placed on the weight of drones and the altitude of flight - only

[54] The Design and Use Order, Annex III. Art. 1.3
[55] The Design and Use Order, Art. 3.
[56] The Design and Use Order, Annex III, Art. 1.3: "S-1: Using a drone outside a populated area, without flying over any third party, staying within the pilot's line of sight, and within a horizontal distance of no more than 200 meters from the pilot; S-2: Using a drone outside a populated area, where no third party is within the area of operation, within a horizontal distance of no more than 1 kilometre from the pilot, and not falling within the definition of S-1; S-3: Using a drone in a populated area, but without flying over any third party, staying within the pilot's line of sight, and within a horizontal distance of no more than 100 meters from the pilot; S-4: Using a drone outside a populated area, but not in a manner falling within the definitions of S-1 or S-2." This paragraph is the English translation of the French text. Retrieved from https://www.loc.gov/law/help/regulation-of-drones/france.php?loclr=bloglaw#_ftn42 (Accessed on 7 November 2016)

drones weighing no more than 2 kg are allowed to fly at an altitude of more than 50 metres.[57] In the S-3 Scenarios, only tethered drones or untethered drones weighing no more than 8 kg is allowed.[58] In the S-4 scenario, restrictions are additionally placed on the purpose of flight: only drones weighing no more than 2 kg is allowed, and the use must be limited to measurement, aerial photography, observation or surveillance. For all scenarios, except for tethered aerostats, it is prohibited to use autonomous drones for "particular activities". Any flights outside those four scenarios must be specifically authorised on a case-by-case basis.

In addition, three aspects of regulations under the Annex III of the Design and Use Order also merit attention. First, it specifies the requirement for a certification of design applying to different types of drones. Second, it articulates the operator's duties. The operator of a drone for "particular purposes" is required to make a declaration to the competent authority describing the purpose of using the drone, and to report to the competent authority annually, indicating the flying hours in the previous year, summarizing the problems encountered, and stating the airworthiness of any drone weighing more than 25 kg.[59] Notably, Annex III also requires the operator to be responsible for knowing and periodically evaluating the level of competence of the pilots.[60] Third, requirements for qualifying pilots are also addressed in Annex III. Pilots of drones for "particular activities" are required to obtain certificate of theoretical competence of flying a drone, and, in some cases, area required to indicate their practical competence, depending on the "particular activity" concerned.[61]

The Airspace Order specifies the restrictions on the use of airspace by drones, such as the altitude of flight in different situations, no-fly zones, prohibited flying time, etc. In general, drones are not allowed to fly higher than 150 metres above the ground, or higher than 50 metres above any artificial obstacle higher than 100 metres.[62] Without prior authorization, drones are prohibited or restricted to fly over certain zones, such as the immediate vicinity of an airfield and its surrounding respectively.[63] Also, drones are prohibited to fly at night except for special conditions.[64] In addition, drones should give way to manned aircraft.[65]

2.3.4 China

In December 2015, the Civil Aviation Administration of China (CAAC) issued the Provisions on the Administration of the Operation of Small Unmanned Aircraft System,[66] which regulate "small UAS" weighing no more than 116 kg. The Provisions are aimed at setting forth the rules for qualifying lawful small UAS operation and preventing unlawful operation.

---

[57] The Design and Use Order, Annex II, Art.1.4.1.
[58] Ibid, Art. 1.4.2.
[59] The Design and Use Order, Annex III, Art. 3.5.4
[60] The "operator" refers to a person or a company who is in the charge of the operation of drones. The "operator" is not necessarily the same person as the pilot.
[61] The Design and Use Order, Annex III, Art.4.2.1.
[62] Airspace Order, Arts. 5.3 & 7.1.
[63] Ibid, Art. 4.
[64] Ibid, Art. 3.
[65] Ibid.
[66] Retrieved from http://www.caac.gov.cn/XXGK/XXGK/GFXWJ/201601/P020160126526845399237.pdf (Accessed on 17 December 2016)

The Provisions categorize small UAS and the rules for the operation of small UAS. Under the Provisions, depending on the weight, purposes and flying distances, seven categories of UAV are defined as follows:

Categories	Aircraft weight (kg)	Take-off gross weight[67] (kg)
I	0 - 1.5	
II	1.5 – 4	1.5 – 7
III	4 – 15	7 – 25
IV	15 – 116	25 – 150
V	UAV for plant protection use	
VI	Unmanned airship	
VII	Categories I and II used beyond the visual line of sight (B-VLOS) outside 100 metres	

Table 2-2 Categorization of small UAVs in China

Table 2-2 above describes the categorization of small UAVs under the Provisions. Generally, the take-off gross weight of a small UAV should not excess 150 kg. Category I does not need to be subject to the Provisions, as long as it does not cause harm during the operation. The Provisions do not apply to aircraft models, unless auto-piloted utilities, command and control data link or other autonomous flying devices are used in such aircraft models.

According to the Provisions, the pilot-in-command[68] is responsible for the operation of UAS and is entitled to make final decisions in emergent circumstances. The pilot-in-command should ensure that UAVs should not trespass restricted areas.

Regarding the operation of UAVs within the visual line of sight, such operations should be carried out during the daytime, and should give way to manned aircraft. In addition to the requirement above, for the operation of UAVs beyond the visual line of sight, pilots should be able to control RPA and override autonomous aircraft at any time. In addition, the pilot-in-command should execute plans in case an UAV beyond the visual line of sight is out of control.

The real-time monitoring system, mainly including the UAS Cloud system and electronic fence, plays an important role in the administration of the operation of UAS. UAS Cloud system refers to the dynamic database system recording the operation of small UAS, providing navigation service and metrological service for UAS users, and monitoring operation data. The UAS Cloud system can also report prohibited behaviour of UAS to competent authorities. For UAS of categories III, IV, VI, and VII, the installation and use of the electronic fence and the connection to the UAS Cloud are required, and the pilot should report every second in densely populated areas and every 30 seconds in non-densely populated areas. For categories II and V, only those operated within key areas and airport clear zones are required to install and use the electronic fence, connect with the UAS Cloud, and report every minute.

[67] The weight of the aircraft plus the batteries, fuel, etc.
[68] "Pilot-in-command", in this Provisions, refers to the pilot who is responsible for the whole process of the operation of UAS and the safety of operation. In comparison, the pilot is the operator of UAVs and holds relevant responsibilities.

Notably, the Provisions specifically regulate the operation of UAS for plant protection, including spraying pesticides and other particles. The pilots should have the knowledge related to the features of pesticides and chemical medicines and their impacts on plants, animals and humans.

In August 2016, the CAAC issued the Provisions on the Administration of Operators in the Civilian Unmanned Aircraft System.[69] Under this Provisions, pilots are required to demonstrate that their knowledge, skills and experience meet the requirement for issuing them a certain type of competence certificate.

Airworthiness is not yet mentioned in UAS regulations in China. However, pilots are required to conduct pre-flight check in order to ensure that the weather condition, the venue for operation as well as the UAS are in safe condition.[70]

2.3.5 Japan

The current law on drones in Japan is the amendment to the Aviation Act came into effect on 10 December 2015 and the new Act on the Prohibition of Flying UAVs over Important Facilities and Their Peripheries (new Act below) promulgated on 18 March 2016.[71] The amendment to the Aviation Act prohibits the flying of drones above 150 metres above the ground level, over densely inhabited districts or areas near airports without permission from the Ministry of Land, Infrastructure and Transportation. Also, the operation of unmanned aircraft must be during daytime and should not be during an public event.[72]

The new Act prohibits the flying of drones over designated facilities, among others, the Prime Minister's office building, the Supreme Court building, embassies and nuclear facilities, and the no-fly areas extend to a 300-metre radius of such buildings and facilities. The punishment in the form of a fine or imprisonment is also regulated in the new Act.

No regulation is yet available regarding the certification of pilots in Japan.

2.3.6 United States

The Federal Aviation Administration (FAA) is the agency that administrates UAS operation and pilots. In June 2016, the FAA issued the Small Unmanned Aircraft Rule ("FAA Rule" below), which is aimed to regulate the operation of a small UAS as well as the certification and responsibilities of remote pilots.[73] The FAA Rule will be added to the Code of Federal

---

[69] 民用无人机驾驶员管理规定 (Provisions on the Administration of Operators in the Civilian Unmanned Aircraft System). Retrieved from: http://www.caac.gov.cn/HDJL/YJZJ/201606/P020160602508407084069.pdf (Accessed on 17 December 2016)

[70] 轻小无人机运行规定（试行）(Provisions on the Administration of the Operation of Small Unmanned Aircraft System, Art. 9).

[71] Regulation of Drones: Japan. Retrieved from https://www.loc.gov/law/help/regulation-of-drones/japan.php (Accessed on 17 December 2016)

[72] See the website of the Japanese Ministry of Land, Infrastructure and Transportation. Retrieved from http://www.mlit.go.jp/en/koku/uas.html (Accessed on 17 December 2016)

[73] FAA. (2016). Operation and certification of small unmanned aircraft systems. Retrieved from https://www.federalregister.gov/documents/2016/06/28/2016-15079/operation-and-certification-of-small-unmanned-aircraft-systems (Accessed on 17 December 2016)

Regulations of the United States to allow routine civil operation of small UAS in the national aviation system.

According to the FAA Rule, a small UAV should not have a weight of more than 25 kg. The flight of a small UAV must remain within the visual line of sight (VLOS) of the pilot-in-command, and must be operated during daytime. Small UAV must also yield right of way to other aircraft. The maximum groundspeed and altitude of small UAV are also stipulated in the FAA Rule.

Regarding the rules on the certification and responsibilities of remote pilot, the FAA Rule requires the establishment of a remote pilot-in-command position. The FAA Rule stipulates the qualifications for a remote pilot certificate.

Notably, under the FAA Rule, airworthiness certification is not required. The remote pilot in command is required to conduct a pre-flight check of the small UAS to ensure that it is in a safe condition for operation.

The FAA Rule does not apply to model aircraft, but it does not limit the FAA's authority to prohibit model aircraft from endangering the safety of the National Airspace System of the United States.

2.4 Trans-National Level

Joint Authorities for Rulemaking on Unmanned Systems (JARUS) is a group of experts from the National Aviation Authorities and regional aviation safety organizations.[74] JARUS aims to recommend a single set of technical, safety and operational requirements for the certification and safe integration of UAS into airspace and at aerodromes. At present, JARUS has been closely collaborating with the EASA by providing a platform for making a unified EU unmanned aircraft regulation.

In addition to JARUS, a number of non-profitable organizations and academic institutions have been working on gaining the knowledge about operational regulations of drones in different countries, providing inclusive platforms for stakeholders to communicate and discuss, and proposing soft regulations, such as code of conduct, guiding principles, etc. with a view to promoting the safe, respectful and responsible operation of drones.[75]

2.5 A Summary

Sections 3 provides an overview of existing rules and regulations at the international, the EU and national levels, applying to a) *the object per se* - the design and production of drones; and b) *the operation* - the safe operation of drones in the common airspace with manned aerial vehicles. As regards the first category, main elements are the specifications of drones, among others, the size, weight, type of engine and, very significantly, equipped sensors and cameras. Regarding the second category, main concerns are the safety requirement for integrating drone operations into civil aviation system. More specifically, there are three main aspects of

---

[74] Retrieved from http://jarus-rpas.org/ (Accessed on 17 April 2017)

[75] For instance, UAViators, which is a humanitarian UAV network, has published its Humanitarian UAV Code of Conduct & Guidelines. Retrieved from www.uaviators.org/docs (Accessed on 8 March 2017)

regulations regarding the operation of drones: requirements for drone operations; pilot qualifications; and air traffic rules (permitted flying time, weather condition, flying height, prohibited areas, visual line of sight, etc.).

