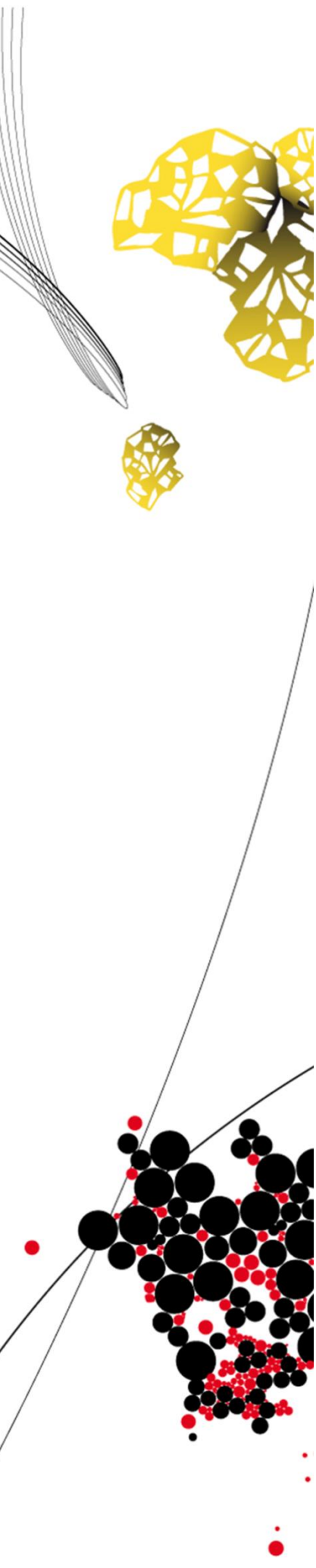


UNIVERSITY OF TWENTE.

Faculty of Behavioural, Management and Social Sciences

European Public Administration

Bachelor Circle 19

Drone technology and human rights

Florin-Costinel Dima

Bachelor of Science Thesis

Supervisors:
dr. Claudio Matera
dr. Martin Rosema

s1619713

06.07.2017

Word count: 19601

Table of contents

Abstract

The use of civilian drones has been increasing in the last decade and a lot of concerns have been raised since EU regulation seems not to cover all of the aspects that the use of such drones implies. Drone regulation is a field where International, European and national law is applicable. Since many experts outlined many issues concerning the usage of civilian drones in the European Union, it is therefore worth analyzing the current regulatory framework on this issue. To this end, this paper provides a clear overview of the regulatory framework and identifies the gaps in legislation with regards to the privacy risks and personal data protection that arise from the use of RPAS. In addition to this, a clear distinction between the terms "privacy" and "data protection" will be made, as these two concepts are usually confused by the public. This paper focuses on the use of civilian drones, protection of privacy and personal data

of individuals and investigates to what extent the current EU regulatory framework for civilian drones respects the human rights protection standards such as privacy and data protection.

List of abbreviations

CAA	Civil Aviation Authority
CCTV	Close Circuit Television
CJEU	Court of Justice of the European Union
DPD	Data Protection Directive
EASA	European Aviation Safety Agency
EC	European Commission
ECHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EP	European Parliament
ESA	European Space Agency
EU	European Union
ICAO	International Civil Aviation Organization
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aircraft System
SESAR	Single European Sky ATM Research
UAS	Unmanned Aerial Systems
UAV	Unmanned Aerial Vehicle
UDHR	Universal Declaration of Human Rights
WP 29	Working Party Article 29

Keywords: civilian drones, RPAS, human rights, privacy, data protection

Chapter 1: Introduction

1.1 Background

During the last decades, people have put more emphasis on their privacy and protection of data, as these are part of their personal lives. Citizens feel uncomfortable when someone has access to their personal life, especially since the use of social platforms on the internet is very popular. The recent innovations in information technology challenge privacy and personal data of individuals, as a lot of personal information is being shared on the internet and usually made public, providing other people access to information which should not be available (Finn & Wright, 2016).

Within the 21st century, large amounts of data can be easily stored, processed and usually shared with others on the internet. For instance, nowadays it is easier for private companies to obtain information about their customers with the help of new technologies, by tracking down their IP addresses, geographic location et cetera.

According to the international expert on privacy, Daniel J. Solove, ‘‘privacy is an issue of power’’ (Solove, 2002). In his article on privacy, he claims that personal information should not be accessed by others, because otherwise it will result in exercising power on the individual whose information is shared. Each individual makes decisions based on personal data and therefore, this data can be used not only to influence our decisions or behavior, but also to produce us physical or mental injuries (Solove, 2002). In addition, privacy is associated with respect, since information that is private, is due to a specific personal reason, making others therefore disrespectful, if not complying with it. If individuals decide to keep private some piece of information, others will have to accept and respect this choice.

The aim of this research is to investigate the extent to which technological innovations, such as drones and their civilian usage, challenge fundamental principles of the EU legal system, like human rights protection standards. Recent highly developed technological innovations such as drones (also called UAVs - unmanned aerial vehicles) are currently sold on the market to private persons for recreational purposes such as ‘‘drone racing’’. In addition to this, drones are also

used by authorities, such as the police for surveillance purposes and for commercial and humanitarian practices (Finn & Wright, 2016). The use of civilian drones has been constantly increasing in Europe in the last two decades and it raises therefore concerns among experts in the field of technology regulation.

Apart from this, drone consumers should also be aware of the risks they are subject to, when handling drones. A study performed by the UK drone safety campaign in 2016 revealed that only 4% of the consumers are aware of the Drone code, which provides information on how to properly use civilian drones (Civil Aviation Authority, 2016). It is important for consumers to know that the data they capture, store and share on the internet is not legal since it is obtained without informing individuals and obtaining their permission. In addition, drones also pose ethical issues if they are used for research purposes, as data collected can be identified (vehicle license plate number for instance) and traced back to individuals without their prior consent.

The use of drone technology raises many issues from the perspective of privacy and data protection of citizens. Civilian drones are usually equipped with a video camera which can capture a lot of information, which mostly consists of personal data. Since individuals are not informed prior to being filmed, civilian drones gather personal data without any permission of the observed. In addition, it is almost impossible for the person who is observed by the drone, to identify the operator of said drone, as there is no kind of registration for civilian drones to this date. For instance, a drone is used for a longer period in the same spot, capturing all persons who are present at that location. If there are persons that do the same activities at the same point in time, such as arriving to work every morning at 9 am with the same car, the drone will capture this action. This way, the operator of the drone can search on the internet for the registration plate of the car and find out who its owner is. In this case, the operator of the drone obtained private information about that person without his/her consent, although at first sight this person could not have been identified. Of course, one might also argue that the problem does not lie with the drone, but the camera it is equipped with. Therefore, more information on this particular issue will be provided later in section 2.1 that deals with drones' applications.

Moreover, similar concerns on privacy and data protection were raised by the Google car taking pictures when developing the Google Street View program. The camera installed on the roof of

the Google Car took pictures in various cities around the world, capturing people entering strip clubs, picking up prostitutes or people who were just sunbathing in bikinis in their own backyard. Although Google defended itself that these pictures were taken from public property, due to the placement of the camera which was on the roof of the car, it also enabled it to capture images from private properties, violating therefore people's privacy. Individuals brought these cases into court as they thought that their privacy and personal data were put at risk. In the case of civilian drones, the situation does not differ a lot, as civilian drones can be easily raised in the sky without anyone's consent, challenging therefore privacy and personal data protection of individuals.

Thus, usually used for the purpose of surveillance and aimed at improving citizens' safety, drones have a direct impact on citizens' privacy and civil liberties (Finn & Wright, 2012). Contrary to their purpose, civilian drones have been found to be a threat to public safety, according to Clarke and Bennett Moses (2014). Due to the complex system of civilian drones, issues such as privacy and data protection should be adequately addressed by regulatory bodies of the EU.

As the European Commission promotes the use of drone technology, the EU must urgently address the issues on privacy and data protection that result from the use of civilian drones and govern these highly developed technological innovations in such a manner that they respect human rights protection standards. The topic of new technological innovations and how the EU attempts to govern them is rather new and a lot of aspects must be taken into account before developing a EU regulatory framework for civilian drones. It is important that any regulation that the EU develops, must comply with its founding principles, and therefore the regulatory framework for civilian drones must be very well established, taking all consequences and risks into account.

In addition, civilian drones are already available on the market, but there is no EU regulation for civilian drones of small size and weight, which means that the Member States are responsible for this category of drones. This study addresses a research question that, not only aims to find if there are any gaps in EU legislation with regards to the use of civilian drones, but also analyses if human rights such as privacy and data protection are protected by the current EU regulatory

framework: **To what extent does the current EU regulatory framework for civilian drones respect the human rights protection standards?**

Since this study embodies a lot of information on drone technology, concepts such as privacy and data protection, as well as human rights and European legislation, need to be properly defined and distinguished. To do so, in order to answer the main research question, five sub-research questions are needed for structuring this paper. In the section below, the five sub-research questions are listed in the order in which they will be answered in this paper and each of the questions will be provided with a separate chapter.

I. *To what extent does the use of RPAS challenge EU citizens' privacy and personal data?*
II. *Which regulators are involved in the regulation process of RPAS?*
III. *What kind of regulations on drone technology already exist in the EU?*
IV. *To what extent does the existing regulatory framework for drones protect the right to privacy?*
V. *To what extent does the existing regulatory framework for drones protect the right to data protection?*

1.2 Methodology

This section of the chapter is meant to outline the methods used in answering the sub-research questions. Each chapter is based on particular theories, legal articles or directives and therefore it is essential to present how this study will be performed.

The research method that will be employed in this paper is mostly legal research, as it focuses on human rights such as privacy and personal data protection on an International, European and national level. In order to provide a clear understanding of law application, relevant case law will be used to outline the decisions of the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR). Decisions taken by these two institutions, combined with the opinion of Article 29 WP, EASA's Prototype' Commission Regulation on Unmanned Aircraft Operations'', the Directorate General for Internal Policies document on drones, the Study on Privacy, Data Protection and Ethical Risks in Civil Remotely Piloted Aircraft Systems

Operations conducted by Finn and Wright for the European Commission and the SESAR JU Study, represent the basis on which this paper is written, as they provide enough information on the current and future regulations for civilian drones.

The research report will consist of seven chapters. The first chapter begins with background information to the topic of drones, followed by the methodology section and finally, the body of knowledge and theories, explaining the concepts of civilian drone, privacy and data protection. The analysis of this study will contain five chapters, in which the sub-research questions will be analyzed and answered, based on multiple documents, mostly documents dealing with policies and legislation of the European Union. European legislation will provide more insight of legitimacy when it comes to the use of civilian drones. This will create an optimal environment for analyzing which actions involving the use of drones are in accordance with the law and which do not respect the fundamental rights of the European Union. In order to clearly distinguish which issues are related to privacy and which are related to data protection, current EU regulations on drone technology will be consulted.

Furthermore, international case law, such as the M.S. v. Sweden or S. AND MARPER V. THE UNITED KINGDOM and previous research findings on drone technology, privacy or data protection will be analyzed as well, in order to distinguish the concepts of privacy and data protection. Some of the international case law is not related to both privacy and data protection, as these are separate issues. Reports released by the European Parliament or the European Commission are essential for this research, as EU regulations, articles, directives and declarations related to this topic are discussed in detail and therefore, the parts in legislation that seem to be missing or incomplete are easier to identify. As an example, the Directorate General for Internal Policies published a report on the use of civilian drones in 2015 which summarizes the type of drones that are currently available on the market, outlines their use and identifies the issues that may appear from using this kind of tools. In addition to this, The Single European Sky ATM Research Joint Undertaking (SESAR JU) developed a study related to the use of drones in the EU which provides useful information on the drone market and their capabilities. This study will be taken into consideration, as it identifies measures that the EU must adopt in order to benefit from the use of drones for developing its internal market.

As mentioned before, in order to perform this study, the analysis will be divided into two main blocks. The first block including chapters 2, 3 and 4 will deal with the EU regulatory framework, focusing on the EU as a regulatory body and its attempt to develop regulations on drone industry.

For the first sub-research question, discussed in the second chapter of the research paper, policy documents and legal documents on new innovations, such as the ‘‘‘Prototype’ Commission Regulation on Unmanned Aircraft Operations’’ and the ‘‘Notice on the Proposed Amendment on the Introduction of a regulatory Framework for the operation of drones’’ proposed by the EASA, The Regulation (EC) No 216/2008 and the Article 29 Working Party, will be analyzed in order to outline the current challenges for EU citizens’ privacy and data protection.

