anno V, n. 3, 2015
data di pubblicazione: 27 ottobre 2015

Saggi

A Legal Approach to Civilian Use of Drones in Europe. Privacy and Personal Data Protection Concerns *

di Cristina Pauner e Jorge Viguri **

1. The new era of drones

Drones[1] are a burgeoning industry whose exponential growth over the next years is unanimously accepted. Their amazing and countless

* This article was elaborated within the framework of CRISP Project (Evaluation and Certification Schemes for Security Products) funded by the European Commission (Grant number 607941) and the support of the Mobility Program of the Ministry of Education, Culture and Sports (PRX14/00107). Professors Artemi Rallo and Rosario García Mahamut have reviewed this study.

** Universitat Jaume I (Spain). Paper subjected to a double blind peer review.

[1] Drones are also known as RPAS (Remotely Piloted Aircraft System), UAV (Unmanned Aerial Vehicle) and UAS (Unmanned Aerial System). These terms are being used interchangeably although technical differences among them must be outlined. Drone has been often used to military use, UAV is a relatively new word that has been adopted by the International Civil Aviation Organisation to encompass an unmanned aerial vehicle and everything involved in their operation including software, aircraft, and operation procedures, UAS includes software and the aircraft vehicle. Ultimately,

usages are a key element to be considered as a revolutionary product as well as their positive economic impact. As highly versatile and productive assets, drones will be able to play any type of commercial, personal or even public role in the future. Drones' applications appear to be limitless and they are gradually being use far beyond the realm of the military: future commercial applications[2], law enforcement activities[3] or communication infrastructures[4], among many others.

In consequence, the use of drones for civil purposes has become the focus of increased attention and concern in Europe. The first challenges to overcome were those related to flight safety, particularly if the drone operates outside the field of vision and in populated areas[5]. Both in Europe and in the United States, aviation regulators have been concerned about this issue regularly. Some geographical and time limits have been

RPAS is the generic word often used for civilian use. For our purposes, the expressions RPAS and drones will be used indiscriminately in this paper.

[2] *Amazon details drone delivery planes*, BBC news, 8 June 2015, http://www.bbc.com/news/technology-32653269 (last visit for all the pages: 27/10/2015). *Delivery by drones in 30 minutes? Amazon says it's coming*, Fox news, 17 June 2015, http://www.foxnews.com/politics/2015/06/17/delivery-by-drone-in-30-minutes-amazon-says-it-coming/.

[3] *The police force using drones to fight crime*, The Guardian, 1 October 2014, http://www.theguardian.com/world/2014/oct/01/drones-police-force-crime-uavs-north-dakota.

[4] *Facebook builds drone for internet access*, BBC News, 30 July 2015, http://www.bbc.com/news/technology-33728704.

[5] A categorisation of drones and their associate regulatory safety regime have been recently proposed by the European Aviation Safety Agency (2015)

established and drones are not permitted to fly in larger urban zones (U.S., Spain, Australia, Canada, etc.).

However, the increasing use of civilian drones requires paying attention to other issues affecting fundamental rights and civil liberties and, in particular, privacy and data protection breaches. Drones can be equipped with a large and heterogeneous variety of pieces, technologies and capabilities – from simple devices such as on-board cameras and sensors to extreme complex technologies such as high-power zoom lenses, night vision, infrared, ultraviolet, thermal imaging, radar technologies, video analytics technology, distributed video or facial and other soft biometric recognition[6]. Given the versatility of these devices and the ability to collect a wide variety of information for long periods of time and over large areas, their impact on privacy and civil liberties are all easy to foresee.

Taking this into account, methods of law enforcement and many iniciatives address the issues of privacy and data protection from ethical, social and juridical perspectives. The aim is «finding a balance between the advantages inherent in the civilian use of drones and possible harm to the right to privacy and data protection (as well as other fundamental rights such as freedom of expression)» (Volovelsky 2014).

This paper analyses the potential privacy and data protection risks related to civilian drones use and looks at the most significant doctrinal, institutional and legislative attempts to mitigate them.

[6] A study on current and future capabilities and applications of drones in Finn and Wright (2012)

2. The EU strategy on the use of drones

A drone, which many refer to as a unmanned aerial vehicle (UAV), unmanned aerial system (UAS), autonomous underwater vehicle (AUV), and many other names, is often simply described as an unmanned aerial vehicle. These aircrafts have been often controlled remotely by pilots from the ground and have been used solely by the military. Increasingly, they are being controlled autonomously following a pre-programmed objective. The development of drones' technology holds out the possibility that manufacturers design and build different types of drones according to the specific needs and requirements of each customer.

Drones using high tech cameras are able to record, store and even upload images and video to the Internet and they may easily violate citizens' rights. Nevertheless, they are increasingly being challenged in the context of an open and global market particularly relating to security, privacy and personal data issues for EU citizens (European Commission 2015).

They are revolutionary products and their potential future applications are still unknown but their use is posing a threat to security, privacy and personal data protection. Legislation no longer reflects technological development and other public and private mechanism should be implemented to ensure a common framework throughout the EU. Gaps exist in relation to EU security, privacy and data protection guarantees on drone activities by private and public stakeholders. In order to overcome such gaps, a series of solutions have been analysed in this paper.