National regulations regarding the operation of drones do not appear to be largely different among countries in terms of the objective and the regulatory scope, though the strictness of some specific rules vary. Commonalities between national regulations include but are not limited to: drone is defined as a type of aircraft (instead of a flying robot, according to the taxonomy in robotics); most national regulations exclude model aircraft for recreational uses from the regulatory scope of unmanned aircraft regulations (French regulation is an exception); all nation regulations provide for a range of restrictions on drone operations for the sake of safety; regulations are categorized mainly based on the weight of unmanned aircraft, but other factors such as the purpose of a flight and whether the flight is beyond VLOS are also important.

Bear in mind that the categorization of drones (at the moment mostly by weight) and the rules regarding drone certification and operational restrictions may change in order to keep pace with the gaining knowledge about safe operations of drones as well as the harmonization of national rules. For instance, the restrictions on the flight beyond the VLOS of the pilot in the US and the Netherlands would be temporary. Also, regulatory gaps need to be bridged, such as special rules for the flying of humanitarian drones.

It is apparent that drone rules and regulations have so far been developed within the aviation legal and regulatory regime, while it is underexplored whether the regulation of "drone" could also fall within the robotics legal regime. These two approaches would lead to the legislation and regulation of drones under different sectors of law.

3 Principles, Rules and Regulations Responding to the Impacts of the Use of Drones

Different from the specific rules and regulations that explicitly apply to the design and the use of drones as addressed in Section 2, Section 3 is aimed to identify existing principles, rules and regulations which might be applicable for the purpose of responding to the implications of the use of drones addressed in Section 2.3. Section 3 is not aimed to provide a comprehensive overview of all applicable rules and regulations at all levels; instead, Section 3 will address general principles contained in each issue together with examples of EU or national legislation.

3.1 Safety Issues

As stated in Section 1.3.1, safety issues concern the safety of airspace and aircraft as well as the safety of people and buildings on the ground. In general, tort law is adequate to respond to damages caused by the flying of drones. The tort of negligence, for instance, imposes a duty to all parties on the causal chain to exercise a reasonable level of prudence in order to minimize any foreseeable harm. In the case of drone operations, the parties concerned include but not limited to designers, software and hardware developers, manufacturers, pilots/operators and decision-makers who decide to deploy drones or set the parameters for their deployment.[76] Among the multiple tortfeasors, the attribution of responsibility and fault is complex, because a fault may have multiple causes: pilot's mistake, technical malfunction due to the defect of programming, and unforeseen events, such as extreme weather.

In order to minimize the threats to the safety of individuals and properties on the ground as well as of the airspace, available common rules include the requirement of certification: designers and manufacturers of aircraft are required to acquire certificates of design and production; holders of drones are required to acquire the airworthiness certificate for their drones; and operators are required to acquire an operator certificate. Other rules relate to the restrictions on drone operations, such as no-fly zone and the requirement of flying during daylight.[77]

In addition, the aspect of insurance is relevant to safety concerns in terms of protecting the potential victims against the risk contained in the operation of drones. Under the EU law, the current insurance framework under the Regulation EC/785/2004 on minimum insurance requirements for air carriers and aircraft operators is generally sufficient for insurance for drones.[78] Problems lie in the threshold of applying third-party insurance, where the mass of aircraft (starting from 500 kg) determines the minimum amount of insurance.[79] This rule proves insufficient for lightweight drones.[80] In addition, it is not yet certain whether the principles of insurance under the Regulation are applicable to drones, namely, whether *all* drones shall be insured as regards their aviation-specific liability in respect of third parties, and whether holders

---

[76] Gogarty, B., & Hagger, M. (2008). Laws of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air, The. *JL Inf. & Sci.*, *19*, 73, at 124.
[77] See Section 2.3.
[78] Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for air carriers and aircraft operators, Art. 2(g).
[79] Ibid, Art.7.
[80] Bernauw, K. (2016). Drones: The Emerging Era of Unmanned Civil Aviation. *Zbornik PFZ*, 66, 223, at 246.

and operators shall ensure that insurance cover *each and every* flight.[81] Reliable information regarding drone incidents collected in the early stage of operations would promote the development of a mature insurance market.[82]

A special problem contained in practice concerns the difficulty of identifying the operator in case of a drone incident and verifying whether the operator was sufficiently insured. A marking obligation has been proposed (using fire-proof plates for the identification of the operator and even the manufacturer).[83] However, the general application of such a marking obligation would be superfluous.[84]

With respect to the commercial use of drones in the future, one should not ignore that there would be drones carrying passengers, though it seems to be the advanced phase of the civilian use of drones. Commercial operations of drones carrying passengers would require more and stricter rules on safety in comparison with operations of small drones.

3.2 Privacy Issues

The term "privacy", though not yet universally defined, could be described as "the interest that individuals have in sustaining 'personal space', free from interference by other people and organisations".[85] Privacy issues covers many dimensions. Traditionally, privacy issues have been divided into four subcategories:

- Privacy of the person, or "bodily privacy": the right to keep body functions and body characteristics private;
- Privacy of personal behaviour: the protection against the disclosure of sensitive personal matters, such as religious practices and sexual activities;
- Privacy of personal communications: a restriction on monitoring telephone, email and virtual communications as well as face-to-face communications through hidden microphones;
- Privacy of personal data, or "data privacy": including images.[86]

With the emergence of new technology, it has been argued that the dimensions of privacy should be expanded to seven categories.[87] The three additional ones are

- Privacy of thoughts and feelings: note that thoughts and feelings can be distinguished from behaviour.
- Privacy of location and space: individuals have the right to move about in public, semi-public and private space without being identified, tracked or monitored.
- Privacy of association: individuals enjoy the right to associate with any type of groups without being monitored.[88]

---

[81] Ibid, Art. 4.
[82] Supra note 28, Section 5.1.
[83] Supra note 28, IV. 6.
[84] Supra note 29, 6.
[85] Clarke, R., Introduction to Dataveillance and Information Privacy, and Definitions of Terms, retrieved from http://www.rogerclarke.com/DV/Intro.html
[86] Ibid.
[87] Supra note 22, 7-9.
[88] Ibid.

In Europe, the right to protect privacy has been enshrined in the Charter of Fundamental Rights of the European Union. Article 7 states that "[e]veryone has the right to respect for his or her private and family life, home and communications". In the US, the Fourth Amendment of the US Constitution protects citizens from "unreasonable searches", in particular in areas where individuals have a reasonable expectation of privacy, such as their houses. One issue meriting attention relates to the tension between protecting the public safety by employing surveillance drones and the protection of citizens' right of privacy. According to the precedents in the US, in order to determine whether the flying of a drone interferes with an individual's *private* space, it is important to investigate whether such a drone is exposed to the public and the flight is considered "routine".[89] Moreover, the sensors equipped with a drone should not obtain more information about activities inside a home than the outsiders with "plain view" can do.[90]

The lawfulness of CCTV surveillance in a *public* space has been reiterated by the European Court of Human Rights that "the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life."[91] Along this reasoning, one can argue that drone surveillance that monitors a public space but does not record would be lawful. Nevertheless, one should keep in mind that, as addressed in Section 2.3.2, drone surveillance appears to be distinguished from CCTV or helicopters surveillance, due to the possible covert monitoring and the ability of dynamic tracing. Taking into account the distinctions, the principle of transparency becomes very important in terms of informing the public. Regarding the public space surveillance which does record the visual data, the recording, storage and disclosure of the data may give rise to an interference with the individual's private life.[92] In the case that a drone records the data during public place surveillance, it is significant that personal images should be masked before disclosure, or the subjects provide their consent prior to disclosure, unless there are sufficient reasons which would justify the direct closure.[93]

To deal with the privacy concern associated with the deployment of drones, in particular for law enforcement purposes, it has been proposed that privacy impact assessment should be proceeded prior to the operation of drones. The main reason is that the existing privacy-related regulations do not adequately address the ethical concerns of social sorting and discrimination via the equipped sensors of drones. Against this background, a "smart surveillance" approach which require explicit privacy assessments in order to ensure the necessity and proportionality of surveillance activities undertaken by drones is proposed.[94]

3.3 Data Protection

As mentioned in Section 1.3.3, the processing of personal data are subject to data protection rules, which have connections with but are still independent from privacy rules. Data protection

---

[89] Finn, R. L., & Wright, D. (2012). Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. *Computer Law & Security Review*, *28*(2), 184-194, at 192.
[90] Ibid.
[91] *Case of Peck v. The United Kingdom*, Judgment of the European Court of Human Rights, Final, 28 April 2013, para. 59.
[92] Ibid.
[93] Supra note 91, paras. 80, 82-84.
[94] Wright, D., Friedewald, M., Gutwirth, S., Langheinrich, M., Mordini, E., Bellanova, R., ... & Bigo, D. (2010). Sorting out smart surveillance. *Computer Law & Security Review*, *26*(4), 343-354.

concerns not only the protection of data privacy, but also the legitimate and secure measures of processing data.

The right to protect personal data is enshrined in the Charter of Fundamental Rights of the European Union.[95] Article 8 provides that personal 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". The right to protect personal data have been embedded in a wide range of European and national legal instruments.[96] The latest development is the Regulation (EU) 2016/679 of the European Parliament and of the Council, which is a framework regulation on the protection of natural persons with regard to the processing of personal data and the free movement of data.[97] Pursuant to the General Data Protection Regulation (GDPR), the processing of personal data shall be lawful if the data subject has given consent about the processing, or the processing is necessary due to other legitimate reasons.[98] There are general principles relating to processing of personal data: *the principle of lawfulness, fairness and transparency*, which refers to the manner of processing data in relation to the data subject; *the principle of proportionality*, which includes purpose limitation and storage limitation; *the principle of data minimisation*, which means that the data shall be "adequate, relevant and not excessive" to achieving the purpose for which the data are processed; *the principle of integrity and confidentiality*, which requires that the data shall be processed in a secure manner.[99]

The GDPR is applicable to the processing of personal data via drones for civilian uses.[100] The application of the principles relating to data protection to the use of drones is not without problems. First, the use of drones brings challenges to the compliance with the principle of transparency. Except for some exemptions, the cameras and sensors used for collecting data and the purposes of processing such data should be made explicit to the individual concerned prior to the collection. However, as identified in Section 1.3.3, the covert manner of capturing data by small-size drones creates a data privacy risk because individuals would hardly be aware of when and where their data are collected. Also, it is difficult for individuals to know who is operating the drone and observing them.