To continue, the following chapter will focus on the regulators for RPAS as these are present on different levels such as International, European and national level and usually their competences are bound to specific requirements. ICAO, EASA, JARUS and NAA’s role in developing regulations on civilian drones will also be discussed in detail. To do so, the paper ‘‘Civilian use of drones in the EU’’, published by the Authority of the House of Lords in 2015 will be used as the main reference for this chapter.

The last sub-research question of the first block will be discussed in chapter 4, and deals with current EU regulations for civilian drones. Since the main research question focuses on human rights, it is important to understand which regulations are already in place on the European level regarding technological innovations such as drones. As the regulatory framework is not codified in a single document, various directives and articles are meant to protect individual’s privacy and data protection rights; therefore, these must be identified in order to be properly analyzed later in chapters 5 and 6. For this chapter, the following documents will be used: Regulation 216/2008/EC, the Riga Declaration, the European Commission’s study on privacy, data protection and ethical risks performed by Finn and Wright in 2014 and EASA’s ‘‘Concept of Operations for Drones: A risk based approach to Regulation of Unmanned Aircraft’’, released in 2015. These documents will provide more insight into European regulations concerning the use of RPAS across the EU.

The second part of the analysis, which consists of the last two chapters, focuses more on the human rights perspective, especially on the right to privacy and the right to data protection, as

these seem to be challenged by the use of civilian drones. Chapter 5 will deal with the first sub-research question of the second block of sub-research questions, focusing on the right to privacy, while Chapter 6 will deal with the last sub-research question, focusing on the right to data protection. For these two chapters, the Treaty on the Functioning of the European Union and the Charter of Fundamental Rights of the European Union will be used to identify which articles guarantee the right to privacy and the right to data protection of EU citizens.

As a conclusion, drones and the applications they carry posed a number of issues in the last decade as they are usually equipped with video-cameras and other applications that can monitor heath, locate geographic position et cetera. In this regard, personal data, that are collected and processed afterwards, represents a serious threat to human rights, such as the right to privacy and data protection. In order to prevent these rights from being disrespected, many articles and policy documents have been published on this topic. These sorts of policy documents clearly outline that drone manufacturers and users must have respect for people's privacy and personal data, implying therefore that these are absolute necessary conditions for drones to be accepted by society. The most relevant documents that focus on this issue are the Article 29 Data Protection Working Party, the EDPS (European Data Protection Supervisor) and the final report on privacy and data protection written by Finn and Wright in November 2014 for the European Commission.

Policy documents of the Directorate General for Internal Policies regarding ''Privacy and Data Protection Implications of the Civil Use of Drones'' will be analyzed accordingly, in order to emphasize that there is a clear relationship between the use of civilian drones and privacy and data protection. As these documents are the most relevant for this study, they form the basis of the analysis that will be performed in the following chapters.

1.3 Body of knowledge and theories

1.3.1 Civilian drones

Within this chapter, terms such as RPAS, UAS or UAV will be introduced and concepts such as privacy and data privacy will be presented. In addition to this, prior knowledge to the topic of

civilian drones will be also outlined.

Terms such as drones, RPAS, UAS or UAV are frequently confused by people and therefore it is important to distinguish between them before analyzing the issue of drone technology per se. The most used term is ‘drone’ and due to its military purpose, it receives a negative connotation in the civil sector.

According to the International Civil Aviation Organization (ICAO) as laid down in its document ‘‘Cir 328/AN/190 on Unmanned Aircraft Systems (UAS)’’, drones are commonly defined as aircrafts that are operated without a human pilot on board. We distinguish between two categories of unmanned aerial vehicles (UAVs) (ICAO, 2011). Within the first category fall those that need a remotely human pilot to guide them, also called Remotely Piloted Aircraft Systems (RPAS). The second category of UAVs consists of those that are autonomous and do not need any interference of a human pilot. As indicated in the Directorate General for Internal Policies’ document PE 519.221, these definitions are acknowledged at international and EU level including the EC and EASA (Directorate General for Internal Policies, 2015).

For the purpose of this study, the term civilian drone will be used for Remotely Piloted Aircraft Systems (RPAS), which is most used by the European Commission in their reports. As this term already implies, RPAS need to be guided by a human pilot, who is usually on the ground controlling the movements of the flying object. RPAS consist of the aircraft and can be seen in the air, the ground station and the radio that enables the pilot station to communicate with the aircraft. The radio also called command and control link enables the pilot to download live data captured by the aircraft.

According to SESAR (Single European Sky ATM Research), the demand for RPAS is expected to reach around 7 million users by 2050, enabling people to use RPAS in their household activities or even commercial activity. Sectors such as Agriculture, Energy and Delivery will benefit most from these highly developed tools. Of course, RPAS differ, from small sizes and very light weight, such as 200g, to very large ones, with 40m large wings (SESAR, 2016).

Drones were originally developed for military and defense purposes and received worldwide attention after the US referred to them as ‘‘killer drones’’ since they were used for hitting targets

in various countries including Afghanistan and Pakistan. After using killer drones for military purposes, many actors raised international and human rights concerns regarding the legality of such actions. Thus, during the last decade, highly developed technological tools in the field of UAVs (reasonable price, effortless operation and lighter craft), received an enormous interest from the public for civilian purposes. In the last three years, the demand for civilian drones has rapidly increased, according to the Directorate General for Internal Policies which published a report regarding the use of civilian drones. This report contained the table below, which summarizes the current uses of drones, type of operators and their purposes (Directorate General for Internal Policies, 2015).

Table 1: Drones civil uses, operators, targets and examples of use

Uses	Type of operator	Targets, examples
Infrastructure protection, monitoring and safety / security inspections	Commercial State	Objects: - Transport (rail tracks, highways, bridges, traffic) - Energy (nuclear plants, dams, dykes, power grids, wind turbines, pipeline and power lines inspection) - Communications (mobile phone towers) - Industry (industrial installations) People: - monitoring unauthorised entry
Geo-spatial mapping	Commercial State	Objects: Mapping and surveying exploration, planning and crisis management
Environment monitoring	Commercial State	Objects: Air, water and other natural resources: pollution monitoring, hazardous material sensing, air/water quality testing, weather monitoring
Precision agriculture	Commercial Private individuals	Crop, animals: Crop and herd inspection, crop spraying to apply pesticides
Law enforcement, surveillance and monitoring of individuals and of people and of electronic communications	State (law enforcement) Commercial (sub-contractors)	Persons: Infrastructure protection against threats and illegal actions, targeted criminal investigation, crowd and public event monitoring, border control/protection, anti-social behaviour, supporting police response Geo-location, interception of communications and of electronic devices, profiling
Civil protection	State (law enforcement, civil protection authorities)	Objects, persons: Infrastructure monitoring, disaster relief and response, search and rescue, firefighting, hazard detection, crisis response
Regulatory enforcement	State (law enforcement, other authorities)	Pollution monitoring, fisheries monitoring, monitoring for illegal logging, wildlife protection and hunting regulations, etc
Journalism, media, film-makers	Journalists, camera-crews, film-makers	People and objects: Live journalistic reporting, investigative reporting, documentary filmmaking, promotional videos, fictional filmmaking
Electronic communications providers	Commercial (service providers)	Objects: Telecommunication and computing devices
Hobby, leisure	Private individuals	Objects and persons

NB: Commercial = companies, professionals.

As shown in the table, the last entry consists of drones used for hobby and leisure by private individuals, that usually track and monitor objects and persons. For this category of RPAS, this report will use the term 'civilian drone'.

When it comes to the types of drones, they can differ due to weight, control system, speed, range, flight endurance and power unit, and lift technology. Another table provides more information on the type of drones, as these are divided into three categories based on their weight: small (0-20/25kg), light (20/25-150kg) and large (>150kg).

Table 2: Different categories of drones on the basis of weight

Type on the basis of weight (MTOM)	Current uses and future potential uses	Description; Types; Price and diffusion	Regulation
Small (0-20 / 25 KG)	- Leisure use and commercial use (surveillance and inspection, photography)	- drones below 2 kg are also called micro-drones and are quickly developing - hundreds of different types; normally multi-rotor or fixed wing aircrafts, guided by GPS, live video streaming camera, - Price: 140 - 28.000 Euro Some available in shops (below 1 kg) - Take-up: those below 2 kg are very widespread	- Falls under MSs regulations
Light (20/25 - 150KG)	- geospatial surveying, wide-area surveillance - Potential to inspect pipelines/power cables, spray crops, search and rescue, border surveillance; forest fire monitoring	- Typically longer range, fixed-wing, B-VLOS, reaches altitudes of 3000 meters - ex: Luna, Hermes 90 - Price: 55.000 - 420.000 Euro	- Falls under MSs regulations
Large (>150KG)	- used by the military and defence - Potential for future cargo (and passenger) transport	NATO classifications: - Class II (150-600 kg): Sperwer, Hermes 450, Watchkeeper; - Class III (>600 KG): MALE - medium altitude, long endurance: Predator, Heron, Hermes 900[6] HALE - high altitude, long endurance: Global Hawk UACVs - strike or combat UAVs: MQ9-Reaper/Predator B Price: 670.000 Euro and above	- Falls under Regulation 216/2008/EC (EASA Regulation): EASA airworthiness certificate, unless operated by a State agency

NB: based on the House of Lords report Table 1 and the Commission study on privacy, data protection and ethical risks in civil RPAS operations.

According to the table above, which was developed by the DG for Internal Policies on civilian drones, small drones (0-20/25kg) are commonly used for leisure and commercial use such as

inspection, surveillance or photography (Directorate General for Internal Policies, 2015). Since they are not expensive (starting from ca. 140 Euro), hundreds of different types of those below 1kg or 2kg are to be found in stores, enabling the public to use drone technology for civilian purposes at a lower, with the larger drones used by the military.

1.3.2 Privacy and Data protection

Many scholars have criticized the introduction of new technological innovations such as drones, as they have broadened their area of purpose, from military to civilian practices (Finn & Wright, 2012). The use of drones has received special attention from many experts in the field of technology, as they are challenging civil liberties, as mentioned in one of the EU Commission working papers (European Commission Staff Working Document, 2012). Specialists from the field of privacy such as Daniel J. Solove, claim that privacy is a complex concept, which does not have a clear definition, but usually consisting of diverse dimensions such as ‘‘privacy of the person, privacy of personal data, privacy of personal behavior and privacy of personal communication’’ (Finn & Wright, 2012). Privacy seems to be usually related to family habits, which includes protection of personal data, making it a human rights issue.

In addition, in their article, Finn and Wright discuss the challenges of using unmanned aircraft systems for surveillance purposes upon privacy (Finn & Wright, 2016). The authors reveal that in the European Union privacy issues are not receiving enough attention from the legislative regulatory bodies when it comes to the use of UAVs, due to their multiple technologies.

In 2016, the same authors wrote another paper addressing the issues of privacy, data protection and ethics resulting from the use of drone technology. They state that the drone industry, due to its products and operations and private operators put privacy, data protection and ethics at risk because drone producers lack the knowledge about EU legislation. The lack of knowledge on EU regulations is a main cause for putting privacy, data protection and ethics at risk. The higher the lack of knowledge on EU standards, the higher the risks of privacy, data protection and ethics is (Finn & Wright, 2016). Causal relationships between drones and privacy/data protection/ethics are identified. The term privacy is often associated with location, behavior and body characteristics. Another positive causal relationship between private operators and privacy is

revealed, as private operators, which are often migrants, young people and workers, are the most likely to affect privacy. This study emphasizes that with the help of a drone, civil persons can obtain information regarding someone's location, can establish a connection regarding the things he/she does and can collect data about his/her appearance, which is often stored and uploaded on the internet. This way, with the help of drones, individuals can unintentionally obtain private information about another person, putting at risk fundamental rights such as privacy and data protection, as codified in Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union.