Since it was crucial that European rules be laid down for this sector, the European Commission (EC) began discussions on drones in 2012

and adopted the first Working Document *Towards a European Strategy for the development of Civil Applications of Remotely Piloted Aircraft Systems (RPAS)* (Commission Staff Working Document 2012), and establishing a European RPAS Steering Group. In addition, in April 2014 and building on the *Roadmap for the Integration of Civil Remotely Piloted Aircraft Systems into the European Aviation System*[7] the EC adopted the *Communication A new era for aviation: Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner* (European Commission 2014), presenting its strategy on the future regulation of drones in the EU in order to respond to the call of the European manufacturing and service industry to remove barriers of the development of drones for civil use while safeguarding public interest. Besides, the European aviation community adopted the Riga Declaration on Remotely Piloted Aircraft (drones) "Framing the Future of Aviation" in March 2015[8] to exchange views on how and under which conditions, drones can help create promising new opportunities in Europe and to ensure that all the conditions are met for the safe and sustainable emergence of innovative drone services.

[7] European RPAS Steering Group, *op.cit.*

[8] The following principles must be noted: «Drones need to be treated as new types of aircraft with proportionate rules based on the risk of each operation, EU rules for the safe provision of drone services need to be developed now, Technologies and standards need to be developed for the full integration of drones in the European airspace, Public acceptance is key to the growth of drone services and the operator of a drone is responsible for its use» (Riga Declaration on Remotely Piloted Aircraft (drones), *Framing the Future of Aviation*, Riga, 6 March 2015. https://eu2015.lv/images/news/2016_03_06_RPAS_Riga_Declaration.pdf).

Ultimately, *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of drones* must be noted. In this regard, the Article 29 Working Party (Article 29WP) notes, the lack of an adequate regulatory framework in most member States. In this context, it states the harmonisation and the modernisation of Member States aviation polices in relation to drones should be encouraged. The document evidences the challenges of large-scale deployment of these aircrafts equipped with sensor equipment, while providing guidelines for interpreting the data protection standards in the context of drones and it sets some guidelines and recommendations to assess the measures necessary to ensure the respect for all other fundamental rights at stake such as human dignity, right to liberty and security, freedom of thought, conscience and religion, the freedom of expression and information, the freedom of assembly and of association, and the right to non-discrimination (Article 29 Data Protection Working Party 2015, 5)[9].

As a result, an exhaustive approach for each type of drone and an analysis of potential threats arising from their use will be required as the progress of industry continues. In the event that a RPAS seriously endangers a fundamental right, corrective and effective measures will be implemented in order to promote absolute respect for the rights and freedoms of the EU citizens.

[9] See an extensive comment on this document on Section 4 of this study.

3. Potential infringements upon privacy and data protection

In this section, attention is drawn to the risks that drones, as a new technology introducing surveillance, present to privacy and data protection rights in the light of the evidence that the regulation of civilian uses of drones is under construction and current regulatory mechanisms do not adequately address privacy and data protection concerns. As it has been highlighted above, there is a gap regulation on privacy issues because «current regulations governing drone operations have more to do with ensuring their safe flight and do little to address the privacy implications» (Privacy Commission of Canada 2013, 1).

A. Concerns about privacy

Drones have been defined as «complex, multimodal surveillance systems that integrate a range of technologies and capabilities» (Finn, Wright, Donovan, Jacques and De Hert 2014, 18) and are able to carry out any type of surveillance: "mass surveillance" and "targeted surveillance"[10].

[10] Two broad types of surveillance can be distinguished: Mass surveillance is also called passive or undirected surveillance which is not targeted on any particular but gathers images and information for possible future use. CCTV and databases are examples of mass surveillance. Targeted surveillance is directed at particular individuals, can involve the use of specific powers by authorised public agencies and can be carried out overtly or covertly. Interception of communications, visual surveillance devices, sensors of movement, "traffic" data are examples of targeting methods (House of Lords, Constitution Committee 2009).

Many authors have pointed out that the real challenge is the convergence of techonologies developments and the combined functions they are able to reach: «While regulation of separate functions e.g. in telecommunications or the use of DNA in identifying an individual has been possible, the real challenge will be in regulating combined functions» (European Group on Ethics in Science and New Technologies 2014, 33). In fact, new threats encompass one of the most relevant features of privacy concerns. The different capabilities of drones support a new and superior level of surveillance: an invisible, noisless, continuous and highly intrusive surveillance over people and places.

Previously, the European Union was presented with two basic questions. First of all, defining the specific scope of drones although this assumption may be extremely complex and secondly, delimiting clearly what privacy encompasses.

Although there is not a universal definition for privacy as it is an evolving concept that depends on society conceptions and technological factors, there is a broad consensus on the consideration of privacy as a fundamental right intricately connected with dignity and a cultural universal as «an essencial part of human flourishing and well-being» (Moore 1995, 56). In the words of the European Group on Ethics in Science and New Technologies (EGE), «Human beings need their own space, both literally as well as figuratively speaking, in order to realise their capabilities and flourish as human beings. Dignity means to respect the need to have one's own space, one's secrets. Robbing a person of his or her privacy is robbing him or her of their dignity» (European Group on Ethics in Science and New Technologies 2014, 72). Privacy has evolved from a simple evocation of the "right to be left alone" to a much

more complex right that enables the free development of one's personality and the construction of personal identity.

The right to privacy – as well as the right to data protection – has been described by law, judicial decisions and doctrine. Regarding the European legal framework, Article 8 of the European Convention on Human Rights (ECHR) states as follows: «Everyone has the right to respect for his privacy and family life, his home and correspondence». Besides, Article 7 of the Charter of Fundamental Rights of the European Union (CFREU) states that a person has a right to respect for their private and family life, home and communications. Future rules for operating drones in the civilian market will be influenced and shaped by this legal framework.