Second, some exemptions of or derogations for the processing of data make the application of rules problematic. Article 85 of the GDPR provides for the exemption of or derogation for the processing of data for "journalistic purposes", which attempts to balance the freedom of expression against the right of data protection. The potential uses of drones by individuals for disseminating information and opinions on newly emerging types of media, such as Twitter, YouTube and Facebook, complicate the definition of "journalistic purposes". Different from the traditional definition of journalists, those "new journalists" are unlikely to be familiar with and

---

[95] Charter of Fundamental Rights of the European Union, proclaimed on 7 December 2000, adopted on December 2009.
[96] E.g. Swiss Federal Act on Data Protection, retrieved from https://www.admin.ch/opc/en/classified-compilation/19920153/index.html; Irish Data Protection Acts, retrieved from https://dataprotection.ie/viewdoc.asp?DocID=1467&ad=1
[97] 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).
[98] General Data Protection Regulation, Art. 6.1.
[99] General Data Protection Regulation, Art. 5.1.
[100] General Data Protection Regulation, Art. 2.2(d).

to abide by professional rules.[101] The European Commission opines that "in order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly".[102] The European Commission's view on the definition of journalism implies the inclusion of wide range of activities undertaken by "new journalists". It can be expected that the increasing risk of data privacy and security caused by processing of data via drones will continue.[103]

Third, Article 2.2(c) stipulates that the GDPR does not apply to "a purely personal or household activity". In practice, the line is rather blurring between "a purely personal or household activity" and an activity that concern other individuals' interest. For instance, a drone equipped with camera is likely to not only monitor the drone operator's house but also the neighbour's garden. In this circumstance, the GDPR would still applicable.

In response to the risk of data privacy and security created by the civilian use of drones, the controller or processor of data are required under the GDPR to proceed *data protection impact assessment* and to comply with the principle of data protection by design and by default.[104] Regarding the data protection impact assessment, Article 35 stipulates that "where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data". Data protection impact assessment is applicable to the processing of data via drones, primarily because drones and their equipped sensors can be considered "new technologies" and are likely to result in a high risk to the rights and freedoms of data subjects. Regarding the principle of data protection by design and by default, Article 25 requires the data controller to "implement appropriate technical and organisational measures, such as pseudonymisation, which are *designed* to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects". Also, "[t]he controller shall implement appropriate technical and organisational measures for ensuring that, *by default*, only personal data which are necessary for each specific purpose of the processing are processed".[105] The principle of data protection by design and by default would introduce more responsibility to the designer and manufacturer of drones.[106]

A specific legal instrument meriting attention is the E-privacy Directive - Directive 2002/58/EC, which applies to the processing of personal data collected by providers of publicly available electronic communications services networks in the EU.[107] Directive 2002/58/EC is applicable to drone operations for electronic communication services. The use of drones for electronic

---

[101] Supra note 20, 266.
[102] Recital 17 of Directive 95/46/EC as well as Recital 153 of the General Data Protection Regulation.
[103] Supra note 20, 267.
[104] As to a comprehensive analysis of "privacy by design", see, e.g. Cavoukian, A. (2012). Privacy and drones: Unmanned aerial vehicles (pp. 1-30). Ontario, Canada: Information and Privacy Commissioner of Ontario, Canada.
[105] Italic added.
[106] Supra note 20, 78.
[107] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, 31/07/2002 P. 0037 – 0047.

communications shall be bound by, among others, the principles of confidentiality and anonymization.[108] At the moment, the relation between the E-privacy Directive and the General Data Protection Regulation is that the latter "shall not impose additional obligations on natural or legal persons in relation to [...] matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC".[109] In 2018, a new E-privacy Regulation is expected to replace the present Directive in order to be compatible with the General Data Protection Regulation.[110]

Regarding the use of drones for law enforcement or public surveillance purposes, a potential tension exists between the protection of public safety and the protection of privacy and personal data. The basic rational is that inferences by a public authority with the rights to privacy and data protection may be justified if such inferences are in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or for the prevention of disorder or crime.[111] According to Article 52(1) of the European Charter, "any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms". In addition, both the Court of Justice of the European Union and the European Court of Human Rights have made similar statements that the limitation on the rights to privacy and the protection of personal data can be justified only if it is "strictly necessary in a democratic society" and offers adequate and effective guarantees against abuse.[112] The Working Party Article 29 identified four "European Essential Guarantees" to make sure interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data do not go beyond what is necessary in a democratic society. The four "Guarantees" are:

A. Processing should be based on clear, precise and accessible rules;
B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated;
C. An independent oversight mechanism should exist; and
D. Effective remedies need to be available to the individual

The GDPR does not apply to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the safeguarding against and the prevention of the threats to public security.[113] Regarding the processing of data collected by drones for law enforcement purposes, Directive 2016/680 is specifically applicable.[114] According to the principles of lawfulness, proportionality and purpose

---

[108] Directive 2002/58/EC, Arts. 5, 6 & 9.
[109] General Data Protection Regulation, Art. 95.
[110] COM (2017) 10 final. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).
[111] European Charter of Human Rights, Art. 8(2).
[112] Article 29 Data Protection working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), adopted on 13 April 2016.
[113] Recital 19 of the General Data Protection Regulation.
[114] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Official Journal of the European Union, L350/60, Art. 1.

as laid down in Article 4 of the Directive 2008/680, personal data shall be collected only for specific explicit and legitimate purposes. Also, the processing of the data shall be lawful, fair, adequate, relevant and not excessive in relation to the purposes for which they are collected. Further processing of the data for another purpose shall be permitted in so far as the data controller is authorized and the processing is necessary and proportionate to that other purpose.[115] Echoing the previous paragraph regarding interferences with the right to data protection, Article 15 of the Directive 2008/680 specifies that "the data subject's right of access to the data may be restricted if it is necessary and proportionate in a democratic society with due regard for the fundamental rights and legitimate interests of the national person concerned".

Considering the novel features of drones, unprecedented challenges with respect to justifying the limitation to the right of privacy and data protection in drone operations for public surveillance and law enforcement purposes may be inevitable.

3.4 Environmental Interference

As addressed in Section 1.3.4, noise nuisance is the major environmental concern in the civilian use of drones. Noise emission standards vary from country to country, and thus the applicability of national regulations relating to noise emission standards to drones need individual investigation. At the EU level, drones are not subject to the noise emissions standards laid down in the Directive on the noise emission in the environment by equipment for use outdoors, because the Directive merely applies to a limited list of equipment, mainly outdoor machinery.[116] It has been proposed that "specific drone noise standards and/or operating restrictions may be needed".[117]

Irrespective of the attributes of drones available in the market, the risks of noise nuisance and gaseous emissions should always not be ignored. One situation is that "in cases where drones are equivalent to traditional aircraft, equivalent noise and gaseous emissions standards are to be applied to contain the environmental impact".[118]

---

[115] Ibid, Art. 4.
[116] Directive 2000/14/EC of the European Parliament and of the Council of 8 May 2000 on the approximation of the laws of the Member States relating to the noise emission in the environment by equipment for use outdoors, Art. 12.
[117] Supra note 28, 15.
[118] Supra note 28, 16.

4 Remaining Challenges and Reflections on the Proposal for Future Regulatory Framework

4.1 Remaining Challenges

The first challenge remains in the tension between the increasing demand of drones and drone services in the market and the regulatory restrictions placed on the testing and certification of drones as well as the validation of drone operations. Moreover, there is a lack of distinction between the regulatory methods for different scales of deployment, i.e. testing in lab or a limited area, small-scale deployment and full deployment. The recently available regulations in place might go too far ahead of the technological development and become a barrier for the early to middle stages of the development of drone technology. To change this quandary, the EASA proposed "phased and gradual introduction of RPAS operations" in the Roadmap,[119] which articulates that the insertion of drones in airspace must be gradual evolutionary: starting from restrictive operations and subsequently alleviate restrictions while technology, regulation and societal acceptance would progress. The ultimate goal is the full integration of drones in airspace for all types of operations.

The second challenge concerns the regulatory and administrative body that makes rules and administrates the design, manufacture and operation of drones. As examined in Section 3, regulations on drones and drone operations predominantly focus on safety issues, but the implications of drones for the society and individuals are largely overlooked, albeit some general requirement for the compliance with principles and rules laid down in privacy and environmental protection regimes. One main reason of causing the status quo is that civil aviation authorities (CAAs) are the major regulatory and administrative bodies involved in the regulating process. The traditional scope of mandate of CAAs for the safety of aeroplane operation and civil aviation determines CAA's limitedness of covering all relevant concerns surrounding drones, inter alia, data protection and security concern. The institutional design of regulatory and administrative bodies goes beyond legal analysis and thus will not be further discussed in the present paper.

Third, with the rapid enlargement of the drone market, transboundary operations of professional drone already occur, but a regulatory framework at regional or international levels is still lacking. The Chicago Convention is so far the only treaty available for drone transboundary operations, but the provisions that are applicable to UAS are far from sufficient. The mutual recognition of national and (when available) the EU drone regulations is required, given that a new treaty for drones may not be necessary.

4.2 Reflections on the Proposals for Drone Regulations in Future

There are a host of reports and academic publications in which the future regulations of drones have been proposed or partly discussed.[120] A synthetic analysis in the present Section

---

[119] Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System, Final report from the European RPAS Steering Group, June 2013, retrieved from http://ec.europa.eu/DocsRoom/documents/10484

[120] For instance, EASA. (2015). Proposal to Create Common Rules for Operating Drones, retrieved from https://www.easa.europa.eu/system/files/dfu/205933-01-EASA_Summary%20of%20the%20ANPA.pdf; TNO. (2015). Technical Aspects Concerning the Safe and Secure Use of Drones, retrieved from http://repository.tudelft.nl/view/tno/uuid%3A6dfe710d-68b0-4bf5-8a45-fddd29fccb1d/.

summarises the main contentions in three aspects: objectives, regulatory approaches, and the form of regulation.

- Objectives

All proposals tough upon two major objectives of regulating unmanned aircraft: a) ensuring the safety of the civil aviation and integrating unmanned aircraft into air traffic regulatory systems; b) protecting the right of privacy and protecting data. Some proposals also explicitly mention the objective of enabling the development of drone technology and promoting the market of civilian use of drones.[121]

- Regulatory approaches

The EASA proposed that the future regulatory framework should be operation-centric, progressive and proportionate to the risk related to an operation. Generally, operations start from small-scale and for simple purpose, and then gradually upgrade to full deployment and for highly professional or highly risky drone services.[122] It is widely agreed that regulations for RPAS should be developed first, and then comes to the regulation of fully autonomous drones. Under the "prototype regulation" published in 2016, UAS operations fall into one of three risk-based categories: "open", "specific" and "certified", which refer to UAS operations with low risk, medium risk and higher risk respectively.[123] The "prototype regulation" lays down rules, technical requirements and administrative procedures for UAS operations in "open" and "specific" categories; UAS operations in the "certified" category are not subject to this Regulation.[124]

- The form of regulation

A topic that has been widely addressed among scholars is how to deal with the dilemma between promoting technological innovation and controlling the adverse impacts arising from the deployment of a new technology on individuals as well as on the society. The challenge lies in how to make proactive and future-proof regulation which can respond to rapid technological development in a more legitimate, effective and efficient manner. The principle-based regulatory approach has been proposed, which states that the shift from the rule-based regulatory approach to the principle-based regulatory approach has the advantages of avoiding regulatory completion and can provides a greater degree of openness and flexibility, allowing for future revisions in the regulatory regimes based on new knowledge.[125]

In addition, the proactive and future-proof regulation can be achieved by decreasing the binding effect of regulation. Some scholars suggest that "soft regulations", such as handbooks and guidelines, could also play effective roles in guiding the design and operation of drones as well

---

[121] See, inter alia, supra note 29.
[122] Supra note 120
[123] Supra note 34, Art. 3.
[124] Supra note, 34, Art. 1.
[125] Fenwick, Mark and Kaal , Wulf A. and Vermeulen, Erik P. M., Regulation Tomorrow: What Happens When Technology is Faster than the Law? (September 4, 2016). Lex Research Topics in Corporate Law & Economics Working Paper No. 2016-8; U of St. Thomas (Minnesota) Legal Studies Research Paper No. 16-23; TILEC Discussion Paper No. 2016-024, retrieved from SSRN: https://ssrn.com/abstract=2834531 or http://dx.doi.org/10.2139/ssrn.2834531

as protecting privacy and data.[126] All stakeholders involved in drone research, development and manufacturing and operation could make self-regulations in the form of, for instance, industrial standards and code of conduct. Some self-regulations could be recognized by regulators later if the impacts of them prove to be positive and far-reaching.