The use of drones as such is not causing any issues, but the applications drones carry, such as video cameras that can capture audio and video data, challenge individual's right to privacy. In addition, these lightweight drones can fly over walls or fences or even enter buildings where they are not allowed to. Individuals are therefore unaware of the fact that they are being recorded and have no control over the processing of the video/audio footages. It is important that data captured with the use of drone technology does not challenge the privacy of the subjects. It is crucial that users and manufacturers are aware of these challenges to privacy and data protection. If personal data is collected via cameras or any other type of sensors that are installed on the drone, data protection legislation applies, meaning that without prior informed consent of the subject, security measures or anonymization of data, this type of surveillance is not acceptable and is unlawful. For drone users, it is not easy to obtain a freely given informed consent. These issues address the gaps in EU legislation regarding drone technology. Users are not required to use symbols, signals or lights, registration plates or to publish any information in the local newspaper, radio or on the internet regarding future drone activities, so that subjects can identify a certain drone. This results in a lack of control for subjects over their privacy and also private data.

Moreover, users that collect personal data by using drones must safely store the data. For this kind of data, it is advised to use encryption, so that only people with a specific decryption key or password/code can access it. These types of legal issues that are connected with drone technology are very much alike those that the Google Street View Car faced. The only exception is that in case of the Google Car, is that subjects were aware of it as the car was being driven on

the streets, wrapped in the company colors, showing the company name to the public. Besides this, it was obvious that the car was collecting images, since a huge camera was placed on its roof. In this case, people could trace the car back to the company or file complaints to the police based on the registration plates. Although the case is very similar, since both the Google Car and the drone are equipped with cameras that collect private data, the drone seems to be more problematic in this regard, as it cannot be traced back to its user. In addition to this, in case of accidents, drones are not insured, making it impossible for damages to individuals or things to be refunded.

1.3.2.1 Concept of Privacy

Many experts from the field of privacy such as Solove, Sommer, Grosse or Wolfe tried to explain the concept of privacy, but they provide different definitions of privacy because the term ‘‘privacy’’ does not have a clear definition. Thus, the word ‘‘privacy’’ comes from the Latin ‘‘privatus’’ which means private, separate.

According to the study on privacy and data protection performed by Finn and Wright, there are seven dimensions of privacy that must be taken into consideration with regards to highly developed tools such as RPAS. These include privacy of the person, privacy of behaviour, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and finally, privacy of association (Finn & Wright, 2014).

Starting with the first dimension of the concept, the privacy of person is associated with the right of persons to keep their body characteristics private. Secondly, the privacy of behaviour refers to the liberty of individuals to behave without being under any type of observation. Thirdly, privacy of personal communication includes all forms of communication such as emails, phone calls, SMS, letters et cetera. Another dimension is privacy of data and image, commonly referred to as data protection, which protects personal data of individuals. In addition, there is privacy of thoughts and feelings, as individuals are free to keep their thoughts and feelings private and not share them with others. The sixth dimension of privacy that Finn and Wright identified is called privacy of location and it enables people to change their location from one place to another, without being monitored. Finally, the privacy of association deals with the issues related to the

freedom of individuals to gather in groups (Finn & Wright, 2014).

1.3.2.2 Concept of Data Protection

The concept of ‘‘data protection’’ is a rather new concept, as it emerged with the invention of the personal computer (PC). Since the concept of privacy mentioned above was not so complex, in order to address all of the concerns raised by the latest innovations, the concept of ‘‘data protection’’ was developed. This concept was created for protecting individuals from eventual abuses of authorities or private parties with regards to the collecting, processing and storing of their personal data.

Although privacy and data protection are similar to some extent, they differ because the concept of privacy is too broad, while data protection is better defined, as it will be revealed in chapters 5 and 6 that deal with the EU laws protecting these two fundamental rights. While the concept of privacy is more related to the intimacy and secrecy of the individual, the concept of data protection can be employed as *corpus juris*.

The concept of data protection caught the attention of many scholars, being therefore subject to many legal instruments. In the following section, the applicable EU legislation for privacy and personal data protection of citizens will be outlined, by identifying those applications that raise concerns when using RPAS technology.

Since the EU aims to promote its values, it is necessary that RPAS used for civil practices and their applications are regulated in such a manner that does not interfere with its fundamental rights, especially with privacy and data protection. The regulatory framework protecting these fundamental rights in the EU consists of both European and national law. For the purpose of this study, a short timeline of the measures concerning the use of drone technology that, at the same time protect human rights such as privacy and data protection, will be presented in the following section.

1.3.3 Applicable EU legislation

In April 2014, the European Commission submitted a document consisting of new measures that can regulate the use of RPAS. The goal of these new measures was to ensure safety and security, privacy and data protection of its citizens. In June 2015, a report on the safe use of drones was communicated to the Committee on Transport and Tourism and a couple of months later, on the 29th of October 2015, it was adopted by the European Parliament. One year later, on the 8th of December 2015, the revised version of the **EASA Basic Regulation 216/2008** was adopted by the European Commission in order to provide safety rules for drone users. Within the same month, the EASA released a **Technical Opinion** concerning legislation for low-risk operations of UAS that is very likely to be changed or amended. Although some Member States such as the Netherlands, Germany, Poland or Romania have already taken some measures in this field, they must comply with new EU legislation. Later in April 2016, the European Council adopted a new regulation and directive on data protection, which on the 4th of May 2016 were officially published in the EU Official Journal. **Regulation 2016/679** regarding processing of personal data entered into force on the 24th of May 2016 and shall apply starting the 25th of May 2018. **Directive 2016/680** on the protection of natural persons regarding the processing of personal data by competent authorities, entered into force on the 5thof May 2016 and all Member States must convert it into national law by the 6thof May 2018 at the latest.

In addition to this, **Article 8** of the Council of Europe Convention on Human Rights ensures EU citizens the right to respect for one's ''private and family life, his home and his correspondence''. The rights guaranteed by Article 8 are the same to those which are codified in **Article 7** of the Charter on Fundamental Rights of the EU. In line with **Article 52(3)**, this right is the same as the corresponding article of the ECHR.

Article 8 of the Charter on Fundamental Rights of the EU relates to protection of personal data. The protection of individuals in the context of processing personal data is also codified in the Council of Europe Convention 108. The **Recommendation R (87)15** of the Committee of Ministers deals with cases in which personal data is used in the police sector. The same is protected by the **Recommendation CM/Rec (2010)13** of the Committee of Ministers.

To continue, **Directive 95/46/EC** of the European Parliament and of the Council of the 24th October 1995 state that individuals are protected with reference to the processing of personal data and on the free movement of such data. On the 27th of November 2008, the **Council Framework Decision 2008/977/JHA** came into force, protecting personal data that is processed in criminal matters. This decisions and directives were based on the **Regulation (EC) 45/2001** of the 18th of December 2000 (processing personal data by the EU bodies) and **Directive 2002/58/EC** of the 12th of July 2002, also called the Directive on privacy and electronic communications. **Directive 95/46/EC** can be applied in the context of processing personal data collected by drones, by both private and public entities. If personal data is shared on social networks, the rights guaranteed by the Directive can be brought to court. Personal data collected from public space is not part of the exemption to this directive (with regards to household exemption) and therefore it would fall into **EU Data Protection law.**

There are more articles and directives that guarantee individuals' privacy and personal data protection with regard to the use of drones such as **Article 4(2) TEU** or exemptions provided in **Article 9 and Recital 17 of Directive 95/46/EC**, but these do not apply to private entities, but to media and journalists' purposes, intelligence national services or to commercial/professional purposes. Having said this, **Article 4(2) TEU** and **Article 9 and Recital 17 of Directive 95/46/EC** will not be part of the analysis performed in chapters 5 and 6, dealing with human rights such as privacy and data protection rights.

Chapter 2: Challenges for civilian drone operators

Unmanned aerial vehicles (UAVs) were originally associated with military purposes because drones were used by the US Army to carry missiles. At the moment, drone manufacturers also develop drones for civilian purposes and therefore the usage of civilian drones has been increasing in everyday life, making the UAV industry a business of billions of dollars. Thus, the increase in these highly developed tools brings a lot of risks and responsibilities. In order to understand what kind of risks and responsibilities arise from the use of drone technology, the following sub-research question must be answered: **To what extent does the use of RPAS**

challenge EU citizens' privacy and personal data?

It should be also mentioned that in this chapter only the risks/consequences of using civilian drones will be discussed, leaving the field of drones used for other purposes out of the question. Since the use of civilian drones per se is not problematic, but the applications drones carry pose a lot of risks, the first section of this chapter will deal with these applications as they are the reasons why human rights such as the rights to privacy and personal data protection might be challenged. In addition, in the second and third section the risks to privacy, respectively the risks to personal data protection with regards to the use of civilian drones, will be presented.

2.1 Drone applications

As already mentioned in the previous chapter, civilian drones are RPAS that need a human pilot on the ground in order to guide them. For this operation, the drone is equipped with various applications, including video-cameras so that the pilot can see objects that can appear in the way of the drone and avoid collision. They usually capture images or video images and with the help of specific software the user can experiment with more applications. For instance, advanced software applications enable facial recognition, movement detection, recognition of registration plates, thermal and Wi-Fi sensors, night view mode, radar, identify location via GPS systems etc. In this regard, drones and the applications they carry imply collection, recording, storing, processing and use of data, allowing the user to identify individuals both directly and indirectly. These types of activities pose new challenges in relation to the right to privacy and data protection of persons.

To continue, the WP 29 and the EDPS performed a couple of studies that outline that drone activities challenge privacy and data protection of citizens. RPAS and the applications they carry, change the competence of surveillance in comparison with satellites, helicopters or CCTV, as they are usually not visible or detectable. In the table presented in the previous chapter, it was underlined that microdrones (below 2kg) are quickly developing making surveillance even more sophisticated. As an example, with common CCTVs the user has limited views of the objects (bird's eye view or fixed view), but RPAS allow mobile view, including 3D. Due to their size, RPAS can enter more locations than other surveillance tools, including private properties, and

can monitor activities of individuals without being noticed. According to the second table of the first chapter, prices for microdrones start around 140 Euros which makes it possible for a huge number of persons to buy and use a drone. Due to their capability of surveillance and tracking people, the use of civilian drones raises concerns in the field of privacy and data protection.

In addition to this, in the last years there have been reported some minor accidents and attacks that involved the use of RPAS. According to a press release of the FBI (Federal Bureau of Investigation), a 26-year-old US graduate student was arrested in 2011 for ‘‘Plotting Attack on Pentagon and U.S. Capitol and Attempting to Provide Material Support to a Foreign Terrorist Organization’’ (FBI, 2011). In the EU, there were also some incidents, as in 2014 in France, UAVs had been spotted near nuclear power plants which are not permitted by the French law (The Guardian, 2014). Another incident took place in Tokyo on the 22nd of April 2015 when an UAV landed on the roof of Japan’s Prime Minister Shinzo Abe’s residence, equipped with radioactive materials (Ripley, 2015).

In this context, it is very likely that UAVs can be also used for terrorist purposes, as these tools can be loaded with artisanal bombs or explosives. According to EASA, the EU will face high threats from terrorist organizations that are using drone technology in the future, as explosives can be placed on different places (EASA, 2017).

For the moment, current challenges to the EU regarding the use of civilian drones include privacy, data protection and ethical risks (EASA, 2017). For the purpose of this study, the main focus will be on the right to privacy and data protection. According to the study on privacy and data protection performed by Finn and Wright and published in 2014 at the request of the European Commission, the risks to **privacy** entail ‘‘the chilling effect for being watched, dehumanization of those under surveillance, transparency and visibility, accountability and voyeurism, function creep, bodily privacy, privacy of location and space, privacy and association’’(European Commission, 2014) and the risks to **data protection** include ‘‘transparency, data minimization, proportionality, purpose limitation, consent, accountability, data security, rights of access, rights of correction, 3rd country transfers, rights of erasure’’ (European Commission, 2014). These types of risks caused by the use of civilian drones will be presented and analyzed in the sections 2.2 and 2.3.

2.2 Privacy risks

Function creep

According to Roger Clarke, the phenomenon of function creep occurs when RPAS are used for other purposes than purchased or intended. For instance, real estate agents or private entities purchase a drone for filming the object they want to sell, such as an apartment, studio, house, building et cetera, but also to present the neighborhood in order to strengthen their selling chances. This implies that people, vehicles or backyards are also captured on video from the sky through civilian drones, without their consent (Clarke, 2014).