Authors have distinguished among different types of privacy[11], being the physical privacy and the informational privacy the most threatened by drones. These risks may arise from an extended use of RPAS not only by law enforcement agencies but, basically, by individuals due to the widespread use of drones in a civilian context (for commercial or leisure purposes) and they have a common aspect: RPAS surveillance may provoke a "chilling effect" that affects to behavioural privacy. The chilling effect may prevent people from exercising their legitimate civil liberties and rights if they have the feeling of being targeted and under surveillance[12].

[11] Physical or phiscological privacy (related to physical protection and to personal autonomy), informational privacy (related to communications), economical privacy (which affects to property) and decisional privacy (related to decisional-making power).

[12] As Clarke (2014, 287) stresses: «Overt surveillance stifles behaviours, including (and desirably) illegal behaviours, but also behaviours that are discouraged by

B. EU legal framework for data protection

As some authors underline the issues that RPAS technology present to data protection are not new compared to other available technologies «because, although RPAS technology in itself is new, the payloads that can be fitted for the purpose of processing personal data are not new technologies. Further, whether data are processed within a surveillance context is irrelevant to determining the relevant data protection issues» (Finn, Wright, Donovan, Jacques and De Hert 2014, 43)[13]. Even so, the existence of data protection laws does not mean that the legal requirements are fulfilled.

There is a wide range of possible risks to the right to data protection that could vary in funtion on the capabilities of the device. However, once the drone is airborne and captures images, any operation that involves the processing of personal data shall comply with data protection rules. It is well known that even the collection of data, without further processing – recording or storage –, it is nevertheless a processing operation that entails the application of the data protection legislation (Article 29 Data Protection Working Party 2004, 15).

organisations with institutional or market power. Covert surveillance, on the other hand, gives rise to the 'panoptic' effect: individuals fear that they may be subject to observation at any time, and that many behaviours might be construed by the powerful to be undesirable. This results in a form of 'self-discipline' – a 'chilling effect' on a wide range of behaviours, and the stultification of freedoms of expression and of innovation…».

[13] See also in this regard, House of Lords, European Union Committee (2015, 46-47).

In the early 1970s, some European countries began adopting privacy laws[14]. In 1995 the European Union approved the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[15]. The Data Protection Directive was created in order to increase legal certainty due to the differences of data protection laws across the EU or even the lack of a data protection legal framework in some Member States. This Directive establishes detailed rules for maintaining the privacy of the subject of the data (in particular, Articles 6, 7, 10, 15 and 17). In 2002, the Directive on Privacy and Electronic Communications[16] was enacted, expanding the doctrine of data protection to internet and cellular service providers.

[14] Sweeden and Germany were the first member states in which a Privacy Act was passed. While Sweden passed the first national law in 1973, the federal state of Hesse passed the first national data protection law in 1970. See Hessisches Datenschutzgesetz (The Hesse Data Protection Act), Gesetz und Verordungsblatt I (1970), 625 altough the first federal data protection act came into force in 1977. See Gesetz zum Schutz vor MiBbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG) of 27 January, 1977, BUNDESGESETZBLATT [BGBI] 1 201 (W. Ger.) [Law on Protection Against the Misuse of Personal Data in Data Processing (Federal Data Protection Act - BDSG)].

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

[16] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic Communications). Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN.

Moreover, Article 16 of the Treaty on the Functioning of the European Union (TFEU) stipulates that everybody has the right to the protection of personal data concerning them. The constitutional recognition of the right to data protection is ensrhined in Article 8 CFREU that states that an individual has the right to the protection of their personal data.

In January 2012, the European Commission proposed a General Data Protection Regulation (GDPR)[17] a comprehensive reform of data protection rules in the EU for the purpose of updating the data protection and privacy framework, specially the provisions contained in the Data Protection Directive. This legislation foreseeably would not come into force in Member States before 2017. The GDPR is expected to be the adequate legal instrument to address the challenges of increased civilian and commercial use of drones.

Articles 2(a) and 2(b) of the Data Protection Directive set out the definition of "personal data" and "data processing". Personal data[18] is defined as any information relating to an identified or identifiable natural person and the processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording,

[17] European Commission, Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, Brussels, 25 January 2012. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=en

[18] For an extensive guidance on the interpretation of the notion of personal data, see Article 29 Data Protection Working Party (2007).

organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Many capabilities of drones are based on data collection and processing: photographs (image), video (voice), biometric data (finger veins, finger prints, iris scans or facial patterns) are collected and processed by drones to carry out surveillance activities and these monitoring activities are subjected to the provisions of the abovementioned regulations. Thus, the legal framework in relation to data protection implications resulting from the use of drones in the Member States is the Data Protection Directive, in connection with the Directive on Privacy and Electronic Communications. There are also aspects applicable to closed circuit television systems (CCTV) that also apply to the use of drones, particularly if they are used for purposes of national legislation video surveillance.

However, some comments on the scope of the Directive must be made. It provides exemptions from the principles on the processing of personal data and enables national legislations to reduce the scope of duties and obligations set out in the Directive for reasons of national security and defence or the prevention, investigation, detection and prosecution of criminal offences or for certain enumerated purposes such as journalism or artistic and literary expression.

