Urban Unmanned Aerial Systems Operations: On Privacy, Data Protection, and Surveillance

By **Eleonora Bassi**, Orcid: <https://orcid.org/0000-0002-1619-3543>

Politecnico di Torino, Italy

ABSTRACT

The drone sector offers a wide range of affordances, opportunities, and economic benefits for society. Delivery services, agriculture monitoring, wildfire control, public infrastructure inspections, humanitarian aid, or drone journalism, are among the activities enhanced by unmanned aerial systems (UAS). No surprise the civilian UAS market is growing fast throughout the world. Yet, on a daily basis, newspapers report serious concerns for people infringing other people's rights through the use of drones. Cybersecurity attacks, data theft, criminal offences brought about the use of this technology frame the picture. Nowadays, several countries are changing their legal rules to properly address such challenges. In 2018, the European Union (EU) started its five year-long regulative process that should establish the common rules and standards for UAS operations within the EU Single Sky by 2023. A similar timeline has been adopted in the United States, so as to provide the jurisdictional boundaries for the civilian use of drones. The United Kingdom (UK) and Japan are adopting new rules too. From a legal point of view, the overall framework is thus rapidly evolving. The aim of this paper is to give attention to (i) privacy and data protection concerns raised by UAS operations; (ii) their monitoring functions and corresponding surveillance issues; and, (iii) how a privacy preserving approach – such as with privacy by design technologies, organizational measures, audit procedures, civic involvement, to name a few – makes a lawful and ethical use of this powerful technology possible.

Keywords – *Civilian drones, UAS, privacy by design, GDPR, surveillance*

Acknowledgements. *I would like to thank Meredith Jones for her detailed editing work.*

Disclosure statement – *No potential conflict of interest was reported by the author.*

License – *This work is under Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) <https://creativecommons.org/licenses/by-nc-sa/4.0/>*

Suggested citation: Bassi, E., "Urban Unmanned Aerial Systems Operations: On Privacy, Data Protection, and Surveillance", *Law in Context*, 36 (2): 61-72. DOI: <https://doi.org/10.26826/law-in-context.v36i2.114>

Summary

1. *Introduction*
2. *The governance of UAS within the European Skyline*
3. *Privacy and data protection concerns between free flow, biz opportunities, behavior monitoring*
4. *Private surveillance, public surveillance, mass surveillance*
5. *Privacy preserving strategies*
 - 5.1 *Privacy by design*
 - 5.2 *Organizational measures*
 - 5.3 *Co-regulation and civic involvement for UAS urban operations*
6. *Conclusions*
7. *References*

1. INTRODUCTION

The drone sector offers a wide range of affordances, opportunities, and economic benefits for society. The activities enhanced by unmanned aerial systems (UAS) include but are not limited to; delivery services, agriculture monitoring, wildfire control, public infrastructure inspections, humanitarian aid, and drone journalism. The civilian UAS market is growing fast throughout the world and yet, on a daily basis, newspapers report serious concerns for people infringing other persons rights with drones. Cybersecurity attacks, data thefts, criminal offences brought about by the use of this technology frame the picture. Nowadays, several states are changing their legal rules to properly address such challenges.

In 2018, the European Union started its five year-long regulative process that should establish the common rules and standards for UAS operations within the EU Single Sky by 2023. A similar timeline has been adopted in the United States (US), so as to provide the jurisdictional boundaries for the civilian use of drones. The United Kingdom (UK) and Japan are adopting new rules as well. From a legal point of view, the overall framework is thus rapidly evolving. The aim of this paper is to draw attention to both privacy and data protection concerns raised by UAS operations, and how they overlap with further issues of surveillance and monitoring functions of drones. A consideration of various kinds of UAS operations, such as delivery services, public infrastructure inspections, medical aids, drone journalism, or public order functions illustrate that a lawful and ethical use of this powerful technology is possible through privacy by design solutions, organizational measures, audit procedures, and civic involvement.

In order to provide a fruitful analysis on how UAS impact on the pillars of the law and of society and how legal systems may properly tackle consequent normative challenges, this paper is divided into four sections beyond this one. The next section (section two) focuses on the legal governance of drones within the European Skyline, which comprises a general regulation from 2018, delegated and implementation acts of the European Commission from 2019, and the soft law of the European Union Aviation Safety Agency (EASA). The overall objective is to set the common rules and standards for UAS operations by 2023. This outcome would represent a reference point for most jurisdictions.

Section three sheds light on both privacy and data protection concerns. Although the EU regulation on data

protection, the General Data Protection Regulation (GDPR), is valid law for the collection and processing of personal data through UAS operations, many issues remain present. They regard business opportunities, behavior monitoring, and the free flow of data.

In the fourth section this paper draws the attention to surveillance concerns. They partially overlap with the issues examined in the previous section and suggest further distinctions be made between UAS operations for private monitoring, public monitoring, and mass surveillance. This differentiation is critical, because further sets of norms on public order, national security, the protection of health, or of the rights and freedoms of others, should be added to the norms on privacy and data protection. Examples of such norms include Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.