[126] Supra note20.

5 An Integrated Process for Key Players to Comply with Laws and Regulations in Their Design and Use of Drones

After identifying existing laws and regulations which are applicable to the design and use of drones in Sections 3 and 4, Sections 5 and 6 will further explore how to ensure the responsible design of drones and drone services from the perspectives of key players and regulators respectively. Section 5 will propose an integrated process to guide the compliance with current laws and regulations by key players involved in drone design and operations, while Section 6 will be a more general study for regulators, categorizing the regulatory approaches for different types of threats or concerns caused by the design and operations of drones.

With a view to ensuring the responsible design and use of drones, an integrated process for diverse players to follow is proposed as shown in Figure 5-1 below. The integrated process functions as a guidance for diverse key players (develops, users, pilots, etc.) in the arena of drone design and services to shape their behaviour, and also enables the involvement of potentially affected parties, e.g. citizens, in resolving the tension between the protection of potentially affected parties and the promotion of new technology.

Such a process integrates the key players as well as the scale and the purpose of designing or operating drones via Steps one and two, and synergises the segmented laws and regulations applicable to drones and drone operations via Step three. After Step three, the key players of a drone design or operation activity will be able to have an overview of the current rules and regulations, and be clear about main problems in their compliance with such rules and regulations. Step four is aimed to guide the key players to be involved in rule-making and policy-making process in order to communicate such problems with regulators and policymakers, and possibly, propose their solutions to such problems.

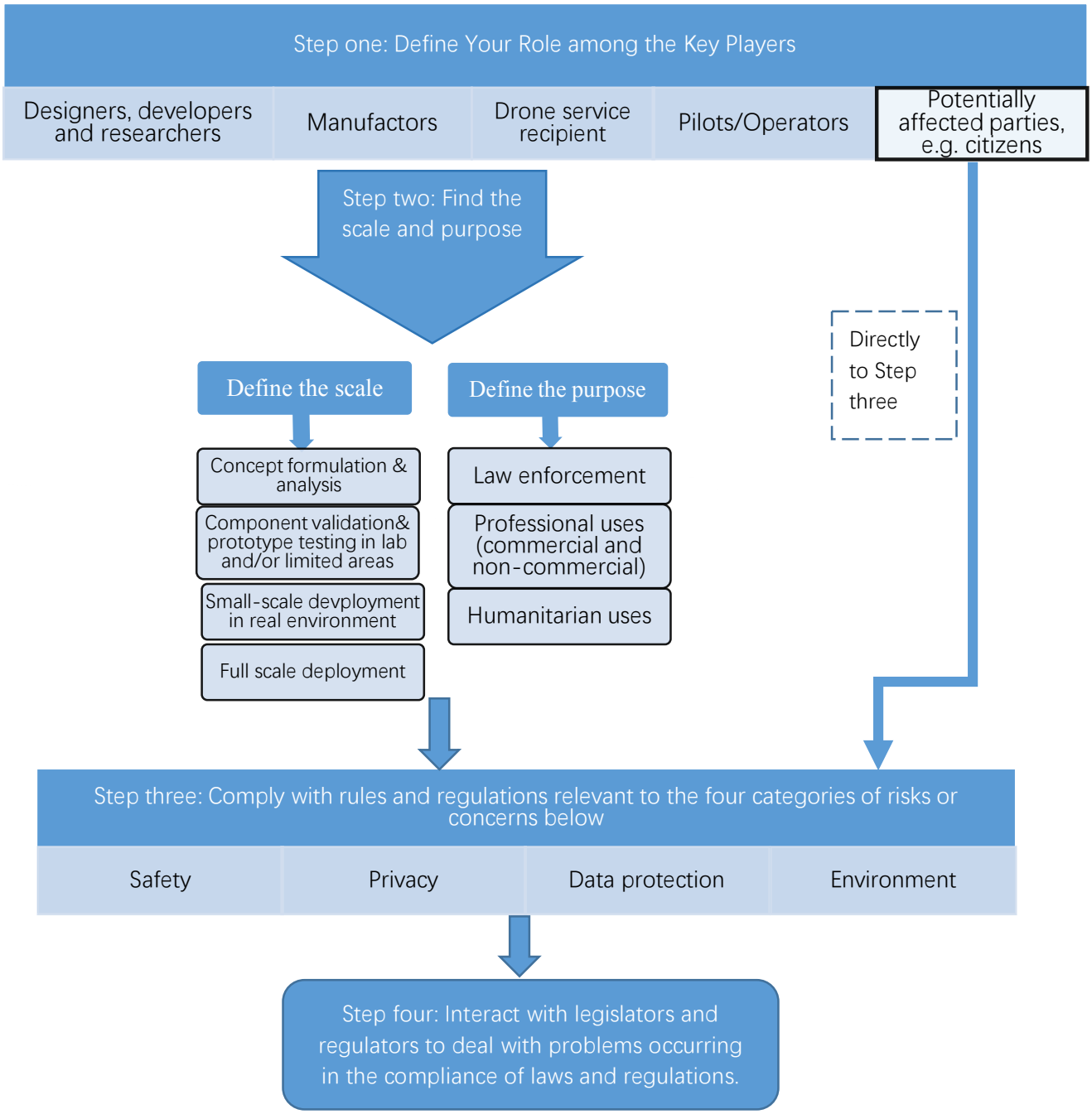

Figure 5-1 Compliance procedures for the responsible design and use of drones

Basically, this integrated process consists of four steps:

Step 1: The process starts from finding oneself the role as one of the key players, including a designer/developer, manufactor, drone service recipient and pilot/operator. Note that in the case of drones for surveillance or law enforcement operations, drone service recipient does not exist, because normally the public authorities own and operate drones themselves. The very right column in Step one represents external parties, such as citizens whose right to privacy could be affected, or a drone insurer whose economic interest is involved. The potential effect

could also be positive, such as citizens who does not order a drone service but indirectly enjoys the benefit from a drone service conducted in public space.

Step 2: Find the scale and (perhaps also) the purpose of designing, manufacturing, using or operating a drone. Regarding the scale, players can classify their proposed activities into one of the four scales: concept formulation and analysis (mainly referring to computer modelling); component validation and prototype testing in lab or a limited area (mainly referring to a testing area, e.g. sport field of a university campus or a drone airport), small-scale deployment in real environment (e.g. a municipality), and full scale deployment. Such classification is inspired from the model of Technology Readiness Level" (TRL scale), which consists of nine levels.[127] The four scales represent the transit from concept formulation into mature operation and full-scale deployment in real environment. Note that the three scales of activities pose different types and degrees of risks. For instance, "prototype testing in limited area" might not pose a privacy risk, while the risk of safety needs to be taken into account at each and every scale. (See detailed description in Table 5-1 below)

Regarding the purpose, as addressed in Section 1.2, drones can be designed and used for three main purposes: law enforcement, professional uses (commercial use, e.g. parcel delivery and precise agriculture; non-commercial uses, e.g. inspection and monitoring activities undertaken by governmental bodies); and humanitarian uses, mainly referring to seek and rescue after disasters. In general, the distinction between purposes makes sense because the applicable rules and regulation can be different. Note that it is not necessary for designers and developers to distinct between purposes when a drone is designed for multiple purposes.

Step 3: Comply with rules and regulations relevant to the four categories (safety, privacy, data protection, and environment) and find out, if any, the problems in the compliance with such rules and regulations. As stated in Section 3, current laws and regulations at international, regional and national levels are available on various databases and websites. Some are designed as step-by-step questions, for readers to acquire legal knowledge relevant to a specific use of drones.[128] Table 5-1 below shows a comprehensive picture of the compliance of four categories of rules and regulations by all key players in each Phase of drone development and deployment.

Table 5-1 Compliance with rules and regulations applicable to drones and drone operation

[127] There are a number of variations of the TRL metrics. One example is available from https://serkanbolat.com/2014/11/03/technology-readiness-level-trl-math-for-innovative-smes/

[128] For instance, the EU drone regulation website enables drone users to easily find the regulations applicable to either recreational or professional uses in a specific EU country. Retrieved from www.dronerules.eu

	Safety	Privacy	Data protection	Environment
Phase 1: Concept formulation and analysis	**Designer/developer/researcher:** Embed the notion of precaution and other ethical principles in their mind-set with a view to minimizing serious harm from the very beginning of their research and development. Voluntarily comply with any guidance or code of conduct available which are drafted and accepted within the designer/ developer/ researcher community. **Other players**: Not yet involved at this stage.			
Phase 2: Component validation & prototype testing in lab and/or limited areas (e.g. airport)	**Designer/ developer/ researcher**: Meet the international/EU/national standards regarding the design of a specific type of drone. In particular, technical measures for avoiding collisions and for preventing drones from trespassing restricted areas should be well built or programmed in the prototype. Voluntarily comply with any guidance or code of conduct available which are drafted and accepted within the designer/ developer/ researcher community. Protect developers' safety during testing. **Pilot**: Comply with certification or licence requirement under the EU and national regulations. **Other players**: not yet involved at this stage	**Designer/developer/researcher**: Take technical measures to protect privacy. For instance, automatic face- masking may need to be built in drones equipped with cameras. **Pilot**: As long as a pilot operates the drone prototype within the limited area, there is no privacy concern. **Other players**: Not yet involved at this stage	**Designer/developed/researcher**: Comply with the principle of data privacy by-design under the EU General Data Protection Regulation. **Pilot**: As long as a pilot operates a drone prototype within the limited area, there is no data privacy or security concern. **Other players**: not yet involved at this stage.	**Pilot:** Mostly no significant environmental concern, but take into account the disturbance.
Phase 3: Small-scale deployment in real environment (e.g. an university	**Designer/ developer/ researcher**: Same as in Phase 1, but be aware of the specific conditions of the real environment and comply with corresponding requirements regarding safety via built-in technical measures.	**Designer/developer/ researcher**: Same as in Phase 1. Be aware that in humanitarian operations or law enforcement operations, the technical measures needed for protecting privacy might be different.	**Designer/developer/ researcher**: Same as in Phase 1. Be aware that in humanitarian operations or law enforcement operations, the technical measures needed for protecting privacy might be different.	**Operator:** Mostly no significant environmental concern, but take into account the disturbance.

campus, a town or a city)	**Manufactor**: Meet all applicable manufacturing standards and requirements, such as the EU General Product Safety Directive (GPSD). **Drone service recipient**: Should not request drone services for any activities that may constitute any criminal offenses. **Operator**:[129] Comply with the drone certification requirements as well as applicable civil aviation laws and regulations under international, the EU or national regimes.	**Manufactor**: Meet all applicable manufacturing standards and requirements. **Drone service recipient**: Should not infringe others' right to privacy during the requested drone services, unless there are sufficient reasons that can justify such infringement. **Operator**: Comply with privacy principles: necessity, proportionality, lawfulness, transparency, etc. when processing the data collected via a drone service. (See Section 3.2)	**Manufactor**: Meet all applicable manufacturing standards and requirements. **Drone service recipient**: If the drone service recipient is the data controller[130], he should be responsible for proceeding data protection impact assessment under the EU GDPR when an operation is likely to result in a high risk to the rights and freedoms of natural persons; Comply with data protection principles: necessity, proportionality, lawfulness, transparency, etc. under the EU law when processing the data collected via a drone service. (See Section 3.3); **Operator**: If the operator is the data controller, he should be responsible for proceeding data protection impact assessment under the EU GDPR when an operation is likely to result in a high risk to the rights and freedoms of natural persons; Comply with data protection principles under the EU law when operators collect and/or process the data.	