Another example is the Canadian police, since it is using drones for surveillance, and captures images and videos in order to obtain information about traffic incidents or crimes. Apart from this purpose, on the videos that are captured through drones, the police can also identify vehicles that are exceeding the speed limit, based on their plate numbers. In turn, the Canadian police can issue speeding tickets based on these video footages, although this was not the purpose of using the drone (Finn & Wright, 2012).

Chilling effect

According to the study of Finn and Wright, people who are aware that are being watched, start to behave differently than they usually do. In the case of civilian drones, this issue is also present, as by the time people realize they are being watched by a drone, they start behaving differently than before. According to Finn and Wright, it has been scientifically proven by philosophers such as Jeremy Bentham and Michel Foucault that people change their behaviour when they are aware they are being watched (Finn & Wright, 2014). This way, their right of exercising their civil liberties is challenged. For instance, a family is having a barbecue on a Saturday in their backyard and they observe that a drone is capturing this moment. Since they cannot know who is filming them and for which purpose, they start changing their actions and movements, as they are being watched. Moreover, Roger Clarke states in his paper on drones' impacts, that behavioural privacy is the most challenged dimension of privacy by the use of civilian drones (Clarke, 2014).

In addition, current CCTV systems used in public places such as in front of banks or in bus stations will be replaced in the future by drones equipped with smart cameras that are able to detect people who are behaving abnormally or differently; this way, public safety will increase and the chance of future terrorist attacks for instance, will decrease, but on the other hand, this implies that people will be under permanent surveillance in public places. If these drones cannot be easily detectable from the ground, people will have no idea about the applications the drone is carrying such as microphones, video-cameras, recognition sensors etcetera. In other words, citizens are unable to find out if they are being observed or not. Furthermore, although they might observe the presence of the drone, they will not be able to identify its owner, being it a marketing company, an authority of law enforcement or a simply person using it for leisure.

Dehumanization effect

Although RPAS by their nature operate without a human pilot on board, they need a pilot in order to be guided to their targets in surveillance missions such as the ones presented in the section above. This means, that pilots who are usually kilometers away, are not physically and psychologically involved in the observation process. For instance, in missions aimed to espionage persons or activities that are performed in a specific area, there were needed some persons to perform the operation. Currently, all of this can be done with the help of RPAS, as they can fly over the area and capture everything that is happening there, or even enter buildings through the windows. This means, that the use of RPAS dehumanize, as the physical and psychological human intervention is no longer needed (Clarke, 2014).

In addition to this, it is expected that the use of RPAS for this kind of missions will increase, especially in the field of law enforcement. Authorities will use the data collected as evidence and present them before courts, but in this situation, it should also be taken into account that bugs or other software related problems might appear.

Transparency, accountability, voyeurism

Using RPAS for tracking and monitoring purposes usually means that the drones cannot be detected and this implies that in most of the situations when people felt being watched, they

could not identify the operator of the drone from the ground. Due to their small size, civilian drones are almost invisible if they are used in public places for capturing images, videos or intercepting phone calls among people. This way, surveillance becomes invisible and the lack of transparency implies that civilian drones used for surveillance purposes raise transparency concerns.

Apart from transparency issues, another risk to privacy caused by the use of civilian drones is related to accountability, as the operators of the drone cannot be easily identified by the ones being watched. In this context, everyone possessing a drone that is loaded with a video camera can monitor other people, without being caught. Therefore, according to the Commission study, it is absolute necessary that civilian drones must be registered to national aviation authorities so that their operations can be performed in a legitimate and lawful way (European Commission, 2014).

Nevertheless, the use of civilian drones also affects the privacy of individuals, since most of the drone operators are using these tools for voyeuristic activities. Civilian drone operators usually use these kinds of RPAS for hobbies and therefore there is no need for a license within the EU at the moment. Under current EU regulations, civilian drone operators do not need authorization for these activities and this is why many people purchase drones for stalking or harassment.

Bodily privacy

One of the dimensions of privacy is bodily privacy and it is challenged by drone applications such as face recognition, finger prints, iris recognition, hand geometry et cetera. RPAS that are equipped with such applications and use them to identify persons, definitely challenge the bodily privacy.

In the Netherlands, the Minister for Safety and Justice stated in 2014 during a session of the Tweede Kamer that he does not exclude a future with drones that are equipped with facial recognition. Biometric analysis is already used by Facebook and LinkedIn, and many other sectors such as the security sector and the commercial sector could use this technology. For instance, drones that are loaded with such applications could be used in the commercial sector for

recognizing consumers, based on their face or iris and recommend them products related to their purchases from the past (European Commission, 2014).

Privacy of location

There are few RPAS that possess applications such GPS, Automatic Number Plate Recognition (ANPR) or video cameras that are able to transmit video footages instantly, violating therefore individuals' privacy of location. Privacy of location or commonly known as the privacy of space, refers to the right of persons to freely change their location, without being identified or monitored (Finn & Wright, 2014). Since RPAS through their applications can track individuals and obtain their geographic location in different places at different times, this implies that the user of the drone can track another person's movements. Moreover, collecting a person's movements may result not only in a privacy issue, but also a personal data issue.

Associational privacy

Another dimension of privacy is the associational privacy. The term refers to the freedom of association of people, and it is a potential risk that can rise from the use of RPAS. As drones equipped with GPS can track persons, they can also track a group of persons doing certain activities. This kind of operations must be taken into consideration especially when drones are equipped with a GPS system and video-camera, as these can pose serious risks to other people. For instance, let us assume that a person buys a civilian drone and plans to use it for identifying anti-social activities in his area of residence, that are committed by teenagers. He monitors the group of teenagers that gather on the street every evening and with the help of the civilian drone, he decides to track them in order to identify their homes. Due to the small size of the drone, the teenagers are not aware about the fact that they are observed.

As a general conclusion of this section, RPAS that are equipped with video cameras and other applications such as GPS or ANPR, raise serious privacy concerns due to their abilities to track and monitor persons. Therefore, civilian drone operators who are using drones for leisure or hobbies must also take into consideration these issues, as they can challenge the right to privacy of persons.

2.3 Data protection risks

Data protection risks arise from the use of civilian drones on the type of applications that are equipped to the RPAS, just like the privacy risks. In this section, the most common risks of data protection related to the use of civilian drones will be outlined, as they can be used among other purposes for data collection.

Invisibility of data collection

Due to their size, RPAS can collect data without being recognized and therefore individuals who are being watched or monitored are not aware of this. Drones can not only collect personal data such as photos, videos or sound but also transfer the data at the same time the subject is being watched. This process is invisible, as the drone operator can be hundreds of meters or even kilometers away from the observed. Most of the individuals, who were being watched, were not aware that photos or videos of them were being collected, processed and even shared with third parties.

Mass collection of data

Since civilian drones can access almost any location, they collect enormous amounts of personal data. Although RPAS are used for a specific purpose, in order to fulfill this purpose, they also, accidentally collect a lot of data that in most of the situations is personal data of individuals. As an example, a drone that is used in the field of construction, apart from its purpose to monitor the evolution of the construction, it also collects images of people near the building which is under construction. Although the purpose of the video-camera loaded on the drone is to monitor different wings of the building, in the background there can also be seen the neighbour's backyard, which can be regarded as personal data.

Furthermore, similar to privacy, the images collected by RPAS that are used by the police to capture the moments of a car accident, can also be used afterwards for issuing speeding tickets to other traffic participants that disobeyed the traffic rules.

Disclosure

In order to assess the use of drone technology for collecting data, two elements must be accorded special attention: the Wi-Fi connection and the private use. The risks for personal data collected through RPAS' applications in case of disclosure are increasing dramatically due to these two elements. This is because, through the wireless communication between the drone and the operator, personal data of individuals can be put at risk by satellites or hackers for instance. Although there were not many cases when hackers took control of drones and the data they were collecting, these scenarios can happen and it is very difficult, or even impossible to identify the hackers.

The second element mentioned above is the private use of individuals, as they are not aware about the risks they can pose related to data protection, in case they disclose the collected data. As most of the current civilian drone operators equip their drones with GoPro cameras for a better imagine quality, let us imagine what happens if technologies such as facial or iris recognition become more accessible for the broader public. According to the Commission study on privacy and data protection, the answer is that the number of drones equipped with such applications will increase and with it, so will the number of abuses and disclosure concerns (European Commission, 2014).

Profiling

Another data protection risk is the so called ''profiling'' of personal data. According to Schermer, data collected through remotely piloted aircraft systems can be correlated with the data that is already stored in databases in order to identify persons or objects (Schermer, 2011). This kind of activities can be performed in the commercial sector or even for combating terrorism. For instance, RPAS can be used for marketing purposes, identifying customers based on their previous purchases. Moreover, selling companies could use RPAS loaded with video-cameras, GPS and face recognition for tracking and identifying their customers based on the cars they drive and their addresses, in order to perform targeted advertising.

Summing up this section, RPAS that are equipped with video-cameras and other applications such as GPS and facial or iris recognition raise serious data protection concerns due to their abilities to identify individuals for various purposes. Therefore, civilian drone operators must be aware of these issues, as they can challenge the right to personal data protection.

2.4 Conclusions

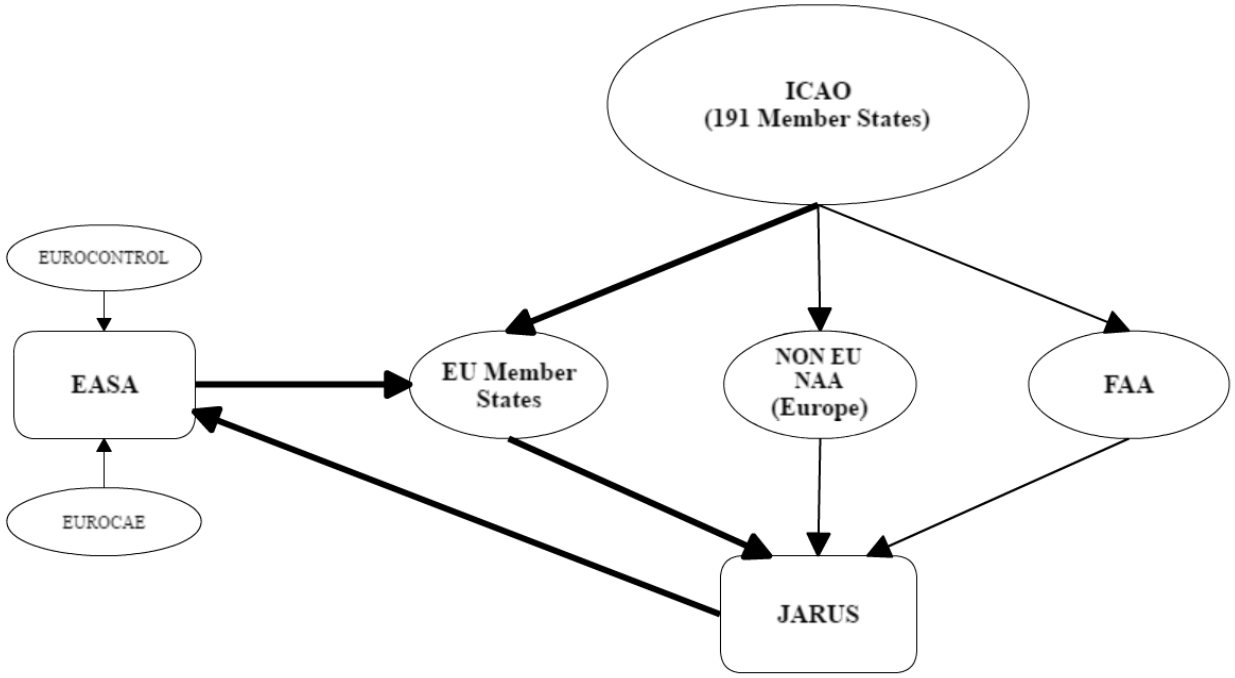
The aim of this chapter was to outline that the use of civilian drones per se is not problematic, but the applications that are loaded on the drones. For instance, GPS systems, facial and iris recognition and video-cameras can be mounted on RPAS, enabling the drone operator to collect personal data about his subjects.

In addition to this, the most common privacy and data protection risks that arise from the use of civilian drones have been identified, since most of the drone operators collect massive amounts of personal data without the prior consent of the observed. Nevertheless, while being watched, individuals begin to behave differently, which raises the issue of behavioural privacy. Civilian drone operators must be aware of all the risks presented in this chapter, although they intend to use the drone for different purposes such as for leisure or hobbies.