As far as we are concerned, Article 3(2) of the Data Protection Directive does not impose the duties of a data controller on an individual who processes personal data «in the course of a purely personal or household activity», also known as the household or domestic exemption. Hobbyist or leisure users would be sheltered from the application of the Directive considering that, in any case, this would

not include situations affecting constant monitoring, even partially, to public spaces or if this data is finally published online. On the other hand, commercial drones are fully subjected to the Directive.

C. Concerns about data protection

In an attempt to summarise, we consider several main risks that arise in relation to the processing of personal data carried out by a drone.

Most of such risks derive from a lack of *adequacy, fairness and transparency* in the collection, storage, and even further transmission and data processing due to the difficulty of perceiving their presence[19]. The covert process of compilation and transmission of data is, generally speaking, an unfair data processing and a breach of the principles relating to data quality.

Article 6 (a) of the Data Protection Directive states that personal data must be processed fairly and lawfully implying that data subjects must be aware of the collection and processing of their personal data and they should be informed in accordance to Article 10 of the above mentioned Directive. These conditions must be met by drone operators when processing personal data.

[19] Some authors refer to a "double invisibility" due to the ability of drones to film and take photographs from a distance that the subject concerned is not aware of the capture of images and the invisible way in which the transfer of data between the RPAS and the collector ordinarily takes place is done (Finn, Wright, Donovan, Jacques and De Hert, 43-44).

As to the GDPR, it declares in paragraph (a) Article 5 that personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to the data subject. In this regard, the information provided to data subjects shall include the identity of the RPAS controller and of his representative, the purposes of the processing for which the data are intended, any further information, such as the categories of data, recipients or categories of recipients of the data, the existence of the right of access to and the right to specify and correct the data concerning them.

More specifically, lack of transparency is also the source of other threats to data protection, mainly, the absence of the data subject's *consent*. As stipulated in Article 7 (a) of the Data Protection Directive, personal data may be processed only if «the data subject has unambiguously given his content». Articles 4 and 7 GDPR specify that consent must be «explicit» for the following reasons: to avoid confusing parallelism with "unambiguous" consent; to have one single and consistent definition of consent, to ensure the awareness of the data subject and to get the same data protection level in the EU.

In other words, consent must be freely, cleary and explicitly given by data subjects. Given these considerations, we can already foresee that drones surveillance in private areas will be forbidden as monitoring in real time or near real time without their explicit consent may be considered an attack on their privacy. Besides, surveillance in public areas shall, at least, provide people with all the information needed about the processing. In relation to free consent, it has frequently been underlined that consent provided by an individual is not valid when the subject has no real choice and he/she cannot deny consent without prejudice such as the case of the pre-ticketed boxes or, regarding RPAS, when an person is

not free to enter or leave a surveyed area without being under surveillance (Article 29 Data Protection Working Party 2015, 12).

Lack of adequacy, fairness and transparency in data processing along with anonymity of those who carry out surveillance raise the question of how to enforce the rights of individuals, how to detect those responsible for surveillance and how to require compliance with their duties to RPAS operators or controllers. Specially, taking into account that uses for RPAS range widely across the public and private sectors as so many are interested in using this technology: from law enforcement agencies to individuals passing through groups and organizations around the world seem keen on launching drones for a variety of purposes. In addition, any error or abuse that may occur with drones is frequently ignored because data subjects' are not even aware of the infringements to their rights to privacy and data protection.

It should be emphasised that Article 22 GDPR takes account of the debate on that principle of accountability. It requires a clear attribution of responsabilities and it describes in detail the responsibility of the controller «to adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation».

Other data quality principles at stake are purpose limitation and data minimisation. Article 5 GDPR sets out these principles, which correspond to Article 6 of Directive 95/46/EC. Regarding to purpose limitation, Article 5 paragraph (b) GDPR states that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Article 29 WP has clarified this principle. It says that «further processing for a different

purpose does not necessarily mean that it is incompatible: compatibility needs to be assessed on a case-by-case basis. A substantive compatibility assessment requires an assessment of all relevant circumstances»[20].

Concerning to data minimisation, paragraph (c) stipulates that personal data shall be adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data.

RPAS may facilitate the capacity to capture, process and store vast amounts of data in an indiscriminate manner which is contrary not only to the purpose limitation but also to the data minimisation principle. Therefore, a detailed programming of their data collected, stored and even shared shall be implemented for any drone operation in accordance with the above mentioned legal provisions. So, for instance, "it should not be possible to further use images of agricultural lands, captured when ensuring that pesticides are rightly disseminated, in order to record data on neighbouring lands and techniques or to film an area to secure it and use the images/videos to fine people who did not pay for the entrance» (Article 29 Data Protection Working Party 2015, 13). Neither should be possible to use willfully any data collected beyond its primary objective.

[20] In particular, account should be taken of the following key factors: (a) the relationship between the purposes for which the personal data have been collected and the purposes of further processing; (b) the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use; (c) the nature of the personal data and the impact of the further processing on the data subjects; (d) the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects. See Article 29 Data Protection Working Party (2013 a, 3).

In this regard, and linked to the previously mentioned principle, paragraph (e) of Article 6 of the Directive – and its equivalent Article 5(e) GDPR - regulate the limited retention principle. It means that the storage period should be limited and data that exceeds the period should be deleted or archived (if allowed). These provisions must be read in connection with the principle of data security. In this regard, implementing the required security measures, removing or anonymising those personal data, which are not strictly needed, is required.