Section five illustrates the aforementioned privacy (and data protection) preserving approach with the examples of privacy by design and data protection by design technologies, organizational measures, and civic involvement. The aim is to show that a lawful and ethical use of UAS technology is possible in the specific context of urban areas.

After providing in-depth discussion on key areas relating to privacy and data protection of UAS systems, the final sections of this paper will provide conclusive remarks

2. THE GOVERNANCE OF UAS WITHIN THE EUROPEAN SKYLINE

In July 2018 the European lawmakers passed the new Regulation (EU) 2018/1139 “on common rules in the field of civil aviation” (the new Basic Regulation). They adopted a new comprehensive legal strategy for the drone sector, which includes a new mandate for the EU Aviation Safety Agency (EASA) on drones and urban air mobility.

The new EU regulatory framework for safe drone operations in the Single European Sky is still in progress. In June 2019, the European Commission adopted two implementing and delegated acts, on the grounds of the Basic Regulation’s mandate. The Commission Delegated Regulation 2019/945 “on unmanned aircraft systems and on third-country operators of unmanned aircraft systems” and the Commission Implementing Regulation 2019/947 “on the rules and procedures for the operation of unmanned aircraft” follow the distinction suggested by EASA in the Opinion 01/2018 (EASA 2018). According to the EU lawmakers, the definition of “technical and

legal requirements” of the legislation is referred to three categories of UAS operations: open, specific and certified.

The 2019 regulations by the EU Commission provide a detailed set of rules on (i) certification; (ii) EU and Third Countries operators; (iii) liability; (iv) risk evaluation; and, (v) design of UAS and connectivity systems. The two 2019 regulations will be fully applicable in 2020, in order to allow both EU Member States and drone operators to have time enough to implement the new set of rules.

In addition, in October 2019, EASA released its Guidance Material and description of means to comply with the regulation (the Acceptable Means of Compliance (AMC)) (EASA 2019a). The AMC casts light on how to carry out the specific operation risk assessment (SORA), which is required for the UAS operation, depending on the ‘specific’ category under scrutiny. Further guidelines will appear soon: EASA should release a number of pre-defined risk assessments models, in order to cover most common drone operations. The first two standard scenarios—concerning Urban Visual Line of Sight (VLOS) and Rural Beyond Visual Line of Sight (BVLOS) above control ground area operations—were published in November 2019 within the new EASA Opinion on “Standard scenarios for UAS operations in the ‘specific’ category” (EASA 2019b). The aim is to simplify the burden for UAS operators, paving the way to the full implementation of the new legal framework, that is, reforming the current air traffic management system throughout Europe and guaranteeing standards for the safety, efficiency and environmental impact of air traffic, so that drones can gradually begin to share the air space (Bassi 2019).

This highly centralized legal network, however, is still part of a more complex set of actors, regulations, and institutions, involved in the governance of UAS within the European Skyline. For instance, Member States (MSs) play a crucial role here. On the one hand, Article 56(8) and Article 71(1)-(3) of the new Basic Regulation grant MSs the possibility (i) to lay down specific national rules on UAS, (ii) to set specific exemptions to some European requirements; and, (iii) to amend implementing or delegated acts of the Commission. On the other hand, in the field of UAS operations, many issues of national security, public order, or the protection of health, mostly fall under the power of MSs. This latter picture reminds us of the current state-of-art concerning the regulation of the use of drones in USA: a different legal framework for each state. Although some common rules exist, such as principles of tort law in US and principles of data protection in EU, most important rules are up to the different states

of the EU. Even the simple test of a drone float involves considerable difficulty and costs in obtaining public safety authorizations, authentication, and national civil aviation green lights (Pagallo 2017a).

In addition, the legal picture should be completed with the different sectors affected by the use of this technology, such as telecommunication law, rules on product liability, criminal and insurance law, and so forth. These sectors cover problems of accountability and voyeurism, transparency and visibility, surveillance and monitoring, which have been widely debated over the past years (Finn and Donovan 2016).

In this paper, the attention is drawn to the fields of privacy and data protection. On the one hand, scholars mostly agree that such fields are particularly under stress with the use of drones. On the other hand, Article 132 of Regulation 2018/1139 (the new Basic Regulation) includes a safeguard clause for privacy concerns, which refers to the application of the General Data Protection Regulation (GDPR) Regulation (EU) 2016/679 and of the Regulation (EC) No 45/2001 (repealed by Regulation (EU) 2018/1725).

Only civilian drone operations are thus under scrutiny in this context. Military and MSs drone operations, such as border surveillance under the Frontex initiative for monitoring people migration via the Mediterranean sea, fall outside the regulatory powers of both the Basic Regulation on Civil Aviation and the GDPR (Marin and Krajčiková 2016). Such kinds of UAS operations, therefore, are left aside in this context.

The next section seeks to explore the overlap between the new Basic Regulation and the GDPR in the case of civilian UAS operations.