Chapter 3: RPAS Regulators

The purpose of this chapter is to find answers to the second sub-research question posed in this paper, namely: **Which regulators are involved in the regulation process of RPAS?** Therefore, this chapter will deal with RPAS regulations on different levels and identify which regulatory bodies can develop legislation for the use of RPAS. Since there are many types of regulators involved in the regulation process of RPAS, this chapter will outline the authorities that are responsible for RPAS regulation on international, European and national level. In order to understand how regulation for the use of RPAS is being developed, the flow chart below will help identify all the regulatory bodies, from international level to European and national level.

The following flowchart[1] is a revised version of the one published by the Authority of the House of Lords and includes all authorities involved in the regulation process of RPAS.



As it can be seen in the flowchart above, regulations for RPAS begin with the International Civil Aviation Organization (ICAO), which drafts regulations on an international level, to the EU Member States, Non-EU states and FAA (Federal Aviation Administration). These three provide input to the Joint Authorities for Rulemaking on Unmanned Systems (JARUS) which in turn drafts regulation proposals for the use of RPAS to EASA (The European Aviation Safety Agency). EASA is the regulatory body of the EU that provides regulation for the current 27 EU Member States.

This flowchart presents all levels of regulators for RPAS: on the international level there is ICAO, on the European level there is JARUS and EASA with its agencies EUROCONTROL and EUROCAE and finally, on the national level there are the EU Member States that regulate the use of RPAS. In addition to this, on the left side of the diagram, the arrows are thicker than the

[1] The original version of the flowchart describing the type of regulators for civilian drones has been published by the Authority of the House of Lord on 5th of March 2015. It can be retrieved from: https://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/122/122.pdf

ones on the right side. The reason for this is to catch the reader's attention as the left part of the diagram is the most important for this study, as the focus of this study is on European legislation. It should be also mentioned, that for the two agencies (EUROCONTROL and EUROCAE) that provide input to EASA, a smaller font size has been used since these two agencies are EASA's smaller agencies.

As there are three levels of RPAS regulators according to the flowchart above, in the following sections each of them will be discussed in detail. To do so, firstly, their purpose in the international arena has been identified and secondly, the provisions that allow them to regulate RPAS will be analyzed. This being said, section 3.1 deals with RPAS regulators on an international level, section 3.2 identifies RPAS regulators on a European level and section 3.3 points out RPAS regulators at a national level.

3.1 RPAS Regulators on International level

Since the early twentieth century, aviation has become an international activity; the International Civil Aviation Organization (ICAO) was established in 1944, as nations signed the **Convention on International Civil Aviation**, also known as the Chicago Convention.

ICAO is an international organization that develops Standards and Recommended Practices (SARPs), aiming to provide support to states when drafting national aviation regulations. Each member of ICAO has at least one national aviation agency (NAA) (few member countries have more aviation agencies) that deals with civil aviation practices such as licensing pilots or providing ATM (air traffic management) services.

According to **Article 8 of the Chicago Convention**, all kind of RPAS, regardless of size, weight and form are not allowed to fly over another state's territory without its permission (Chicago Convention, 1944).

The UASSG (Unmanned Aircraft Systems Study Group) established by ICAO in April 2007, consisted of experts on aviation from the member countries, stakeholders and industry groups, which analyzed the challenges posed by RPAS to aviation regulation. Due to the accelerated use

of RPAS, later, in November 2014, the UASSG revealed that by the end of 2018, RPASP (Remotely Piloted Aircraft Systems Panel) will pursue the work of the former UASSG in order to maintain the level of safety in aviation activities by developing a manual on the use of RPAS.

3.2 RPAS Regulators at the EU level

The European Aviation Safety Agency (EASA) was established in 2003 and it is located in Cologne, Germany. It performs regulatory activities for any aircraft operations within the EU. According to the EU **Regulation 216/2008**, EASA is entitled to regulate only RPAS over 150 kg, implying that for RPAS below 150 kg, EASA is no longer responsible and this kind of RPAS are subject to regulations developed by the national aviation agencies of the Member States (NAAs). EASA performs its tasks with the help of another two agencies, EUROCONTROL (European Organization for the Safety of Air Navigation) and EUROCAE (European Organization for Civil Aviation Equipment).

EUROCONTROL represents an intergovernmental organization consisting of 41 Member States and another 2 Comprehensive Agreement States. The aim of this organization is to create with their partners a Single European Sky, helping European aviation to prevail against challenges to safety, capacity and performance. Air traffic operations that are performed within European territory are to be done safely and efficiently, without harm to the environment.

EUROCAE is a non-profit organization, established in 1963 in Switzerland, which focuses on electronic equipment for aircrafts, providing aviation standards for airborne and ground systems. The specifications for airborne electronic equipment that EUROCAE developed, was approved by the 1967 ECAC (European Civil Aviation Conference). ECAC suggested that specifications proposed by EUROCAE are relevant and since then they form the basis of national legislation. In addition to this, **Regulation (EC) No 552/2004** of the 10th of March 2004 supports EUROCAE in managing European aviation standards.

Furthermore, the Joint Authorities for Rulemaking on Unmanned Systems (JARUS) consist of a number of experts from the EU Member States, NAAs and FAAs, who work together on drafting proposals on technical, safety and operational requirements for the use of UAS. This organization advises EASA in order to develop European standards regarding the use of UAS, including

RPAS. In this regard, JARUS also takes part in regulating RPAS at the European level.

3.3 RPAS Regulators on National level

As mentioned previously, regulation for light RPAS (below 150kg) is no longer the responsibility of the EASA, as this kind of regulations fall under the jurisdiction of the Member States. All Member States have their own NAA/NAAs (National Aviation Authority) regulating aircraft operations. For instance, in the Netherlands, the Ministerie van Infrastructuuren Milieu: Inspectie Leefomgevingen Transport is responsible for the use of RPAS below 150 kg.

Since most of the RPAS used for civilian purposes fall under the category of RPAS below 150 kg, where EASA has no competence, member states' NAAs have their own regulations on the use of RPAS. In this regard, according to The Royal Aeronautical Society, increasing EASA's competence might be a good idea, as all RPAS of the same category could fall ''under identical regulatory rules as the rest of the European Union'' (Royal Aeronautical Society, 2014).

3.4 Conclusions

The purpose of this chapter was to identify the regulators of RPAS and analyze their position in the international arena by identifying their area of intervention and their competences in order to clarify the role that the EU can play in this domain. To do so, section 3.1 identified ICAO as the RPAS regulator on international level, section 3.2 revealed that EASA is the main regulator on European level, but JARUS and the agencies EUROCONTROL and EUROCAE also play a significant role, and finally, section 3.3 outlined that there can be more types of regulator(s) on national level, for instance in the Netherlands there is the Ministerie van Infrastructuuren Milieu: Inspectie Leefomgevingen Transport, that regulates RPAS below 150 kg. However, as EASA has no competence for regulating RPAS with a total mass below 150 kg, national aviation agencies of the Member States are responsible for providing rules on the use and production of RPAS.

As the role of the EU was clarified, the next chapter will deal with the current EU regulatory framework in order to identify which regulations are applicable with regards to the use of RPAS.

Chapter 4: EU regulatory framework for drones

The purpose of this chapter is to answer the third sub-research question of this study: **What kind of regulations on drone technology already exist in the EU?** While the previous chapter focused on the authorities that are responsible for developing regulations for the use of RPAS at different levels, in this chapter, current European regulations for the use of drone technology will be identified and analyzed. In addition to this, the position of EU institutions, bodies and agencies with regards to the drone industry will be outlined in order to clarify their opinion on the regulatory framework for RPAS within the EU.

This chapter will be divided into two parts. The first part will contain two sections and will focus on soft law measures that include the position of the European Commission and Parliament, Council of the European Union and EASA. In addition to this, the Commission's COSME will also be presented, as it plays an important role for the users of drone technology. The second part of this chapter will concentrate on the hard law measures, including current regulations for RPAS use, namely Regulation 216/2008/EC and the Riga Declaration.

4.1 Position of the EU institutions, bodies and agencies

4.1.1 European Commission

For almost three decades, the EU Commission has been promoting the drone industry and strives for a strong EU aviation market. In comparison with other countries/regions, the EU is the leader when it comes to civilian drones' operators. Most of them are to be found in EU countries such as France, Germany or the UK. According to the Commission, the drone industry will continue to grow rapidly, so that based on its estimations after 10 years on the aviation market the drone industry will value approximately 15 billion Euros per year. Furthermore, the Commission estimates that the industry of civilian drones will boost employment and more than 150.000 jobs will be created in order to sustain the growth of this business (European Commission, 2014).

Furthermore, in the 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'', the Commission states that ''RPAS are an emerging market to create jobs and growth'' by giving example the number of Japanese RPAS operators that grew by 18 times during the period 1993-2005, reaching almost 14.000 RPAS operators (European Commission, 2014). Therefore, the Commission urges the introduction of a common regulatory framework on drones and also provides a strategy in order to support the EU aviation market to reach its potential. According to the Commission's opinion, the drone industry needs regulations on the EU level so that RPAS can be easily used in the whole EU airspace, without interfering with other safety standards on civil aviation developed by national authorities.

In addition to this, the Commission also raised the issue of insurance in case of accidents caused by RPAS operators and emphasizes that privacy, protection of personal data and security of its citizens must be protected and included in the regulatory framework in order to ensure public acceptance towards the use of drones (European Commission, 2014).

Finally, the Commission states that the EU must urge the development of the drone industry, mentioning that a strong drone industry will provide many economic benefits for the EU in the long term. On the other hand, the Commission also stresses the importance of a risk-based legal approach that shall address the issues of privacy, safety and security.

4.1.2 EASA

Since EASA is the main regulator of RPAS in the European Union, it is responsible for creating technical rules, safety standards and other rules on operating aircrafts. Apart from this, EASA assists the European Commission in technical, administrative and scientific matters related to the field of aircrafts within the EU civil airspace.

According to EASA's most recent document related to RPAS, namely ''The Introduction of a regulatory framework for the operation of drones'' published on the 12th of May 2017, it is very clear that EASA wants to regulate all kinds of RPAS regardless of size and weight and urges the introduction of a common EU regulatory framework for drones, that protects the privacy, safety and data protection of citizens. In addition, EASA published a brochure in May 2015 called

‘‘Concept of Operations for Drones: A risk based approach to Regulation of Unmanned Aircraft’’, in which it identifies three categories of drone operations: open category, specific operation category and certified category (EASA, 2015).

Firstly, the ‘open category’ refers to low risk operations and safety of these operations can be ensured through mass limitations, EU safety standards and a couple of minimum operational rules. Secondly, the authorization for the ‘specific category’ of RPAS should be given only by the NAA, so that the operator can perform a risk assessment. Finally, the third category, the so called ‘certified category’, is the most complicated, as its requirements should be treated similar to manned aviation. In addition to this, EASA suggests that drones falling into this category should be regulated by both national aviation authorities and EASA.

Moreover, EASA recognized the need of better regulations with regards to privacy and therefore it suggested that civil drone operators should register their RPAS with the local authorities, so that persons who think their privacy is being violated by others through the use of civil drones, can file a complaint with the local authorities and so the drone operator can be identified.

After the European Commission asked for assistance, EASA released in December of 2015 the document ‘‘Introduction of a Regulatory Framework for the Operation of Unmanned Aircraft’’; the document contained the three categories of drone operations of the former document from May of 2015 based on their risk, and an additional twenty-seven different proposals for regulating the low-risk operations of RPAS, regardless of size.

4.1.3 Council of the European Union

Officials from the fields of transport, energy and telecommunications that meet at the Council of the European Union, recommend an EU approach on the future use of civilian drones, in order to enable this industry to reach its full proficiency. According to the Press release of the 3335th meeting of the Council, the majority of ministers of Transport, Energy and Telecommunications of the Member States suggested that civilian drones should be introduced into normal airspace, but that safety regulations should be improved. In addition to this, few delegations stated that data protection and privacy rules are sufficient for the introduction of remotely piloted aircrafts

into normal airspace. A general European approach to civilian drones was emphasized and EASA was suggested for governing technical and safety standards, licenses and certificates (Council of the European Union, 2014).

Furthermore, a couple of delegations mentioned that the introduction of civilian drones should be done progressively, as there are many types of civilian drones, based on their specifications. Therefore, elementary drones should be authorized first. In order to develop EU rules on the use of civilian drones, EASA could also take into account the national rules of the Member States and try to complement them.