Integrity and confidentiality of the data stored by a RPAS must be assured as well as checked for any potential transfer of data to third countries. Two main risks regarding security and illegal disclosure of data captured by RPAS have been reported (Finn, Wright, Donovan, Jacques and De Hert, 45-46). First, the transmission of data collected is done through wireless communication, which is not a reliable technology in terms of security and may put the confidentiality and integrity of data at risk. And secondly, the enthusiastic reception given to RPAS by private citizens raises the potential harm to unlawful disclosures of personal data as private use is still unregulated in terms of data protection.

In the face of these threats, Article 17 of the Directive determines that data controllers and processors, where applicable, must implement appropriate technical and organisational measures to protect personal data processing from accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access. In fact, data storage and data communications are vulnerable in a number of ways and the content of the data may be changed in transit, intercepted, copied, stolen,

etc. So, data stored in any device such as drones have to be removed as soon as purposes for the processing have been achieved[21] and retained in a safety manner by the data controller or anonymised (Article 29 Data Protection Working Party 2014) to avoid unnecessary danger of loss, theft and unauthorised use or removal.

The indiscriminate storage of data may also lead to the risk of function creep because drones may, for example, be purchased for precisely orientated uses, but may serve for other contested purposes. They can be used, for example, to detect illegal immigration on borders or at sea but, at the same time, there is a risk to misuse such technology to keep watch on minor or irrelevant events. As noted above, using RPAS for more than their stated purpose is contrary to Article 6 (b) of the Directive and will foreseeably be contrary to Article 5 GDPR.

Finally, the issue of function creep is enabled, among others, by data linking, central databases and profiling which is another major challenge for data protection rights. «Profiling» means any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person's health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements (Article 29 Data Protection Working Party 2013 b). The analysis can be used strategically with different pur-

[21] «For example, the images/videos captured by drones with the purpose to secure the open-air area of a festival shall only be retained for the time necessary to investigate possible complaints or security related issues» (Article 29 Data Protection Working Party 2015, 17).

poses by actors in the private sector (such as commercial, online advertising or direct marketing purposes) or in the public sector (such as anti-terrorism purposes). This technique is not allowed from a general approach by Article 15 of the Data Protection Directive that applies to computerised decision making about individuals[22] and it will be strictly forbidden under Article 20 GDPR.[23]

4. Solutions addressing a consistency EU data protection framework

After an initial phase in which attention has been placed on safety and security issues associated to the flying of drones, a very perceptible movement is focussing attention on the privacy aspects of this new technology. This movement can be perceived in Europe as well as in the U.S. In this country, on 4 March 4 2015, the U.S. Commerce Department's National Telecommunications and Information Administration

[22] Article 15 of the Directive on "automated individual decisions" says individuals have a general right «not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him».

[23] Article 20 GDPR: «1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour». A study on profiling in the GDPR in Vermeulen (2013).

(NTIA) announced that it is seeking comments on «privacy, transparency and accountability issues regarding commercial and private use of unmanned aircraft systems». NTIA's announcement is in response to a Presidential Memorandum (The White House 2015) issued on 15 February which directed NTIA to initiate a multi-stakeholder engagement process to develop a framework which addressed the issues above. While recognizing the benefits of increased usage of drones, the Presidential Memorandum notes the privacy, accountability and transparency concerns raised by drones. Alongside these initiatives, the United States Congress has adopted several bills for the purpose of protecting the right to privacy against intrusions by federal and state law enforcement and executive agencies (Thomson 2013).

In Europe and over the last years, many positive initiatives have come forth warning about the risks that the use of drones poses to privacy and other fundamental rights and picking the obligations to be met. These efforts have come from organisations with different scopes (at national or European level), from different perspectives (legal, economic or ethical alternatives) formulating a wide range of different solutions (technological proposals, voluntary or self-regulatory rules or legal framework).

On the lines below, we offer an overview of these initiatives and we identify some common remedies proposed in Europe taking as a reference the most recent and influential institutional documents on this issue – namely, the abovementioned Opinion on Ethics of Security and Surveillance Technologies issued by the EGE on 20 May 2014, the Opinion of the European Data Protection Supervisor (EDPS) published on 26

November 2014 and the Opinion 1/2015 adopted last 16 June by European Data Protection Authorities – as well as academic contributions.

A. Legal and statutory solutions

EU is looking for a common approach, encouraging and promoting cooperation between Member States to develop common rules (standards) and a regulatory framework for civil and commercial use of drones. In order to achieve this objective, reviewing the current European framework on data protection is essential.

At European level, the Data Protection Directive confers a number of important tasks to GDPR to face the challenges of the civil and commercial use of drones and it is expected that the new regulation will build an adequate framework to protect privacy rights of citizens. On the other hand, the review of EU legislation directly linked to the use of drones is suggested. E-Privacy Directive that applies to electronic communications to adapt and extend it to new technologies such as digital interfaces is a clear example and VoIP — Voice over Internet Protocol, indeed IP communications, broadband communications — products and also corporate private networks would be included in the remit of any revised Directive.

Some authors (Volovelsky 2014, 319) and institutions (Article 29 Data Protection Working Party 2015, 19) have also suggested adopting specific legislation intended to regulate the civilian use of drones. In this regard, they point out that the following aspects should be studied and detailed for its later implementation: the obligations and requirements that

will be imposed on operators of drones for civilian use (with strict limitations on the type of technology e.g. cameras installed in these devices), types of data that a drone may be authorized to collect; procedures for erasing data no longer necessary or relevant to the purpose for which they were collected or processed, period of time within which data can be stored, among others.