[129] The term "operators" refers to either legal persons or natural persons, while the term pilot refers to a natural person.
[130] The term 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. General Data Protection Regulation, Art. 4(7).

Phase 4: Full scale deployment, e.g. on a national basis or across national boundary. (not yet realized)	The major concerns would be same as in Phase 2, but the degree of risks could be higher, and accordingly, the proceeding of, for instance, privacy impact assessment, could be stricter.	**Operator**: Comply with national or local regulations regarding noise control when deploying drones in an inhabited area; Complying with international, the EU and national laws regarding the prevention of air pollution and complying with national policies regarding CO_2 mitigation when a drone is generated by a combustion engine.

Note that the use of drones for the purposes of preventing and detecting criminal offenses and executing criminal penalties are administered by state authorities and are not subject to civil drone regulations. For instance, the General Data Protection Regulation is only applicable to the processing of data collected via *civil* operations of drones. In addition, rules on the necessary and proportionate interference by competent authorities with the rights to privacy and data protection for the purposes of safeguarding public safety, national security, etc. are applicable to the use of drones for law enforcement.[131]

Step 4: Key players interact with legislators/regulators. Bear in mind that, at the moment, regulations for the design of drones and safe operation of drones are under rapid development, and thus the current regulations, for instance in the EU countries, are likely to be replaced by unified EU regulations in a few years. Other national regulations are also expected to be (largely) modified in the coming years. In addition, rules or guidelines on mutual recognition of drone certification, pilot licence, operation authorization, etc. between countries are under development. Hence, all key players should keep in mind that, though they must comply with the current national regulations as well as relevant international and regional standards and rules, they could meanwhile actively keep communication with regulators and legislators and inform them the problems they encounter during their compliance with current rules and regulations. Also, key players could propose their possible solutions to such problems.

The interaction between regulators and key players, in particular developers and operators, should be an iterative process. In response to the problems contained in the compliance, regulators could make derogations from the current regulations for certain types of drone operations within a certain period of time and a limited area (e.g. in Phases 1 and 2), and the key players could propose to experiment with drone operations which are allowed by such a derogation from current regulations.[132]

It is without doubt that regulators and lawyers also play significant roles in promoting responsible design and use of drones. Regulators may keep dialogs with all players, and lawyers could even work with the players in an interdisciplinary environment. For regulators, Steps 1 and 2 could, in an early stage of research and development, determine which legal pathways (enabling, restrictive or prohibitive) seem open to new drone designs and operations. The functions of lawyers in the integrated process include but are not limited to three aspects. First, in Step 3, lawyers can provide a specific player with the legal knowledge about existing rules and regulations related to safety, security, privacy and nuisance at international, regional, national or municipal levels, depending on the targeted market in which the designed drones will be sold and the individual condition of a proposed drone service activity. Second, in Step 4, lawyers can help the specific player to deal with difficulties in the compliance process. Third, in both Steps 3 and 4, lawyers can play as the bridge between potentially affected parties, such as insurers and citizens, and key players, such as drone developers and users. Lawyers, together with other players, could communicate with regulators, addressing the problems associated with the compliance with current rules and regulations, addressing the problems associated with the compliance with current rules and regulations.

---

[131] See Section 3.3 for a detailed discussion.
[132] This topic will be addressed separately in another paper.

6 Major Regulatory Approaches in Response to Different Threats or Concerns

The end of Section 5 mentioned that the development of the regulations of drones and drone operations is ongoing. Section 6 will go beyond the current laws and regulations and explore a more general question: how to choose different regulatory approach in response to threats or concerns arising from different reasons? This exploration aims to provide the basic regulatory tools for regulators and policymakers to follow.

The analysis of major regulatory approaches addressed in the present Section applies the risk governance theories concerning differentiated approaches that respond to scientific risks, social and political implications, scientific uncertainties and perceived risks (ambiguities). One well-known theoretical framework concerning the governance of classified risks was developed by Andrew Stirling. Based on the division of four different states of knowledge - risk, ambiguity, uncertainty and ignorance, he listed methodological responses to the four states of knowledge respectively, and provides a framework that synergizes the precautionary and participatory approaches together with traditional "science-based" risk assessment.[133] Similarly, Ortwin Renn and Andreas Klinke classified risk-based, precaution-based and discourse-based approaches to deal with the challenges of complexity, uncertainty and ambiguity respectively.[134]

Based on the theoretical frameworks stated above, a portfolio of classified regulatory approaches to deal with different types of threats or concerns associated with drone design and operation is illustrated in Figure 6-1 below :

[133] Stirling, A. (2008). Science, precaution, and the politics of technological risk. *Annals of the New York Academy of Sciences*, *1128*(1), 95-110, at 103, Figure 4 and 106, Figure 5.
[134] Klinke, A., & Renn, O. (2002). A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies. *Risk analysis*, *22*(6), 1071-1094.

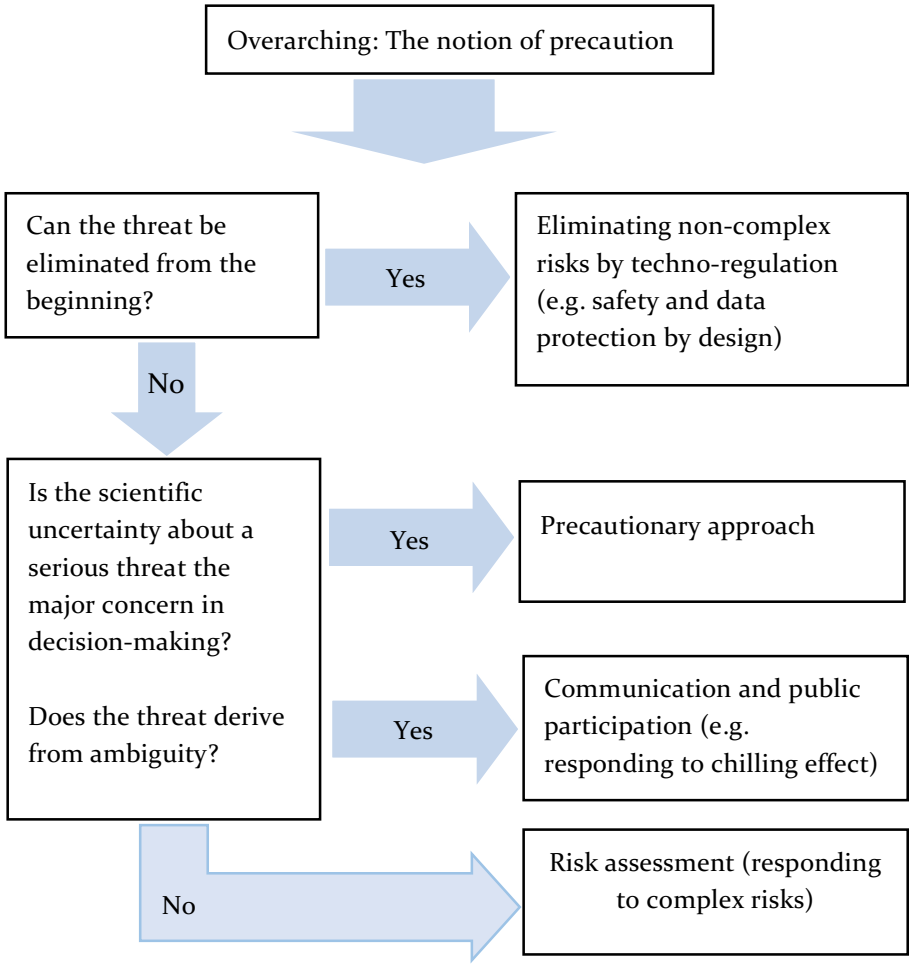

Figure 6-1 The portfolio of regulatory approaches

As shown in Figure 6-1 above, the notion of precaution plays an overarching role in guiding the whole process of the design and operations of drones with a view to ensuring an adequate degree of protection of individuals, the society and the environment. The portfolio consists of four major regulatory approaches: a) designed-in regulations via technical measures (or called techno-regulations), b) the precautionary approach, c) communication and public participation, and d) risk assessment. Techno-regulations can be widely applied to the threats that can be eliminated from the beginning. Typical examples are the programmes or components embedded in a drone for the purposes of sensing and avoiding collision, control and communication, and geo-fencing. Privacy-by-design methods also belong to techno-regulation. With respect to threats that cannot be eliminated from the beginning, then other approaches take place to minimize and control them. The precautionary approach refers to a range of regulatory measures, such as some of the aforementioned, which aim to avoid significantly or seriously adverse impact regardless of the availability of decisive evidence. The precautionary approach is applicable when scientific uncertainty is the major concern and a risk of serious or significant harm is compelling. Communication and public participation are specially applied by public authorities to solve the problem of chilling effect. Public participation encompasses negotiation amongst stakeholders, inclusive discussion, public

access to information, engagement with the public, etc.[135] Risk assessment is an approach to evaluate risks and find risk mitigation methods, when a threat cannot be prevented from the beginning. Risk assessment covers a series of procedures to deal with complex risks.

The four regulatory approaches stated above are the major tools for regulators to respond to different types of threats and concerns associated with drone design and operations. Note that those four regulatory tools might not be able to deal with all risks and concerns, but they would be sufficient to respond to most of them. Their connotations and the scope of applications will be elaborated in Sections 6.1-6.4.

6.1 Designed-in Regulation

The term "designed-in regulation" refers to a regulatory approach that embeds regulation into the system or components of a machine or a software via technical measures. Techno-regulation could also be phrased as "techno-regulation" or "built-in regulation". For instance, some built-in features make drones law-abiding by nature. Such features could also make it easier for users to comply with regulations. The built-in features include, among others, weight and other restrictions on kinetic energy, height limit, radius limit, line of sight, autonomous functions (when the pilot's control is lost), Wi-Fi bandwidth availability[136]. Similarly, designed-in-regulation could also effectively deal with fully autonomous aircraft by relying on automated route-selection, traffic-detection, and collision-avoidance system.[137] Moreover, designed-in regulation is also recognized as an effective tool for data protection. As addressed in Section 3.3, the recent EU General Data Protection Regulation incorporates the principle of data protection by design as one of the main principles. According to the principle of data protection by design, data controllers are required to "implement appropriate technical and organisational measures" in order to protect the right of data subjects.