4.1.4 European Parliament

The Committee of Transport and Tourism of the European Parliament released in 2015 the ‘‘Report on Safe Use of Remotely Piloted Aircraft Systems (RPAS), Commonly Known as Unmanned Aerial Vehicles (UAVs), in the field of Civil Aviation’’. The report, which was released on the EP’s own initiative, was structured based on the Riga Declaration and the Commission’s suggestion of eliminating the 150kg rule regarding RPAS, and develop a common EU set of rules on the use of civilian drones. Nevertheless, the Transport and Tourism Committee acknowledged EASA competence of regulating drones on the European level and suggested that EASA should extend their competence in the field of RPAS (European Parliament, 2015).

4.2 Dronerules.eu

Within the European Union, besides EASA, the Directorate General for Growth also promotes safety standards for drones as they invested 1 million Euros in COSME programme. Under this programme, the DG for Growth created a website called *dronerules.eu*, in order to inform civil drone users about the laws and regulations that apply in the Member States of the EU, Norway and Switzerland. The website provides few videos, handbooks, safety guides and privacy case studies, which are meant to inform civil drone operators that they are legally responsible for their actions, implying that they must take privacy and data protection of others into account. In addition, operators are provided with rules, guidelines and national legislations related to drone activities.

The website contains information on recreational and professional UAS activities and focuses on three main aspects: privacy and data protection, safety and insurance. This website is constantly updated with new information including case studies, national legislation, tutorials etc. For instance, last time the EU privacy rules were updated was on the 2nd of April 2017.
The aim of the *dronerules.eu* website is to raise awareness to all drone users across Europe and offer them all the information about European authorities and legislation that are involved in the regulatory process of drones. As the programme will end in December 2017, by that time it needs to contain all EU and national laws with respect to safety, privacy, data protection and insurance applicable to RPAS use.

4.3 Regulation 216/2008/EC

As mentioned in the previous chapter, the EU does not have any regulations for drones over 150kg due to the current regulation on European level, namely the Regulation 216/2008/EC. This regulation is also referred to as the ‘‘Common Rules in the Field of Civil Aviation’’ and deals with regulations only for aircrafts over 150 kg. Drones with a mass over 150 kg are subject to EU law and are governed by EASA, while drones with a mass below 150 kg are regulated by the EU Member States. At the moment, there are only a few Member States (Germany, The Netherlands, UK, Poland, Denmark, France, Romania, Sweden, Italy and Spain) that have developed national laws on the use of drones, taking into account the risks of privacy and data protection. When it comes to safety operations and conditions for handling a drone, national laws differ from MS to MS, but it is very common that civilian users are required an authorization in each of the MS mentioned above. In addition to this, according to the European Commission, due to the different rules on the use of drones among the MS, the overall growth in drones is hindered (Finn & Wright, 2014).

As a conclusion, only drones with a total mass over 150 kg are subject to EU law, which is governed by EASA based on the Regulation 216/2008/EC. For drones with a mass below 150 kg, regulations on this kind of light drones lie with the Member States. Since there are only few members states that regulate the use of such drones, this means that in the other Member States, the use of drones below 150 kg is not regulated at all, raising therefore a lot of concerns among EU citizens with regards to the right to privacy and data protection.

Summing up, based on the Regulation 216/2008/EC, the EU does not regulate drones with a mass below 150 kg, which implies that most of the civilian drones as they weight under 150 kg are only regulated by some Member States. This means that issues raised by the use of drones with a mass below 150 kg, challenging citizens' privacy and data protection must be met by other legislative instruments such as human rights, so that citizens can be protected by the law in case their rights to private life and personal data are being violated.

4.4 Riga Declaration

Furthermore, in March 2015, the Commission, national authorities, members of civil aviation organizations and RPAS manufacturers adopted the Riga Declaration on Remotely Piloted Aircraft - ''Framing the Future of Aviation''; this declaration contains new insights for future drone regulations as aviation activities must be backed with higher levels of safety and respect individual's privacy. According to the Riga Declaration, civilian drones should be treated as new types of aircrafts and therefore tailored regulations must be developed, since drones that are not guided by the operator in a safe and legitimate manner, can pose potential privacy and personal data protection risks. These regulations refer not only to the use of RPAS, but also on the production of RPAS and therefore drone manufacturers must invest in the production of drones and equip them with applications in such a way that citizens' safety is not put at risk and the drones can be fully integrated in the European airspace.

In addition to this, the EU needs to develop safety rules for highly developed tools such as drones and include them in civil aviation. One of the most important principle raised during this convention, is that the drone user must be responsible for his/her actions including drone accidents. It should be also mentioned, that the drone operator is responsible for the insurance of the drone, so that in case of any accidents caused by the drone in use, third parties can be compensated accordingly.

4.5 Conclusions

In this chapter, the position of the European Commission and Parliament, EASA and Council of the European Union have been presented. The enumerated EU institutions and agencies aim for a

stronger drone industry and a new EU regulatory framework for civilian drones as the use of RPAS can pose privacy, data protection and ethical risks to EU citizens. Nevertheless, the Commission's COSME programme provides much information for civilian drone users, so as to ensure that they are aware that operating a drone within the European territory means that both European and national law is applicable, reducing therefore their chances of committing illegalities.

Moreover, the EU regulatory framework for civilian drones which includes Regulation 216/2008/EC and the Riga Declaration on Remotely Piloted Aircrafts has been clarified. However, the current regulatory framework does not fully address and protect all the rights of individuals. According to the Regulation 216/2008/EC, the EU does not regulate drones with a mass below 150 kg, stating that this is the responsibility of the Member States. From another point of view, not all Member States provide regulations for the use of drones, which means that in some Member States there is no kind of regulation for civilian drones and in this context privacy and personal data of individuals is not protected.

Based on the Regulation 216/2008/EC, it can be concluded that drone users cannot be held responsible by EASA for privacy or personal data complaints, as the EU is not entitled to regulate these tools below 150 kg. Only the national aviation authorities of the Member States are entitled to provide rules on the use of RPAS with a mass below 150 kg. Having said this, the EU regulatory framework does not provide regulations for all types of drones, meaning that privacy and personal data rights must be protected by other legislative instruments such as the EU Charter of Fundamental Rights or the Universal Declaration of Human Rights. Moreover, as the current regulatory framework provides only minimal protection for privacy and personal data of individuals, it is important that these gaps must be filled. According to the discussions between the Commission, Council and Parliament, EASA should extend its competences and regulate all types of drones regardless of size or weight. As a response for this, EASA released a new basic proposal on the use of RPAS in May 2017, mentioning that it would be better for the EU, if it could regulate all types of drones and fill the gaps in legislation.

As this was the end of the first block of sub-research questions dealing with the EU regulatory framework, focusing on the EU as a regulatory body and its attempt to develop regulations on

drone industry for both users and manufacturers, the next block of sub-research questions will focus on the human rights such as privacy and personal data protection.

Chapter 5: Civilian Drones and EU Privacy law

This next chapter will analyze if the use of civilian drones respects the right to privacy, which is a human right according to the Universal Declaration of Human Rights. In order to do this, the following sub-research question will be addressed: **To what extent does the existing regulatory framework for civilian drones protect the right to privacy?**

This chapter focuses on the right to privacy, also known as the right to private life. The aim of this chapter is to analyze if the current European regulatory framework for civilian drones respects this particular right. Since this right is regulated under EU law, instruments that recognize the right to privacy will be discussed in detail. For the purpose of this analysis, the most relevant instruments that recognize the right to privacy are the ECHR (European Convention of Human Rights) and the CFREU (Charter of Fundamental Rights of the European Union).

To begin with, **Article 8 of the ECHR** is the most common legal basis with regard to the right to privacy within the European Union. The next section deals with Article 8 ECHR, identifying its meanings that are relevant for this study. In addition to this, relevant case law related to surveillance purposes in line with Article 8 will be explained. Several opinions of the European Court of Human Rights related to visual surveillance will be employed as well, as these lead to other principles under EU law that are also significant for RPAS regulation in the European Union. In addition to this, Article 7 CFREU will be analyzed as well, because it does not differ from Article 8 ECHR and due to its direct effect before national courts, it is part of the legal basis with regards to the right to private life.

5.1 Article 8 ECHR

‘‘*1. A person has a right to respect for their private and family life, home and correspondence.*

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.’’

Article 8 ECHR consists of two paragraphs that will be discussed in the following. Section 1 of Article 8 presents specific rights guaranteed to every EU citizen, namely the right to respect for private life, family life, home and communications (Art.8(1), ECHR). Section 2 of Article 8 deals with the limitations to the rights enunciated in Section 1, stating that in certain circumstances such as ‘‘the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’’ exceptions to this right may apply (Art. 8(2) ECHR).

Since the current concept of ‘‘private life’’ may not be clearly protected by the rights outlined in Article 8(1), The Strasbourg Court interpreted each of these four rights and assigned them only broad definitions. As an example, the concept of *home* can be defined by ‘‘a hotel room, a room in a guest house’’. The same court stated that Article 8 is also relevant for the right to personal data protection. Moreover, according to Article 8(2), one can claim his right to private life unless it does not interfere with other liberties or interests such as ‘‘prevention of crime’’ or ‘‘protection of health or morals’’ et cetera.

In addition to this, it is very important that interference with Article 8 respects the three necessary requirements as stated in the second paragraph: interference should be legitimate (‘‘necessary to a democratic society’’), well-reasoned and ‘‘in accordance with the law’’ (Art. 8(2)). Interferences with rights enumerated in Art.8 are to be determined by the Member States, as they can decide if such interferences are legitimate or justified.

The aim of the European Convention of Human Rights is to protect citizens in order for them to

enjoy their human rights without any interference of public authorities. According to Art. 8(2) ECHR, individuals are protected against the interference of public authorities such as states and therefore the convention is applicable only for vertical relationship such as ‘‘state vs. individual’’. As interference with the right to privacy can by caused by private parties, not only by public authorities, all the articles of this convention have been guaranteed for having a horizontal effect of implementation too. In addition to this, the Convention is recognized for having a direct effect on national level as well (Cozzi et. al, 2016). This means that on one hand, citizens can make use of the provisions of Art. 8 ECHR in case of interference with both states or private parties and on the other hand, the Convention can be also used in front of a judge from a national court or in cases against a State, without being necessary to come first to the European Court of Human Rights in Strasbourg.

In addition, the right to private life can be applied in different ways, depending on the sphere in which the drone operator decides to use the drone. Therefore, it should be distinguished between private and public space, as Article 8 can be applied only to the private sphere of the individual, which is delimited from public sphere by physical boundaries. For instance, places such as home or personal relationships including relations with family members and friends are considered to belong to the private sphere of the individual. Any interference with this sphere is subject to Article 8 ECHR, meaning that if a drone operator performs surveillance activities within this private sphere, it will cause an interference with Article 8(1).

Regarding the situation of drone activities performed in public spaces, one cannot expect the same degree of privacy, as by definition, public spaces are open to anyone that has access to it, implying that individuals are aware that they can be recognized by others when entering a public space (European Commission, 2014). According to the Venice Commission, ‘‘any human being moving in public areas may well expect a lesser degree of privacy’’ (Finn & Wright, 2014). This does not mean that individuals entering a public space have no right to privacy at all, so they can still expect a lower degree of privacy unless they have satisfactory reasons. In this situation, the reasonable expectations of privacy are to be determined by the Strasbourg Court. In other words, Article 8 ECHR can be applicable also in public spaces, but it is up to the Court to determine if an interference with Article 8 is present or not.

To conclude, drones used in public areas that perform transparent monitoring activities except recording, do not interfere with rights enumerated in Article 8. Contrarily, when civilian drone operators monitor other individuals via drone applications, collect images or videos or disclose the data collected in public areas, they interfere with Article 8(1) ECHR. On the other hand, this interference can be justified, for instance, if the activity performed by the drone operator was meant for legitimate purposes or other requirements laid down in Article 8(2).

5.2 Article 7 CFREU

According to Article 6 TEU, provisions of the EU Charter are identical to the Treaties from a legal perspective. In this regard, Article 7 of the Charter of Fundamental Rights of the European Union contains almost the same phrase that can be also found in Article 8(1) ECHR:

‘‘*A person has a right to respect for their private and family life, home and communications.*’’

The only difference can be found at the end of the sentence, as the EU has replaced the word ‘‘correspondence’’ with ‘‘communications’’, due to the emerging technological innovations.