However, it may create legal uncertainty over the reliability of the rules in force. Legislation can't be adapted at the same time to technological changes and they tend to be more general without regulating specific situations. The following solutions intend to complement legislation to provide a more focused response to the current and future challenges posed by drones.

B. Technological solutions

There is a general agreement on the use of technology to support the respect of the legislation. These proposals fall under the concept of "technology governance" which is based on the idea of technology as a neutral and general tool to solve the problems of information in the age of global communications. The need of a global solution regarding security and surveillance and the absense of common privacy and data protection voluntary standards is a starting point. For this reason, it has been proposed that the solution will come from the technology as long as national regulations are so different and global information is pro-

cessed by different actors located all around the world under different jurisdictions. Privacy by Design (PbD)[24], Privacy by Default (PbDefault)[25] or Privacy Impact Assessment (PIA),[26] among others, are well-known technological governance instruments. The so-called Privacy Enhancing Technologies (PETs) would facilitate ensuring that breaches of the data protection rules and violations of individual's rights are not only something forbidden and subject to sanctions, but technically more difficult[27]. As the EDPS underlines PbD and PbDefault principles and the performance of a PIA in specific cases will be clearly stipulated in the proposed GDPR (Articles 23 and 33, respectively) (European Data Protection Supervisor 2014, 10).

In this regard, the EGE states that the development of security and surveillance technologies by public and private organisations in Europe

[24] «This principle means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal» (European Commission 2010). On this topic, Verdure (2012) and Cavoukian (2011, 3).

[25] Privacy by Default is a software design concept that aims to include a requirement that privacy settings that limit the sharing of personal data be turned on by default. It may prohibit the collection, display, or sharing of any personal data without explicit consent from the data subject. It has not been approved yet. It is being considered by a number of data protection authorities, including the European Commission.

[26] Privacy impact assessment (PIAs) is a proactive technique that aims to identify and reduce the privacy risks through the misuse of personal information. It is a voluntary process which assists organisations in assessing (identifying and minimising) the privacy risks of new projects or policies.

[27] European Commission (2007). In support of the technological solutions, see Huxting (2010).

must adopt privacy design principles because the «European values of dignity, freedom and justice must be taken into account before, during and after the process of design, development and delivery of such technologies. PETs should be integrated from the outset and not bolted on following implementation» (European Group on Ethics in Science and New Technologies 2014, 91). No less important, the advantage of taking preventive measures such as PbD is that they ensure efficacy and justice much better than any reactive measures such as economic compensation for breaches of privacy. The incorporation of storage and deletion schedules would be an example of PbD approach. It would imply that the devices embodied in drones should be design in a manner to allow secure storage of data over a defined period of time and automatic deletion once this period is exceded. The design of drones may also be flexible and different categories of sensors can be proposed depending on private sector buyers' business objective. This would allow buyers to choose the model of drone that would interfere with privacy the least. Privacy interferences can be as well avoided by providing tools with "data protection friendly funcionalities" such as the possibility to switch on/off sensors in flight, automatic masking of private areas or face-blurring effects for images that are unintentionally recorded (European Data Protection Supervisor 2014, 15).

If we refer to PIAs, some pioneering contributions such as the Guide on Regulatory Impact Assessment by the Spanish Data Protection Agency (AEPD 2014) or the Code of Practice for Privacy Impact Assessment by the Information Commissioner's Office (ICO 2014, 4-10) must be emphatised. In this sense, Data Protection Agencies have played a key role in adapting the existing regulations on data protection to the unique

characteristics of drones and it must be ensured that Data Authorities have sufficient legal powers, technical expertise and resources to ensure effective levels of enforcement across the European Union.

Ultimately, certification schemes, seals and marks have become very popular and have received much public and private coverage, especially regarding security products, services and systems[28].

All these technological solutions are highly recommended as a proactive tool to security or privacy breaches, among others. Although these have always been considered as a voluntary mechanisms, they will become increasingly important in the future since the GDPR might foresee high penalties especially in cases of intentional or negligent incompliance[29].

[28] Among other initiatives, we highlight the CRISP Project (Evaluation and Certification Schemes for Security Products) that aims to facilitate a harmonised playing field for the European security industry by developing a robust methodology for security product certification including drones. CRISP will enhance existing security evaluation and certification schemes by offering an innovative evaluation methodology that integrates security, trust, efficiency and freedom infringement assessment dimensions, inter alia and notably, the rights to privacy and personal data protection. More info at http://crispproject.eu/

[29] Article 70 GDPR states in paragraph 2a the following: «To anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions: a) a warning in writing in cases of first and non-intentional non-compliance; b) regular periodic data protection audits; c) *a fine up to 100 000 000 EUR or up to 5% of the annual worldwide turnover* in case of an enterprise, whichever is higher". However, paragraph 2b states that "if the controller or the processor is in possession of a valid 'European Data Protection Seal' pursuant to Article 39, a fine pursuant to point (c) of paragraph 2a shall only be imposed *in cases of intentional or negligent incompliance*».

C. Solutions from a social and voluntary perspective

The domestic use of drones is a constant concern for public authorities and regulators as many privacy violations may occur as a result of an inappropriate use of drones' by particular users. As described above, while commercial drones must comply with the Data Protection Directive, hobbyist and leisure users are exempt. In this regard, some remedies have been proposed.