Designed-in regulation includes three categories: techno-enforcement/compliance of existing legal rules, techno-enforcement/compliance of self-regulations and smart techno-regulation. The first two categories have so far been widely applied by drone developers and designer who embed regulations into drones via designing or programming, but the third category is merely a prospect. Techno-enforcement/compliance of existing legal rules refers to the enforcement or compliance with existing legal regimes of a jurisdiction in which the design or operation of a drone takes place. Techno-enforcement/compliance of self-regulations refers to the enforcement or compliance with, for instance, designing guideline, manufacturing standard or a code of conduct accepted by a group of stakeholders. Such self-regulations could effectively compliment with existing legal rules, not only for bridging regulatory gaps, but also for exploring innovative regulation and collecting experiences. The third dimension is only associated with autonomous drones. The regulation becomes "smart" because autonomous drones can apply rules to specific situations in real world and make decisions by themselves. Depending on the real situation during operation, the autonomous drone has discretion over

---

[135] Supra note 133, p. 106, Figure 5.

[136] Perritt Jr, H. H., & Sprague, E. O. (2014). Law Abiding Drones. *Colum. Sci. & Tech. L. Rev.*, *16*, 385-451, at 430-432.

[137] E.g. Nokia and Europe's first drone-based Smart City traffic management test facility collaborate to ensure safe global aerial operations. Available at https://www.nokia.com/en_int/news/releases/2016/09/26/nokia-and-europes-first-drone-based-smart-city-traffic-management-test-facility-collaborate-to-ensure-safe-global-aerial-operations.

how to apply rules. For instance, when a rule only provides a range (flying no further than 500 metres, for instance), and the autonomous drone decides how to apply it to different situations, transferring the range into a specific number.

Critiques surrounding the first two categories of designed-in regulation are worth attention. The main challenge is that designed-in regulation lacks flexibility. The real society is far more complex than the estimated scenarios, based on which the behaviour of drone is programmed. For instance, geo-fencing is programmed to prevent drones from flying certain areas where are clearly specified in relevant regulations, which means that it is not possible to apply geo-fencing to an area where should be temporarily restricted due to emergencies but is not included in the geo-fencing programme. In comparison with traditional way of enforcing regulations through executor, techno-regulations improves the effectiveness and efficiency but meanwhile losses flexibility and the ability to deal with emergencies. In addition, not all legal norms can be translated into technical design.[138] In particular, problems raise when some provisions are conflicting.

The third category of designed-in regulation could respond to the challenges stated above, because it solves the problem of inflexibility. However, whether and when smart designed-in regulation can be applied in the future would highly rest with the development of robotics as well as the legal and ethical implications. After all, the "smartness" would enable autonomous drones to disobey some existing rules in special situations. For instance, it might happen that a drone flies too close to a helicopter, but the quickest way of avoiding collision is to fly over a building nearby with geo-fencing. In this situation, the drone is capable of deciding whether it is necessary to fly into the gen-fenced area for a short time until the helicopter passes by. Thanks to the self-learning ability, if the drone repeats the same behaviour every time when it faces the same situation and the result is always positive, the drone could then "create" a new rule when it needs to make a decision in a quandary. In other words, smart techno-regulation means not only applying existing rules to complex situations in a flexible manner, but also creating new rules or new exceptions from existing rules from positive experiences collected by autonomous drones.

Taking into account the shortcomings of designed-in regulation, it nevertheless has great potential in contributing to a more efficient and less costly enforcement of laws and regulations and in preventing unlawful drone behaviour from the beginning.

A better approach could be a combination of "regulation *of* drones" by regulating human behaviour and "regulation *through* drones" by embedding regulations into drones.[139] On the one hand, simple and specific rules may be suitable for hard-coding in IT systems. On the other hand, one cannot only rely on building in legal requirements in the design of systems as a means of ensuring automated compliance with law.[140] For instance, with respect to data protection, it is suggested that designers should try to internalise the data protection framework as part of

---

[138] Leenes, R., & Lucivero, F. (2014). Laws on robots, laws by robots, laws in robots: Regulating robot behaviour by design. *Law, Innovation and Technology*, *6*(2), 193-220.
[139] Adapting from the concept of "regulation *of* robot" and regulation *through* robot", in ibid.
[140] Koops, Bert-Jaap, and Ronald Leenes. "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law." *International Review of Law, Computers & Technology* 28.2 (2014): 159-171, at 167.

their mindset, and design the system on the basis of carefully considered strategies that work within the specific context of the system at issue.[141]

In practice, designed-in regulation requires a deep interaction and collaboration between lawyers and drone designers and developers is indispensable. Without doubt, that designers and developers need to know what regulations they must take into account in designing or programming drones, and lawyers themselves are not able to build regulations into drones.

6.2 The Notion of Precaution and the Precautionary Approach

When the severity or/and the likelihood of a risk is/are unknown due to the limitation of knowledge, the *notion of precaution* becomes an overarching concept which needs to be embedded into the regulation of an emerging technology or a new product. 'It is of course true that we should take precautions against some speculative dangers."[142] Since 1970s, the idea of precaution has been widely incorporated into laws and policies that deal with technologies, activities or substances that may threaten human health (food safety, medication, nuclear power, terrorism, weapons), natural resources (fisheries, biological diversities) and the environment.[143] In the case of drone technology, the notion of precaution is useful in terms of guiding the whole process of the design and operations of drones with a view to ensuring a high degree of protection of individuals, the society and the environment. In particular, such a notion is actually more an ethical responsibility of every designer and developer from the very beginning of research and development.

It is significant to clarify that the notion of precaution is much broader than the precautionary principle. As a legal principle, the precautionary principle has a much narrower connotation, which has gradually developed via legislative and judicial practices. At the international level, the precautionary principle has been adopted in a growing number of treaties dealing with climate change, marine pollution, air pollution, biodiversity degradation, biosafety, etc.[144] Nevertheless, its legal status as customary international law is still controversial, because state practices are still divergent and inconsistent, and no uniform formulation is available. An example of divergent practices of the precautionary principle can be found in the EU law and the US law. The precautionary principle was adopted as a legally binding principle in Article 191.2 of the Treaty on the Functioning of the European Union, and has great influence on EU legislation as well as judicial practices.[145] On the contrary, such a high level protection of health

---

[141] Ibid, 168.
[142] Sunstein, C. R. Throwing Precaution to the Wind: Why the 'Safe' Choice Can Be Dangerous, Boston Globe, July 13, 2008, retrieved from http://archive.boston.com/bostonglobe/ideas/articles/2008/07/13/throwing_precaution_to_the_wind/
[143] Cameron, J., & Abouchar, J. (1991). The precautionary principle: a fundamental principle of law and policy for the protection of the global environment. *BC Int'l & Comp. L. Rev.*, *14*(1).
[144] E.g. United Nations Framework Convention on Climate Change, Art. 3; 1992 Helsinki Convention (Baltic Sea area), Art. 3(2); 1996 London Protocol to the Convention on the Prevention of Marine Pollution by Dumping of Wastes and Other Mater, 1972, Art. 3(1);1994 Protocol to the 1979 Convention on Long-range Transboundary Air Pollution on Further Reduction of Sulphur Emissions, Preamble; 1998 Protocol to the 1979 Convention on Long-Range Transboundary Air Pollution on Heavy Metals, Preamble; Convention on Biological Diversity, Art. 3; 2000 Cartagena Protocol on Biosafety, Arts. 1, 10(6) & 11(8).
[145] EU laws that adopt the precautionary principle include, for instance, the EU General Food Law Regulation 178/2002, Regulations 1107/2009 and 396/2005 concerning pesticides and Regulation

and environment by adopting restrict standards on food, chemicals, genetically modified organisms and nanotechnology is generally unavailable in the US legal systems.[146]

Basically, the precautionary principle enshrines that insufficient scientific evidence on a risk of serious harm posed by, for instance, a new technology, cannot be used as justification to authorise the deployment of such a technology. Decision-makers may nevertheless take restrictive or even prohibitive measures in order to prevent the materialization of the uncertain risk. Based on the concept of the precautionary principle, three elements – *risk, uncertainty and precautionary action* – can be abstracted. Among the three elements, a risk of serious harm and insufficient scientific evidence are the two elements that collectively trigger the precautionary approach, and a precautionary action is the response to the risk in spite of the uncertainty.

This report submits that the strict form of the precautionary principle *as conceptualized above* is not applicable to drones and drone operations – in so far as foreseen to date. The major reason is that civil uses of drones normally do not pose a risk of a serious harm to the society, and scientific uncertainty is normally not the major concern that influences decision-making. In other words, the strict form of the precautionary principle normally cannot be triggered. One may argue, in some worst-case scenarios, that the precautionary principle could be triggered. For instance, when flying a fleet over inhabited areas, the fleet poses a risk of serious harm to the public and the likelihood of an accident is uncertain. Nevertheless, in such a scenario it is still not necessary to trigger the precautionary principle. First, the likelihood of an accident does not represent a scientific uncertainty but rather a risk. Second, the abovementioned EU and international precedents of the application of the precautionary principle share a commonality: the potential harm is borne by the whole society and the environment. For instance, GMO food cannot be adequately tracked or segregated, and people will consume them unwittingly. On the contrary, professional or public operations of drones usually take place in certain areas and the potentially affected place and people are predictable. Hence, the proceeding of a risk assessment rather than invoking the precautionary principle would be appropriate. It is neither necessary nor proportionate to trigger the precautionary principle for the operations of civil drones; improper application of the principle would lead to an overregulation of civil drones.

However, it is without doubt that soft forms of precautionary principle are still broadly applicable to the design and operation of drones. To avoid confusion, those soft forms can be phrased as *precautionary approaches*, which reflect the notion of precaution but incorporate a much higher level of flexibility and variety rather than provide precise rules for decision. Contrary to the clear thresholds to invoke the hard form of the precautionary principle, no specific threshold is required to invoke precautionary approaches.

In a broad sense of precaution, both drone regulators and stakeholders should apply appropriate and proportionate precautionary approaches to their work. The main approaches for stakeholders include: promoting research into the early detection of potential hazards; promoting innovations in safer and cleaner alternatives to replace the potential harmful components; enhancing collaboration between stakeholders by establishing standards and code

---

1907/2006 concerning the registration, evaluation, authorisation and restriction of chemicals. Regarding judicial practice, in 2016 the CJEU upheld the validity of the restriction on the marketing of electronic cigarettes under the EU Tobacco Products Directive of 2014.

[146] Stoll, P., Douma, W., & Sadeleer, N. (2016). CETA, TTIP and the EU precautionary principle. Legal analysis of selected parts of the draft CETA agreement and the EU TTIP proposals.

of conduct; foresighted protective measures taken by stakeholders, inter alia, designers and developers. Developers and designers of drones should embed precaution into their mind-set, in order to avoid serious harm to customers from the very early stage of research and development.

Regulators and decision makers should accommodate designing regulations and making decisions with the notion of precaution. Soft regulations, such as guidelines, would be useful, when decisive scientific evidence is still absent but a minimum regulation for the purpose of protecting humans and the environment is demanded. Note that the modification or termination of a precautionary approach would be necessary, when the result of periodical evaluations along the pace of technological advances indicates so.