As the charter has the same legal value as the treaty, Art. 7 CFREU can be employed for the same reason since its meaning does not differ. Since the Charter of fundamental rights of the European Union has direct effect, individuals who claim that there is an interference with the right listed in Art. 7 CFREU can bring other people before national courts.

5.3 Conclusions

The aim of this chapter was to identify if European privacy laws are applicable to the use of civilian drones. The ECHR and the EU Charter contain provisions that guarantee the right to private life, but both instruments do not clearly specify what private means, leaving the term ‘private’ very broad so that it can be applied in all situations concerning privacy issues. European citizens can use these two instruments as a legal basis before national courts in order to defend their rights. With regards to RPAS technology, both Article 8 ECHR and Article 7 CFREU can be used for protecting any interference with all types of drones regardless of their purpose.

However, in section 5.1 the analysis of Article 8 ECHR revealed that not all interferences are sentenced by EU law, as to some extent, these interferences can be justified. Although in Chapter 2, it has been revealed that RPAS use poses serious risks to privacy of the individual, drone operators can justify the interferences with Article 8 ECHR. As an example, police officers that use RPAS technology for preventing crimes and collect personal data of citizens can justify this interference if they can prove that their activity is performed under a legal basis. In cases when private parties or commercial organizations must justify the interference with the right to private life, this will be not as easy as for law enforcement authorities.

Furthermore, although the Article 8 has not only vertical effect, but also horizontal effect, this means that private parties or individuals can also make use of the provision included in Article 8 ECHR against another private party. In this context, the situation in practice is not that simple. Due to the current regulatory framework for drone presented in Chapter 4, there are no means for identifying the owner of a drone with a mass below 150 kg, so that the drone operator can be sued and brought before national courts in case of interference with Article 8 ECHR. A possible solution for this issue may be the introduction of registration plates for drones, so that the owner of the drone can be identified more easily, but this would still post difficulties, as citizens cannot see from a distance the registration plate of a small sized drone. Another option would be if drone owners could be obligated to register online on local aviation authorities' websites with the time and place of performing drone operations, so that in case of any complaints they can be identified. Of course, this would not mean that all drone users would comply with this rule, but they should be informed that in case they are being caught performing such activities without prior registration to local aviation authorities and interfere with the Article 8 ECHR, they will have to face severe punishments.

Having said this, although the privacy of individuals is protected by Article 8 ECHR and Article 7 CFREU, there are still gaps in legislation that need to be filled by either the EU or EASA.

Chapter 6: Civilian Drones and EU Data Protection law

This chapter will analyze if the use of civilian drones respects the right for personal data protection, which is a human right according to the Universal Declaration of Human Rights. In order to do this, the following sub-research question will be addressed: **To what extent does the existing regulatory framework for civilian drones protect the right to data protection?**

This chapter focuses on the current regulatory framework for data protection. In the case of civilian drones' usage, European data protection law applies as well, because RPAS applications can record images or videos and locate the geo-position of persons without prior consent, challenging therefore EU data protection law. As this kind of data is collected and processed by RPAS applications, it implies that European data protection law can be applied in these kinds of situations. The topic of data protection is more complex than the topic of privacy, as data protection laws include not only treaties, directives and framework decisions of the EU, but also international and bilateral agreements. Since the use of civilian drones increases rapidly within the EU, the legislative powers of the EU proposed frameworks that can be used by many organizations in order to protect personal data of EU citizens.

European citizens are entitled to the right to data protection, as this fundamental right is codified in Article 8 of the EU Charter and Article 8 of the Council of Europe Convention. In addition to these two articles, this chapter will also analyze other provisions such as the Council of Europe Convention 108, European Directive 95/46/EC also called the Data Protection Directive (DPD), European Directive 2002/58/EC also known as the e-Privacy Directive and the General Data Protection Regulation (GDPR), as these contribute to the regulatory framework for data protection.

6.1 Article 8 ECHR and the Convention 108

In regard to the usage of civilian drones, while the right to privacy protects individuals from being surveilled by drones despite data not being collected, the data protection right applies only

when RPAS applications have already collected personal data.

The Court of Strasbourg initially stated that Article 8(1) ECHR does not assure full protection of personal data. The Strasbourg Court established a connection between Article 8 ECHR and personal data in the judgment of the cases of *S. AND MARPER v. THE UNITED KINGDOM* in 2008 based on the applications 30562/04 and 30566/04 of Mr. S. and Mr. Michael Marper against the United Kingdom of Great Britain and Northern Ireland and the Case of *M.S. v. Sweden* in 1997. In both cases, the court officially revealed that personal data is linked with Article 8 ECHR, as ‘‘the right to respect for private and family life are guaranteed by Article 8 ECHR’’ (Kilkelly, 2003).

To continue, The Council of Europe outlined that Article 8 ECHR is not efficient since it cannot cover all issues that may appear in the case of new technologies, including the drone technology. Although there were other national laws protecting the right to data protection, the procedure employed differed in many instances. In this regard, the Council of Europe developed the Convention for the Protection of individuals, also known as the Convention 108. Decisions and principles established by the European Court of Human Rights were included in the Convention. In line with other new principles that were added to it, a new European Data Protection instrument was developed.

6.2 The Fundamental Rights Charter (Article 8) and the Lisbon Treaty (Article 16)

‘‘*1. Everyone has the right to the protection of personal data concerning him or her.*
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.’’

Article 8 of the Fundamental Rights Charter protects the right to data protection and is the first legal document that recognizes personal data as a fundamental right. In comparison with the ECHR, the right to personal data protection is independent from the right to privacy, as for these

two fundamental rights are provided two distinct articles, namely Article 7 and Article 8 CFREU.

According to Article 16 TFEU:

‘‘*1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*’’

It is clear that the first paragraph of Article 16 TFEU is a repetition of Article 8 CFREU, stating that ‘‘everyone has the right to the protection of personal data concerning them’’. Again, this provision can be used as a comprehensive legal basis for issues related to personal data protection.

6.3 The Data Protection Directive 95/46/EC

Article 3(1) of the Directive 95/46/EC mentions the following:

‘‘*This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system*’’(Article 3(1) Directive 95/46/EC).

The term ‘‘automatic processing’’ used in this context is very broad and meant to include all types of CCTV or other surveillance systems, RFID (Radio-frequency identification) and microphones. All these applications are usually equipped on civilian drones and therefore this Directive can be applied in the case of data collection via drone technology. The term ‘‘personal data’’ used in Article 3(1) of the Directive 95/46/EC is explained in Article 2 of the same

Directive as ‘‘any information-including sound and images’’, The Article 29 WP released an opinion on this matter as the concept of personal data was too vague (Article 2 Directive 95/46/EC). According to Article 29 WP, the DPD is applicable when images, videos or sounds of identified or identifiable persons are collected and processed, as these are personal data. Since nowadays, through software systems different, data can be put together and make possible the identification of individuals either directly or indirectly, Article 29 WP emphasized the point of identifying someone indirectly, because in this case the situation is more complex. As an example, if a civilian drone user captures the overhead of an individual that cannot be identified without further hi-tech applications or software, in this context this is considered to be personal data. Thus, if the drone user captures the same image in the front- or backyard of a building that he might identify that person without further software or high-tech applications, this is personal data.

Furthermore, the Data Protection Directive 95/46/EC serves as a legal basis in the case of personal data processing via drone applications, both by private parties and public organizations/authorities for any reasons except law enforcement. The rights enumerated in the Directive have some exceptions such as household and law enforcement activities.

6.3.1 Household exception

A household exception can be applied, when private individuals perform personal and family life related activities. The directive also mentions, that if the data collected is then shared or uploaded on online platforms via the internet, this exception cannot be applied and the rules provided by the Directive 95/46/EC have to be followed. In the case of civilian drones, users must be aware of this fact as they are not covered by the household exception when they use the drone in public spaces for leisure or hobby activities. If such activities are performed on private property, the household exception can be applied, and the guarantees stated in the Directive 95/46/EC no longer apply.

6.3.2 Law enforcement activities

The second exception to Directive 95/46/EC represents law enforcement activities, as authorities

such as the police are allowed to collect and process personal data without being subject to EU law. In the case of exchange of such data between EU Member States, this exception does not apply anymore, and the guarantees enumerated in the Directive can be enforced. In addition, collecting and processing personal data via drone technology by national intelligence services is not covered by EU law as according to Article 4(2) TEU, as this is a national security matter and therefore each Member State is responsible for it, including collecting and processing of personal data of individuals.

6.4 The General Data Protection Regulation

The General Data Protection Regulation aims to improve the current rules and principles related to personal data of EU citizens collected by technologies, including drones. This Directive will replace the data protection Directive 95/46/EC of 1995 and will be applicable starting from the 25th of May 2018 by the law enforcement authorities that employ drone technology in order to collect personal data of individuals. As an example, if the Dutch government uses a drone for collecting and processing of personal data of persons, that occurs in a Dutch judicial or police context, this Directive shall apply.

The current data protection framework does not focus on technology and therefore the legislation in this regard is vague and very difficult to interpret, as the situation in practice differs. The current legislation is technologically neutral, but it identifies which measures are still to be implemented, while on the other hand, it is very broad so that emerging technologies such as RPAS can be adapted into the legislation as well.

Although current data protection legislation and aviation rules are not technologically oriented, the GDPR introduces new security measures such as encryption of data so that they can fill the gaps in legislation concerning the use of RPAS. According to the GDPR, two new principles are proposed, namely Data Protection by Design and Data Protection by Default.

6.4.1 Data Protection by Design

The first principle, Data Protection by Design, aims to provide more privacy protection by

including in the design of the products the specifications and practices. While according to the Data Protection Directive, the operator was responsible for following the rules of the DPD, in the General Data Protection Regulation, the operator is the only one accountable for the issues that might appear from using highly developed tools such as drones. The idea behind this is that by making the drone operator the only legally responsible, drone manufacturers will be forced to develop products with the right specifications. These specifications are meant to provide a minimum standard of data protection, which would make the drone industry fall in line with the new regulation and therefore respect privacy and data protection rights of individuals.

As already stated in the previous sections, one of the main challenges for RPAS technology is that in practice, the enforcement of privacy and data protection is not as easy to impose as it may seem. Therefore, if the Privacy by Design rule will be used for drones and their applications, issues such as privacy and data protection will be reduced considerably. Moreover, another benefit of this measure is that manufacturers will be responsible for new innovations.

6.4.2 Data Protection by Default

The second principle which is called Data Protection by Default, strives to achieve a maximum level of privacy by means that will automatically protect personal data. One of the two means that were identified is minimization of data so that personal information cannot be collected, processed and shared with third parties. The second measure would be to collect personal data only for very clear purposes so that the use and retention of data can be reduced as much as possible.

As a conclusion, according to many experts from the field of data protection, these two soft regulatory mechanisms, namely Data Protection by Design and Data Protection by Default are meant to reduce the risks to privacy and data protection of citizens that are associated with the use of civilian drones (Finn & Wright, 2014). In addition, the GPDR will protect personal data of EU citizens even more than the previous directive, as many new provisions of the regulation ‘’strengthen the right of individuals to erasure, transparency and data breach’’ (Verboven, 2016).

In this context, data protection challenges associated with the usage of civilian drones within the

EU is expected to be reduced. However, the GDPR still does not provide new provisions regarding the applicability of the regulation beyond the EU borders. For instance, if personal data collected by civilian drones through their applications is shared in real time with third parties or stored on online platforms such as Google Drive or iCloud, outside EU borders, in this situation the legislation is still not clear if the GDPR is applicable or not. The proposed GDPR does only marginally address the applicability of EU data protection legislation, but still fails to cover all aspects.

6.5 The e-Privacy Directive

Within the telecommunications sector, protection of personal data is a sensitive topic and therefore, as a complement to the Directive 95/46/EC, the Directive 2002/58/EC, also referred to as the ‘‘e-Privacy Directive’’, has been developed.