To begin with, the EGE has supported that domestic use of drones should be subject to an authorisation and proper oversight to ensure safety and prevent misuse. Further, the EGE also suggests that those seeking authorisation for the use of surveillance drones must show that the proposed use is justified, necessary and proportionate and it recommends that policies and procedures governing the domestic use of drones for the purpose of surveillance should be publically available in the interests of transparency. More specifically, the EDPS clarifies the criteria to determine if the processing carried out via RPAS falls out of the scope of the household exception[30]

[30] The combination of the following factors shall be used to determine whether or not any particular processing falls within the scope of personal or household processing: if the personal data is disseminated to an indefinite number of persons, rather than to a limited community of friends, family members or acquaintances, if the personal data is about individuals who have no personal or household relationship with the person posting it, if the scale and frequency of the processing of personal data suggest professional or full-time activity, if there is evidence of a number of individuals acting together in a collective and organised manner, if there is a potential adverse impact on individuals, including intrusion into their privacy (European Data Protection Supervisor 2014, 9).

Regarding users, the Article 29 WP seeks to raise awareness of the intrusive potential of small drones by facilitating as much information as possible and, when feasible, maps that clearly identify where its use is permitted. For operators it is advisable to avoid the flight over private areas and buildings, even where it is permitted.

An initiative related to information for users, public and pilots is the creation of an on-line registration system. This database would be used by commercial drones' pilots to inform about their flights plans, data protection policies increasing transparency and it would enable citizens to identify the operator and some helpful information to exercise their rights. Some concerns have also been raised on the lack of awareness that exists among commercial drones pilots on their legal responsibilities regarding privacy and data protection. Therefore, among other options, the publication of guides for pilots on the impact of data protection legislation is suggested[31] This has been the case in the following countries: in UK, the Information Commissioner's Office (ICO 2015) has recently revised the CCTV Code of Practice, the *Commission nationale de l'informatique et des libertés (*CNIL) in France has issued several guidances and documents focused on drones and videosurveillance techniques[32] and

[31] This proposal has been supported by the European Union Committee of the House of Lords which echoes the suggestions made by the Centre for Democracy and Technology, Professor De Hert and Ms Jaques or Trilateral Research and Consultancy Ltd in their written evidences for the Commitee (House of Lords, European Union Committee, 2015, p. 65).

[32] The following documents and guidances must be outlined: Commission nationale de l'informatique et des libertés (2012, 2013, 2014).

the Commission for the Protection of Privacy (CPP) in Belgium has also been actively involved in the use of drones[33].

Finally, for both, users and pilots, education has been suggested as a powerful instrument to clarify benefits and risks of the use of drones. People must know the implications of the use of security and surveillance technologies (how, why and for what purpose their personal data is affected) and civilian operators have to be warned about the consequences (and responsabilities) that their actions may have for the right to privacy.

5. Conclusions

Drones are one of the most advanced equipment in the field of robotics, aeronautics and electronics and in the near future they will fulfill a wide variety of important roles in society.

Nowadays, the real scope of drones is not well known since they can generate infinite combinations and can be equiped with a wide range of technological products, services or systems.

GDPR and other EU legislation might not accomodate to the whole unpredictable high-tech revolutions in a nearest future. Furthermore, different national legislation is applied by EU member states which may increase legal uncertainty.

[33] Commission for the Protection of Privacy, *Privacy Commission responds about drones. FAQ section,* http://www.privacycommission.be/en/node/16643

To avoid this, other technological and social solutions shall be implemented for their effective control. Technological governance intruments (PbD, PbDefaut or PIAs) and effective certification schemes (standards, seals and marks) that protect the rights of citizens such as their security, data protection and privacy would also encourage a coherent European framework.

Finally, a public debate to raise awareness of the security, privacy and personal data protection implications of the use of drones should be carried out.

Bibliography

Agencia Española de Protección de Datos (AEPD) (2014), *Guía para una evaluación de impacto en la protección de datos personales*, 29 Octubre, http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

Article 29 Data Protection Working Party (2004), *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*, WP89, 11 February, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf

Article 29 Data Protection Working Party (2007), *Opinion 04/2007 on the concept of personal data*, WP136, 20 June, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Article 29 Data Protection Working Party (2013 a), *Opinion 03/2013 on purpose limitation*, WP203, 2 April, http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf

Article 29 Data Protection Working Party (2013 b), *Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation*, 13 May, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130513_advice-paper-on-profiling_en.pdf

Article 29 Data Protection Working Party (2014), *Opinion 05/2014 on Anonymisation Techniques*, WP216, 10 April, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Article 29 Data Protection Working Party (2015), *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones*, WP

231, 16 June, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf.

Cavoukian, A. (2011), *Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers*, in *Information and Privacy Commissioner*, Canada, August, http://www.ipc.on.ca/images/Resources/pbd-law-policy.pdf.

Clarke, R. (2014), *The regulation of civilian dornes' impacts on behavioural privacy*, in *Computer Law and Security Review*, n. 30.

Commission nationale de l'informatique et des libertés (CNIL) (2012), *Use of personal data protection and drones,* 30 Octobre, http://www.cnil.fr/linstitution/actualite/article/article/usages-des-drones-et-protection-des-donnees-personnelles/.