6.3 Communication and Public Participation

In practice, risk can be simplified into assessed and perceived risk. Assessed risks reflects a methodical attempt to objectively describe all significant harms within a defined system, while perceived risk reflects an individual's subjective judgment about particular dangers[147] Perceived risk is also understood as ambiguity, which reflects an individual's subjective judgment about particular dangers. The belief that a risk poses a serious threat produces public attention and fuels public anxiety.[148] "Chilling effect" is an effect resulting from such a "belief", which is essentially an ambiguity amongst the public.[149] The potential chilling effect caused by the (covert) surveillance drones is one of the major problems that regulators aim to resolve at a systemic level. The core to tackle chilling effect is to convince the public that their concern on data privacy has always been taken into consideration by public bodies, and a certain level of privacy risk is controllable and tolerable.

With respect to the public perception of surveillance drones, ambiguities could occur either because of the lack or the delay of correct information delivered to the public (cognitive ambiguity), or because of biases arising from values differences between individuals (values-related ambiguity). To deal with the former, communicating and sharing knowledge with the public are effective ways of correcting misinformation. Besides, a transparent process of assessing and evaluating privacy risks as well as the provision of publicly accessible information are vital for the public to (re)build the trust in public authorities.

However, sometimes, the methods of clarifying facts and sharing knowledge are not sufficient, because the public have ambiguities arising from biases or conflicting values. In this situation, "[a]mbiguities demand public participation."[150] The public, in particular the potentially affected parties, need to be involved in decision-making processes in order to discuss with the authorities the necessity of surveillance, the trade-offs between public security and data privacy, and some values-related issues such as desirable lifestyles and visions on new technologies. Major methods include peer review, negotiations amongst stakeholders, inclusive discussions, public access to information and engagement with the public. A detailed design of public

---

[147] Smith, B. W. (2016). Regulation and the Risk of Inaction. In *Autonomous Driving* (pp. 571-587). Springer Berlin Heidelberg.
[148] Supra note 134, 1088.
[149] The definition of "chilling effect", see Section 1.3.2.
[150] Supra note 134, at 1089.

participation to clear chilling effect will be left to local authorities, taking into account the initial public perception of surveillance drones in their own governing areas.

Notably, communication and public participation can be applied not only to deal with perceived risks but also in the process of assessing and managing 'objective' risks, which will be addressed below.

6.4 Risk Assessment and Management

Traditionally, the concept of risk consists of two elements: the severity and the likelihood of a risk. A risk is considered quantifiable when both elements are known. If one or both elements are unknown, such a risk is unquantifiable. Risk assessment is an effective method to deal with quantifiable risks of safety, security, environmental harm, etc. Risk assessment is an essential part of a responsible regulatory and decision-making framework for a new technology. The core components of a risk assessment include identification of hazards, the assessment of their exposure and adverse effects, risk characterization, risk evaluation, making a decision and reviewing the risk assessment.[151]

Switzerland was the first country which adopted a risk-based and operation-centred approach in its national drone regulation. In addition to general regulations regarding drone sizes and the distance and location of drone operations, applicants are required to submit an extensive "total hazard and risk assessment" based on the Guidance for an Authorisation for Low Level Operation of RPAS (GALLO) in order to obtain a permit to fly drones beyond the visual line of sight or above densely inhabited areas.[152] The GALLO process has been adapted to Specific Operational Risk Assessment (SORA) in the EASA proposal of the future EU unmanned aircraft regulation. It is proposed that, for the operations belonging to the "specific" category,[153] a SORA shall be performed by operators in order to mitigate risks to persons and properties on the ground and to other airspace users to an acceptable level.[154] Considering the fact that the majority of expected operators in the "specific" category have no experience in performing safety risk assessment, they need to follow the common requirements for "standard scenarios", such as "industrial inspections" and "precision farming and monitoring".[155]

The SORA is an example which shows how to apply the approach of risk assessment in the regulation of drone operation. First, it indicates a threshold of application: a proposed drone operation needs to proceed a risk assessment when the risk is likely to be higher than negligible. Second, the SORA indicates the advantage of applying risk assessment: promoting technological development and drone market while taking due account to the risk to persons and properties. Compared to a case-by-case permit based on diverse applications submitted by operators, the SORA enables operators to mitigate risks by following clear procedures as well as examining

---

[151] Renn, O. (2008). Risk governance: coping with uncertainty in a complex world. Earthscan, 73.
[152] See a summary of Swiss RPAS regulation: Eyes in the Sky: Regulatory Framework for operation of Drones in Switzerland, retrieved from http://www.mll-legal.com/news-events/news/details/eyes-in-the-sky-regulatory-framework-for-operation-of-drones-in-switzerland/
[153] See Section 2.2.
[154] EASA. (2015). Technical Opinion - Introduction of a regulatory framework for the operation of unmanned aircraft, p. 25, retrieved from https://www.easa.europa.eu/system/files/dfu/Introduction%20of%20a%20regulatory%20framework%20for%20the%20operation%20of%20unmanned%20aircraft.pdf
[155] Ibid.

specified factors as indicated in the risk assessment framework,[156] and therefore largely increases the possibility and efficiency of permitting a drone operation. Third, taking into account the complexity of the SORA, the formulation of "standard scenarios" again speeds up the process of finding mitigation measures in order to mitigate risks to an acceptable level.

Regardless of whether the SORA will be adopted by national drone regulations, risk assessment could be a useful approach for the regulation of drone operation. The design of the elements and procedures contained in a risk assessment would vary from country to country. Nevertheless, be aware of the threshold, the advantage and the limitation of using the risk assessment approach would always be helpful for regulators and policy-makers.

[156] Specified factors include, e.g. areas of operation, airspace, design of the unmanned aircraft, pilot competence, effect on environment. See, ibid, p. 24.

7 Conclusions and Recommendations

Civil uses of drones have shown their potentials in benefiting individuals and the society in a wide range of areas, and would create a promising market which provides attractive profits and job opportunities. Meanwhile, the threat concerning safety and concerns about security, privacy and data protection associated with civil uses of drones arise debates within and beyond academia on the pros and cons of employing drones. The ideal setting of rules and regulations at an early stage could not only foster the development of drone technology but also largely avoid damages caused by irresponsible design and uses of drones.

The present report concludes that laws and regulations applicable to drones and drone operations are available, albeit not sufficient. During the present research project, the author noticed that there is a prevailing misunderstanding among non-lawyers that "there is by far no regulation on drones and drone operations". It is important to highlight that there are a range of legal and regulatory instruments available to regulate drones and drone operations: first, many rules under civil aviation laws are also applicable to drones, because drones fall within the definition of "aerial vehicle", and the flying of drone should comply with civil aviation laws in order to ensure aviation safety in a shared airspace with manned aircraft. Second, basic rules and principles under data protection laws and personal privacy laws are also applicable to drones, as long as any type of drone operation would impact on personal and data privacy. Therefore, the submission that "there is by far no regulation on drones and drone operations" is wrong.

However, it is true that the current laws and regulations are not sufficient. Remaining issues include: first, specific regulations on the design and production of drones ("the object *per se*" as described in Section 2.5) and on drone operations are not yet available in many countries, in particular developing countries. The status quo is that in many countries customers can easily buy drones from the market but cannot legally operate them. In addition, thanks to the international e-commerce, nowadays one can easily order a drone designed and manufactured in a foreign country. However, due to the lack of international standards on designing and operating drones or the mutual recognition of national drone regulations, even if one country had its domestic regulation on drones and drone operations, problems would still arise when a drone is designed in accordance with one country's regulation and cannot be operated in another country because of the inconsistent regulations. In sum, the lack of specific regulations and the lack of shared standards heavily hinder the increasing market of drone services, and very often result in a prohibition of or highly restricted drone operations.

Second, there is an obvious tension between the increasing demand of drones and drone services in the market and the regulatory restrictions placed on the testing and certification of drones as well as the validation of drone operations. This tension can be reflected from almost all recently enacted national regulations on drones (see Section 2.3).

Third, taking into account the special attributes of drones, e.g. small sizes (in comparison with manned aircraft) and possibility of equipping drones with various gadgets (in comparison with traditional CCTV system), some existing rules regarding civil aviation safety and data protections become inapplicable. There is a challenge on how to integrate the regulation of drones and drone operations into civil aviation laws. Also, data protection laws need to respond to unprecedented problems arising from civil uses of drones.

The present report also concludes that specific regulations on drones at the international, the EU and nation levels are all rapidly progressing. A relatively mature regulatory framework can be expected within five years. The main goals of making such regulations are, first, ensuring the safety of the civil aviation and integrating unmanned aircraft into air traffic regulatory systems; second, protecting the right of privacy and protecting data; and third, enabling the development of drone technology and promoting the market of civil use of drones. In practice, the first goal is always prioritized. However, the protection of personal and data privacy is yet to be given higher attention than a general call on the compliance with existing principles and rules contained in privacy and environmental protection regimes.

With a view to ensuring the compliance with laws and regulations in their design and operation of drones, the present report proposes an integrated process (Section 5) to shape the behaviour of key players by raising their awareness of all types of potential risks throughout the whole process of their activities, by guiding them to comply with existing legal principles, rules and regulations, and by showing them the channels to provide their opinions for regulators if problems that lead to non-compliance occur. The integrated process functions as a guidance for diverse key players (developers, users, pilots, etc.) in the arena of drone design and services to shape their behaviour, and also enables the involvement of potentially affected parties, e.g. citizens, to resolve the tension between the protection of potentially affected parties and the promotion of drone technology. The process consists of four stages. First, find oneself the role as one of the key players, including designer/developer, manufactor, drone service recipient and pilot/operator. Second, key players find the scale and the purpose of designing, manufacturing, using or operating a drone. Third, key players comply with rules and regulations relevant to the four categories of threats or concerns, namely safety, security, data protection and environment, and find out if there is any problem in the compliance with such rules and regulations. Potentially affected parties are also involved in this process. Fourth, key players interact with legislators and regulators to deal with problems occurring in the compliance of laws and regulations. Such an interaction could be iterative, and the key players could propose to experiment with drone operations which are allowed by a derogation from current regulations.

In Section 6, the present report moves to the perspective of regulators, and proposes a framework of classified regulatory approaches to deal with different types of threats or concerns associated with drone design and operations. The notion of precaution serves as the overarching concept in guiding the whole process of the design and operations of drones with a view to ensuring a high degree of protection of individuals, the society and the environment. Designed-in regulations via technical measures are suitable for eliminating non-complex risks; the precautionary approach is applicable when scientific uncertainty is the major concern and a risk of significant harm is compelling; communication and public participation are specially applied by public authorities to solve the problem of chilling effect; and risk assessment and management covers a series of procedures and strategies to deal with complex risks.

Regarding the further development of the tools proposed in this report, Step 4 of the integrated process will be elaborated, indicating the mechanism of interaction between drone regulators and key players. With respect to the portfolio of regulatory approaches, further developments include how different regulators can apply this approach to their sectors, taking into account their distinct objectives in the regulation of civil drones. Moreover, exceptions will be analysed parallel to the common applications of regulatory each approach. For instance, when making a decision, it might be lawful not to follow the result of risk assessment, if a type of drone operation is proved necessary in an emergency.