This e-Privacy Directive replaces the old Telecommunications Privacy Directive 1997/66/EC and deals with personal data that is collected by electronic communications services or public communications networks operating within the EU. The e-Privacy Directive is not applicable in case of law enforcement activities, just like the DPD. In addition, it aims to regulate communications, traffic and location data, including unwanted messages or mails such as spam, cookies, and the geographic position of the device used etc. Therefore, the e-Privacy Directive is also commonly referred to as the ‘‘EU cookie Directive’’. The aim of this Directive is to assure EU citizens that their online data, such as cookies, are not used by companies or private entities to track them. This is also relevant in the case of the companies or private entities using RPAS for collecting personal data of persons in order to track them for various purposes.

This new Directive prevents using cookies or geographic positions of individuals via RPAS as a way to gather personal data. Personal data collected through cookies via RPAS technology is subject to the guarantees enumerated in the e-Privacy Directive.

6.6 Conclusions

The aim of this chapter was to identify the current regulatory framework for EU data protection,

and to assess its applicability with respect to the use of civilian drones in practice. In this context, each legislative instrument that is applicable to personal data protection has been presented and examined. From the analysis, it can be concluded that each data protection instrument can be applied differently, depending on the purposes of the drone operation. Although some Directives are similar to some respect and some of the articles are almost identical, they apply for different sectors based on the type of processing data. For instance, for sectors such as law enforcement, household, telecommunications and Internet services, protecting the right to personal data can be achieved by employing different Directives/Articles.

The European regulations for data protection are also applicable for the use of RPAS. Unlike the right to privacy, data protection regulations may differ due to the purpose of the collecting of personal data; for instance, law enforcement authorities and private users of drones for leisure or hobby purposes that collect and process personal data via RPAS applications such as microphones, images, videos and sounds, are exempted from regulations of European Data Protection Directives. However, these two types of operators must take Article 8 CFREU into consideration, as this article guarantees individual's rights and principles with respect to data protection, regardless the purpose.

Summing up, RPAS users that collect personal data for commercial purposes fall under the application of the Data Protection Directive 95/46/EC. On the other hand, telecommunication companies and Internet providers using drone technology in order to broaden their areas of services are subject to the e-Privacy Directive 2002/58/EC, directive that is meant to complement the DPD 95/46/EC. In addition, civil RPAS operators collecting and processing personal data of others can benefit from the household exemption under certain conditions, being therefore not subject to the Data Protection Directive 95/46/EC.

In addition to this, the DPD will be replaced by the GDPR in May 2018. Although it brings some improvements such as Data Protection by Design and Data Protection by Default which will reduce the threats to privacy and data protection, the provisions of the regulations are still broadly defined. According to the Commission, the reason for this general approach is that future technological innovations could also be integrated in the legislation. However, the GDPR does not address all the current issues that occur from using drone technology and therefore it can be

concluded that, although the new regulation shows some improvements towards data protection rights, it is still not able to fill the gaps in legislation as some issues associated with the use of civilian drones remained unresolved, meaning that the current regulatory framework for civilian drones only marginally protect the right to personal data for EU citizens.

Chapter 7: Conclusion

7.1 Conclusion

The purpose of this study was to identify the current EU regulatory framework for civilian drones and determine if this respects human rights such as privacy and personal data protection. The analysis performed in this study reveals that the current EU regulatory framework for civilian drones only marginally respects the right to privacy and data protection of individuals. Although there are enough legal instruments that can be used against the risks to privacy and data protection of individuals posed by the use of civilian drones, such as the Article 8 ECHR, Data Protection Directive 95/46/EC, General Data Protection Regulation and the e-Privacy Directive, there are still gaps in legislations that need to be filled. In order to do so, the need to identify the types of RPAS regulators was evident. Within the EU, EASA is responsible for regulating only drones with a mass above 150 kg, meaning that privacy and data protection risks posed by operators of drones below 150 kg was not EASA's responsibility. However, this does not mean that these operators are not subject to EU law anymore, and therefore an analysis of the applicability of EU legislation on privacy and data protection was performed. The study revealed that the situation in practice is more complex, as the legal instruments that can be used depend on the types of the drone operation; in some cases, it is almost impossible to employ EU laws as the drone operator cannot be identified. In this context, for the three categories of RPAS proposed by EASA, the legal gaps could be filled as follows: EASA should be responsible for the open category, NAAs for the specific category, and both EASA and NAAs for the certified category, as these drone categories raise different levels of risks for privacy and data protection.

In addition to this, as privacy and personal data protection are not only EU fundamental rights,

but also fundamental human rights, an assessment from this perspective was performed and outlined that human rights cannot fill the legal gaps from EU legislation. As a conclusion, the current EU regulatory framework for civilian drones only marginally cover aspects of privacy and personal data protection, meaning that it must urgently improve its regulatory framework for civilian drones so that rights as privacy and data protection can be fully protected.

7.2 Ideas for new regulations

Besides legislation, new regulations are absolutely necessary in order to address the risks to privacy and data protection that the use of RPAS poses. The main ideas for new regulations that the EU must develop include: registration of civilian drones, obligating manufacturers to produce drones that respect privacy and data protection standards and making the drone operator aware of the legal consequences when data protection or privacy rights are violated. In addition to this, the EU could prevent data from being processed by forbidding manufacturers to equip the drones with biometric technology or behaviour detection applications. Drone manufacturers can include automatic blurring systems and make drones more visible, so that the chance of processing personal data via drone applications could be reduced.

Nevertheless, each civilian drone should be equipped with physical and electronic labels so that the drone user can be easily identified: via a physical label in the form of a registration plate containing the serial number of the tool and by an electronic label, a RFID chip that allows the authorities to identify the type of data that is collected by the drone. Another idea for new regulation is the encryption of data, so that it cannot be accessed by unauthorized persons.

7.3 Recommendations for future research

Since drones could be equipped in the future with systems that automatically blur the faces of individuals, so that users can collect video footages from public areas without challenging the right to privacy and data protection, it is worth studying if the blurring of faces is enough for avoiding individuals from being recognized. In addition to this, it can also be analyzed if the whole human body is necessary to be blurred by drone applications, so that commercial

organizations cannot identify the physical aspects or the clothes of individuals and use this data for targeted advertising.

Moreover, since, due their size and weight, drones can fly over vast areas and overcome fences or even enter buildings through windows, a lot of data can be collected while individuals are not aware. In this context, should drones be made more visible by the manufacturers so that they can be recognizable from a distance? Would it be a good idea if, during their implementation, they would emit sounds and lights so that individuals become aware of the presence of the drone?

Another area that can be studied is the applicability of the General Data Protection Regulation beyond EU borders, as drones can collect data on EU territory and share them in real time with third parties or store them on online storage clouds such as Dropbox, Google Drive, iCloud etc., that are located across EU borders. Although the GDPR brings new security measures that aim to protect personal data even more than the previous Directive, it still does not address all the aspect associated with civilian drones.

References

Scientific articles:

Brunstetter, D. R., Jimenez-Bacardi, A. (2015). Clashing over drones: The legal and normative gap between the United States and the human rights community. *International Journal of Human Rights, 19*(2), 176-198. doi:10.1080/13642987.2014.991214

Chulvi, C. P. (2016). The emerging use of civilian drones in Spain. Legal status and impact on the right to data protection. Revista de Derecho Político, 1(95), 83.

Clarke, R. (2014). Managing Drones' Privacy and Civil Liberties Impacts. *Retrieved from*: http://www.rogerclarke.com/SOS/Drones-PCLI.html

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 and Security Review, 30*(3), 230-246.

Clarke, R., Bennett Moses, L. (2014). The regulation of civilian drones' impacts on public safety. *Computer Law and Security Review, 30*(3), 263-285. doi: 10.1016/j.clsr.2014.03.007

Finn, R. L., Wright, D. (2012). Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications. *Computer Law and Security Review, 28*(2), pp. 184-194. doi: 10.1016/j.clsr.2012.01.005

Finn, R. L., Wright, D. (2016). Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organizations. *Computer Law and Security Review, 32*(4), pp. 577-586. doi: 10.1016/j.clsr.2016.05.010

Pauner, C., Kamara, I., Viguri, J. (2015). Drones. Current challenges and standardization solutions in the field of privacy and data protection. ITU Kaleidoscope: Trust in the Information Society (K-2015), pp. 67-73.

Schermer, B. W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review, 27*(1), 45-52.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review. 90*(4), p.1143.

Solove, D. J. (2008). *Understanding privacy*. Cambridge, Mass.: Harvard University Press.

Verboven, J. (2016). No fly drone - Drones versus the right to privacy. Thesis Master Law & Technology. Tilburg University.

Volovelsky, U. (2014). Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study. Computer Law & Security Review, 30(3), pp. 306-320.

<u>Regulations, opinions, policy documents:</u>

Case of M.S. v. Sweden. (1997). The International Journal of Human Rights, 1:4, 95-97.

Retrieved from: http://www.tandfonline.com/doi/pdf/10.1080/13642989708406703

Case of S. AND MARPER v. THE UNITED KINGDOM. (2008). European Court of Human Rights. *Retrieved from:* https://rm.coe.int/168067d216

Charter of Fundamental Rights of the European Union. *Retrieved from:* **http://www.europarl.europa.eu/charter/pdf/text_en.pdf**

Cozzi et. al. (2016). Comparative Study on the implementation of the ECHR on the national level. Council of Europe. *Retrieved from*: https://rm.coe.int/16806fbc14

Directive 95/46/EC. (1995). European Parliament and Council. *Retrieved from:* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Directorate-General for internal policies. (2015). Privacy and data protection implications of the civil use of drones. *Retrieved from:* http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/519221/IPOL_IDA(2015)519221_EN.pdf

Drone safe. (2016). Consumer Drone Users. An audience insight report. *Retrieved from:* http://dronesafe.uk/wp-content/uploads/2016/11/CAA_Consumer_Drone_Users_report.pdf

European Convention on Human Rights. (1953). *Retrieved from*: http://www.echr.coe.int/Documents/Convention_ENG.pdf

European Commission Staff Working Document. (2012). Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS). *Retrieved from:* http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013438%202012%20INIT

European Union Committee. (2015). Civilian use of drones in the EU. 7th report of session 2014-15. Authority of the House of Lords. *Retrieved from:* https://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/122/122.pdf

FBI. (2011). Boston Division. Press release. *Retrieved from*: https://archives.fbi.gov/archives/boston/press-releases/2011/massachusetts-man-charged-with-

plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-material-support-to-a-foreign-terrorist-organization

Finn, R.L., Wright, D. (2014). Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations. European Commission. doi: 10.2769/756525 *Retrieved from*: https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj8wMythPDUAhUJnRQKHfmjC34QFggrMAA&url=http%3A%2F%2Fec.europa.eu%2FDocsRoom%2Fdocuments%2F8551%2Fattachments%2F1%2Ftranslations%2Fen%2Frenditions%2Fnative&usg=AFQjCNGz8x2xO7bX2MLsu_uOAuErp4WOcA

International Civil Aviation Organization. 2011. Cir 328 AN/190. Unmanned Aircraft Systems (UAS). *Retrieved from:*https://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf

Juul, M. (2015). Civil drones in the European Union. European Parliamentary Research Service. *Retrieved from:* http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571305/EPRS_BRI(2015)571305_EN.pdf

Kilkelly, U., (2003). The right to respect for private and family life. *Human rights handbooks*(1). *Retrieved from*: https://rm.coe.int/168007ff47

Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones (2015). Working Party 29 Article 29. *Retrieved from*: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf

Riga Declaration on Remotely Piloted Aircraft. (2015). Framing the future of aviation. *Retrieved from:*http://ec.europa.eu/transport/sites/transport/files/modes/air/news/doc/2015-03-06-drones/2015-03-06-riga-declaration-drones.pdf

Ripley, W. (2015, April 22). Drone with radioactive material found on Japanese Prime Minister's roof. CNN. *Retrieved from*: http://edition.cnn.com/2015/04/22/asia/japan-prime-minister-rooftop-drone/index.html

Royal Aeronautical Society. (2014).Written evidence (RPA0018). *Retrieved from:* *http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-sub-b-internal-market-infrastructure-and-employment-committee/civil-use-of-remotely-piloted-aircraft-systems-rpas/written/12723.html*

Single European Sky ATM Research. (2016). European Drones Outlook Study. *Retrieved from*: http://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf

The Guardian, (2014, October 31). More drones spotted over French nuclear power stations. *Retrieved from*: https://www.theguardian.com/environment/2014/oct/31/more-drones-spotted-over-french-nuclear-power-stations