Commission nationale de l'informatique et des libertés (CNIL) (2013), *Drones: What prospective vision, which issues for freedoms?*, 6 Décembre, http://www.cnil.fr/linstitution/actualite/article/article/drones-quelle-vision-prospective-quels-enjeux-pour-les-libertes/.

Commission nationale de l'informatique et des libertés (CNIL) (2014), CNIL vs. Apple Retail France, *Video surveillance at work: Closing of the formal notice from the company*, 14 Octobre, http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Bureau/D2014-051_MED_APPLE_RETAIL.pdf

Commission Staff Working Document (2012), *Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)*, SWD (2012) 259 final, 4 September, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013438%202012%20INIT

European Aviation Safety Agency (2015), *Concept of Operations for Drones: A risk based approach to regulation of unmanned aircraft*, March, http://www.easa.europa.eu/system/files/dfu/204696_EASA_concept_drone_brochure_web.pdf

European Commission (2007), Communication from the Commission to the European Parliament and the Council on *Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM(2007) 228 final, Brussels, 2 May, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0228&from=EN.

European Commision (2010), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A digital Agenda for Europe*, 26 August, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R%2801%29&from=EN

European Commission (2014), Communication from the Commission to the European Parliament an de Council, *A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner*, COM (2014) 207 final, 8 April, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52014DC0207.

European Commission (2015), *Data protection Eurobarometer out today*, 24 June, http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm.

European Data Protection Supervisor (2014), *Opinion on the Communication from the Commission to the European Parliament and the Council on "A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner"*, 26 November,

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-11-26_Opinion_RPAS_EN.pdf.

European Group on Ethics in Science and New Technologies (2014), *Opinion on Ethics of Security and Surveillance Technologies (n. 28)*, Brussels, 20 May, http://ec.europa.eu/DocsRoom/documents/11493.

European RPAS Steering Group (2013), *Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System,* Final Report, June, http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap_en.pdf

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

Finn, R. L, D. Wright, A. Donovan, L. Jacques and P. De Hert (2014), *Privacy, data protection and ethical risks in civil RPAS operations. D3.3: Final report for the European Commission,* 7 November, http://ec.europa.eu/DocsRoom/documents/8550.

House of Lords, Constitution Committee (2009), *Surveillance: Citizens and the State,* Second Report, 21 January 2009, http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1804.htm.

House of Lords, European Union Committee (2015), *Civilian use of drones in UE*, 5 March, http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/122/122.pdf.

Huxting, P. (2010), *The Strategic Context and the Role of Data Protection Authorities in the Debate on the Future of Privacy*, in *European Privacy and Data Protection Commissioners' Conference Prague*, Czech Republic, 29 April,

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-04-29_Speech_Future_Pricacy_EN.pdf.

Information Commissioner's Office (ICO) (2014), *Privacy Impact Assessments: Code of Practice,* February 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

Information Commissioner's Office (ICO) (2015), *In the picture: A data protection code of practice for surveillance cameras and personal information,* Version 1.1, 21 May 2015.

Moore, A. D. (1995), *Privacy Rights: Moral and Legal Foundations*, Pennsylvania State University Press.

Privacy Commission of Canada (2013), *Drones in Canada. Will the proliferation of domestic drone use in Canada raise new concerns for privacy?*, March.

UK Government (2013), *Home Office Surveillance Camera Code of Practice,* presented to Parliament Pursuant to Section 30 (1) (a) of the Protection of Freedoms Act 2012, June, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf.

The White House (2015), *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights and Civil Liberties in Domestic Use of Unmanned Aircrafts Systems,* February, https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

Thomson, R.M. (2013), *UAV in domestic surveillance operations: Fourth Amendment implications and legislative reponses*, Congressional Research Service, 3 April, https://www.fas.org/sgp/crs/natsec/R42701.pdf.

Verdure, J. (2012), *Le concept de Privacy by Design: Un Remède à L'insuffisance des Moyens Actuels de Protection de la vie Privée*, 22 Février, http://www.e-juristes.org/le-concept-de-privacy-by-design-un-remede-a-linsuffisance-des-moyens-actuels-de-protection-de-la-vie-privee/.

Vermeulen, M. (2013), *Regulating profiling in the European Data Protection Regulation. An interim insight into the drafting of Article 20*, Centre for Law, Science and Technology Studies (LSTS), Vrije Universiteit Brussel, 1 September, http://emsoc.be/wp-content/uploads/2013/11/D3.2.2-Vermeulen-Emsoc-deliverable-profiling-Formatted1.pdf.

Volovelsky, U. (2014), *Civilian uses of unmanned aerial vehicles and the threat to the right to privacy. An Israeli case study*, in *Computer Law & Security Review*, n. 30.

anno V, n. 3, 2015
data di pubblicazione: 27 ottobre 2015

Abstract

A Legal Approach to Civilian Use of Drones in Europe. Privacy and Personal Data Protection Concerns

Drones are a growth industry evolving quickly from military to civilian uses however, they have the potential to pose a serious risk to security, privacy and data protection. After a first stage focused on safety issues, Europe is facing the challenge to develop a regulatory framework for drones integration into the airspace system while safeguarding the guarantees of fundamental rights and civil liberties.

This paper analyses the potential privacy and data protection risks related to civil drones' applications and looks at the major doctrinal, institutional and legislative attempts but also proposes technological and social solutions to mitigate them.

Keywords: drones, RPAS, privacy, personal data protection, Directive 95/46/EC, General Data Protection Regulation.