In the end of the repost, several recommendations are provided for policymakers when considering the tension between technological innovation and the potential risks posed by emerging technologies:

- Ethical values should always be embedded into technological innovations.
- It is significant to facilitate and promote close collaboration and interaction between engineers and rule-makers. Techno-regulations are possible only if engineers and rule-makers work together.
- It is wise to take a tailored approach to tackle different types of threats or concerns differently, taking into account the attributes of the technology in question.
- The notion of precaution is useful in terms of guiding the whole process of the design and operations of drones with a view to ensuring a high degree of protection of individuals, the society and the environment. Although precautionary measures normally need not to be applied to drone technology, the notion of precaution should be embedded into designer and developers' mindsets and soft precautionary approaches might be necessary.
- Making decisions in a transparent and participatory environment is the key to correct misperception and towards the public's acceptance of a new technology in the society.

8 References

Bernauw, K. (2016). Drones: The Emerging Era of Unmanned Civil Aviation. Zbornik PFZ, 66, 223.

Bolat, S. (2014). Technology Readiness Level (TRL) math for innovative SMEs. Retrieved from https://serkanbolat.com/2014/11/03/technology-readiness-level-trl-math-for-innovative-smes/

CAAC: Provisions on the Administration of the Operation of Small Unmanned Aircraft System. Retrieved from http://www.caac.gov.cn/XXGK/XXGK/GFXWJ/201601/P020160126526845399237.pdf

CAAC. Provisions on the Administration of Operators in the Civilian Unmanned Aircraft System.

Cameron, J., & Abouchar, J. (1991). The precautionary principle: a fundamental principle of law and policy for the protection of the global environment. BC Int'l & Comp. L. Rev., 14(1).

Case of Peck v. The United Kingdom, Judgment of the European Court of Human Rights, Final, 28 April 2013.

Charter of European Union, proclaimed on 7 December 2000, adopted on December 2009.

Charter of European Union, proclaimed on 7 December 2000, adopted on December 2009.

Clarke, R. (2014). The regulation of civilian drones' impacts on behavioural privacy. Computer Law & Security Review, 30(3), 286-305.

Clarke, R. (2014). Understanding the drone epidemic. Computer Law & Security Review, 30(3), 230-246.

Clarke, R., & Moses, L. B. (2014). The regulation of civilian drones' impacts on public safety. Computer Law & Security Review, 30(3), 263-285.

Clarke, R. (2016). Introduction to Dataveillance and Information Privacy, and Definitions of Terms. Retrieved from http://www.rogerclarke.com/DV/Intro.html

COM. (2014). Communication from the Commission to the European Parliament and the Council. A new era for aviation, Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner. COM/2014/0207

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Official Journal of the European Union, L350/60,

Directive 2000/14/EC of the European Parliament and of the Council of 8 May 2000 on the approximation of the laws of the Member States relating to the noise emission in the environment by equipment for use outdoors.

Drone regulations of EU countries. Retrieved from www.dronerules.eu

Du. H & Heldeweg, M. A. (2017). Responsible Design of Drones and Drone Services. Legal Perspective (Synthetic Report). University of Twente (forthcoming). Research report commissioned by NWO (The Netherlands Organisation for Scientific Research).

EASA. (2009). Policy Statement on the Airworthiness Certification Policy of Unmanned Aircraft Systems. Retrieved from https://www.easa.europa.eu/system/files/dfu/E.Y013-01_%20UAS_%20Policy.pdf; EASA. (2015). Concept of Operations for Drones - A risk based approach to regulation of unmanned aircraft. Retrieved from https://www.easa.europa.eu/system/files/dfu/204696_EASA_concept_drone_brochure_web.pdf

EASA. (2015). Proposal to Create Common Rules for Operating Drones. Retrieved from https://www.easa.europa.eu/system/files/dfu/205933-01-EASA_Summary%20of%20the%20ANPA.pdf ; TNO. (2015). Technical Aspects Concerning the Safe and Secure Use of Drones. Retrieved from http://repository.tudelft.nl/view/tno/uuid%3A6dfe710d-68b0-4bf5-8a45-fddd29fccb1d/

EASA. (2015). Technical Opinion - Introduction of a regulatory framework for the operation of unmanned aircraft. Rretrieved from https://www.easa.europa.eu/system/files/dfu/Introduction%20of%20a%20regulatory%20framework%20for%20the%20operation%20of%20unmanned%20aircraft.pdf

EASA. (2016). "Prototype" Commission Regulation on Unmanned Aircraft Operations. Retrieved from https://www.easa.europa.eu/system/files/dfu/UAS%20Prototype%20Regulation%20final.pdf

EU General Food Law Regulation 178/2002, Regulations 1107/2009 and 396/2005 concerning pesticides and Regulation 1907/2006 concerning the registration, evaluation, authorisation and restriction of chemicals. Regarding judicial practice, in 2016 the CJEU upheld the validity of the restriction on the marketing of electronic cigarettes under the EU Tobacco Products Directive of 2014.

European Commission. Commission Staff Working Document Impact Assessment, Accompanying the Document, Proposal for a Regulation of the European Parliament and of the Council on Common Rules in the Field of Civil Aviation and Establishing a European Union Aviation Safety Agency, and repealing Regulation (EC) No 216/2008 of the European Parliament and of the Council, SWD (2015) 262, 15.

FAA. (2016). Operation and certification of small unmanned aircraft systems. Retrieved from https://www.federalregister.gov/documents/2016/06/28/2016-15079/operation-and-certification-of-small-unmanned-aircraft-systems

Fenwick, Mark, Kaal, Wulf A., Vermeulen & Erik, P. M., Regulation Tomorrow: What Happens When Technology is Faster than the Law? (September 4, 2016). Lex Research Topics in Corporate Law & Economics Working Paper No. 2016-8; U of St. Thomas (Minnesota) Legal Studies Research Paper No. 16-23; TILEC Discussion Paper No. 2016-024. Retrieved from SSRN: https://ssrn.com/abstract=2834531 or http://dx.doi.org/10.2139/ssrn.2834531

Finn, R. L., & Wright, D. (2012). Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. Computer Law & Security Review, 28(2), 184-194.

Finn, R. L., & Wright, D. (2016). Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organisations. Computer Law & Security Review, 32(4), 577-586.

Finn, R., Wright, D., Jacques, L., & De Hert, P. (2014). Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations. Final Report, Luxembourg: Publications Office of the European Union, 39.

Finn, R.,Wright, D, & Friedewald, M. “Seven types of Privacy” in Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (Eds.), European Data Protection: Coming of Age, Springer, Dordrecht, 2013.

France: Arrêté du 17 décembre 2015, Relatif à la conception des aéronefs civils qui circulent sans personne à bord, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent (Order on the design of unmanned civil aircraft, the conditions of use and required capabilities of the people who use them). Retrieved from http://www.flyingeye.fr/wp-content/uploads/2015/01/DEVA1528542A-propre.pdf.

Germany: Gemeinsame Grundsätze des Bundes und der Länder für die Erteilung der Erlaubnis zum Aufstieg von unbemannten Luftfahrtsystemen gemäß § 16 Absatz 1 Nummer 7 Luftverkehrs-Ordnung (LuftVO). Retrieved from https://www.uavdach.org/aktuell/NFL-1-281-13.pdf

Global Drone Regulation Database. Retrieved from: www.droneregulations.info

Globe. (July 13, 2008). Retrieved from: http://archive.boston.com/bostonglobe/ideas/articles/2008/07/13/throwing_precaution_to_the_wind/

Gogarty, B., & Hagger, M. (2008). Laws of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air, The. JL Inf. & Sci., 19, 73.

ICAO. (2011). Unmanned Aircraft Systems (UAS), Cir. 328, Glossary. Retrieved from http://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf

Irish Data Protection Acts, retrieved from https://dataprotection.ie/viewdoc.asp?DocID=1467&ad=1

Japan: Regulation of Drones: Japan. Retrieved from https://www.loc.gov/law/help/regulation-of-drones/japan.php

JARUS. Retrieved from http://jarus-rpas.org/

Klinke, A., & Renn, O. (2002). A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies. Risk analysis, 22(6), 1071-1094.

Koops, Bert-Jaap, and Ronald Leenes. "Privacy regulation cannot be hardcoded. A critical comment on the ‘privacy by design’ provision in data-protection law." International Review of Law, Computers & Technology 28.2 (2014): 159-171.

Leenes, R., & Lucivero, F. (2014). Laws on robots, laws by robots, laws in robots: Regulating robot behaviour by design. Law, Innovation and Technology, 6(2), 193-220.

Nokia and Europe's first drone-based Smart City traffic management test facility collaborate to ensure safe global aerial operations. Available at https://www.nokia.com/en_int/news/releases/2016/09/26/nokia-and-europes-first-drone-based-smart-city-traffic-management-test-facility-collaborate-to-ensure-safe-global-aerial-operations.

Perritt Jr, H. H., & Sprague, E. O. (2014). Law Abiding Drones. Colum. Sci. & Tech. L. Rev., 16, 385-451.

Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for air carriers and aircraft operators.

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)

Relatif à l’utilisation de l’espace aérien par les aéronefs qui circulent sans personne à bord (Order on the use of airspace by unmanned aircraft). Retrieved from http://www.flyingeye.fr/wpcontent/uploads/2014/09/DEVA1528469A-propre.pdf

Renn, O. (2008). Risk governance: coping with uncertainty in a complex world. Earthscan.

Riga Declaration on Remotely Piloted Aircraft (drones) - "Framing the Future of Aviation", Riga, 6 March 2015. Retrieved from https://ec.europa.eu/transport/sites/transport/files/modes/air/news/doc/2015-03-06-drones/2015-03-06-riga-declaration-drones.pdf

Schoch, D. & Linder, A. (19 Feb. 2016). Eyes in the Sky: Regulatory Framework for operation of Drones in Switzerland, retrieved from http://www.mll-legal.com/news-events/news/details/eyes-in-the-sky-regulatory-framework-for-operation-of-drones-in-switzerland/

Smith, B. W. (2016). Regulation and the Risk of Inaction. In Autonomous Driving (pp. 571-587). Springer Berlin Heidelberg.

Stirling, A. (2008). Science, precaution, and the politics of technological risk. Annals of the New York Academy of Sciences, 1128(1), 95-110, at 103, Figure 4 and 106, Figure 5.

Stoll, P., Douma, W., & Sadeleer, N. (2016). CETA, TTIP and the EU precautionary principle. Legal analysis of selected parts of the draft CETA agreement and the EU TTIP proposals.

Sunstein, C. R. Throwing Precaution to the Wind: Why the ‘Safe’ Choice Can Be Dangerous, Boston

Swiss Federal Act on Data Protection, retrieved from https://www.admin.ch/opc/en/classified-compilation/19920153/index.html

The Netherlands: Regeling op afstand bestuurde luchtvaartuigen. Retrieved from http://wetten.overheid.nl/BWBR0036568/2016-07-01

The Working Party Article 29 was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Retrieved from: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131216_reply_to_rpas_questionnaire.pdf

TNO (2016), Final Report: Technical Aspects Concerning the Safe and Secure Use of Drones. Retrieved from https://www.thehaguesecuritydelta.com/uavs-drones

Wright, D., Friedewald, M., Gutwirth, S., Langheinrich, M., Mordini, E., Bellanova, R., ... & Bigo, D. (2010). Sorting out smart surveillance. Computer Law & Security Review, 26(4), 343-354.