3. FREE FLOW, BIZ OPPORTUNITIES, AND BEHAVIOR MONITORING MEET DATA PROTECTION

It is no mystery that drones have worried EU privacy and data protection regulators over the past years. According to the Policy Department for Citizens’ Rights and Constitutional Affairs of the Directorate General for Internal Policies of the European Parliament:

In terms of risks for privacy and data protection, drones normally carry video-cameras to allow pilots to fly them. These images can be easily recorded and stored, and are often uploaded onto the internet. The privacy of private life and property can be interfered with and violated when drones capture images of people in their houses or

gardens. A series of other applications and payloads can also be installed on drones, allowing the gathering and processing of personal data and seriously interfering with and potentially violating citizens' rights to privacy and data protection. (European Parliament 2015)

The new Regulation takes into account such potential threats (Regulation (EU) 2018/1139). In 2014, the European Data Protection Supervisor (EDPS) released the Opinion "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 Data Protection Supervisor 2014). The EDPS stressed that UAS operations for civil purposes must comply with the fundamental rights to privacy and data protection, whereas "in the EU, unlike other jurisdictions, the location in a public or private space is not a relevant criterion when determining whether the right to privacy and the right to data protection apply or not."

As mentioned above in the previous section, the GDPR is now valid law for the use of drones processing personal data. The GDPR hinges on the assumption that the processing of personal data is a risky activity (Pagallo, Casanovas and Madelin 2019), much as authorities do in the field of civil aviation for the use of drones. The set of norms on data protection impact assessments, on data protection by default and by design, on consent, should thus be abided by. It is noteworthy that Annex IX, point 1.3, of the new Basic Regulation requires designers and operators of UAS to embed the data protection by design principle into the technology, for each UAS operation, device, or system. We return to this below in fifth section of this paper.

However, it seems fair to admit that drones do not only raise data protection and privacy issues. Due to their versatility (Clarke 2014, Finn and Wright 2016), the list of threats is long (Budinska 2019). According to Rachel Finn and Anna Donovan, for instance:

The application of drones in civil contexts can have the following effects: a chilling effect; dehumanisation of the surveyed; transparency and visibility, accountability and voyeurism; function creep; bodily privacy; privacy of location and space; and privacy of association. (Finn and Donovan 2016)

In addition, we should examine how UAS operations can interfere with third parties' devices and communications, how e-privacy and cybersecurity rules are to be applied in this context, what role telecommunication companies

should play in the governance of UAS operations, and whether the latter require band and frequencies of their own.

Still, UAS operations raise and magnify a further set of challenges that partially overlap with the data protection and privacy issues mentioned above in this section. As the Working Party on Privacy and Data Protection Issues Relating to the Utilisation of Drones put it, the capabilities of UAS operations

when combined with technologies and applications, change and transform the nature of surveillance, magnifying it, when compared to other similar tools (satellites, aircrafts, helicopters, CCTV) (Article 29 Data Protection Working Party 2015).

Such surveillance and monitoring functions of UAS operations partially fall under the jurisdiction of the GDPR. Pursuant to Article 35(3) of this latter regulation on a new generation of data protection impact assessments, a Data Protection Impact Assessment:

"shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing (...); (b) processing on a large scale of special categories of data (...); or (c) a systematic monitoring of a publicly accessible area on a large scale."

It seems fair to admit that all these hypotheses materialize with many UAS operations. As a result, in the wording of Article 35(2) of the GDPR, "the controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment." Here, data protection officers and civil aviation authorities have to collaborate, in order to strike a fair balance between the protection of personal data and the security of civil aviation operations (Bassi et al. 2019).

On the other hand, both surveillance and monitoring functions of UAS operations may fall beyond the scope of the GDPR. Due to their well-known versatility, drones can indeed be used for wildfire monitoring and the monitoring of transports and public infrastructures, monitoring of animal behaviours and urban surveillance for national security, or public order reasons. The aim of the next section is (i) to explore how such surveillance and monitoring

functions of UAS operations are regulated in Europe, and (ii) to complement the set of rules on civil aviation and data protection introduced in the previous sections of this paper. A further level of complexity follows as a result.

4. PRIVATE SURVEILLANCE, PUBLIC SURVEILLANCE, MASS SURVEILLANCE

We live in what some scholars dub as the “new surveillance society,” whereas drones are in fact one of its crucial ingredients. The aforementioned Opinion 01/2015 of Article 29 Working Party on drones stresses five reasons why this technology represents a powerful means of surveillance. First, UAS operations may be invisible, or non-detectable. Second, contrary to the bird’s eye view of satellites and aircrafts, or the fixed view of CCTVs, drones allow for a mobile view, which includes 3D resolution. Third, UAS operations can access more locations, for example; private properties, across fences or through windows. Four, drones can observe in detail and follow persons easily. Five, this technology is cheap, and persistent, i.e. drones can follow persons for a long time. All in all, in the wording of the EU data protection authorities, “all these specificities simplify and improve covert and overt surveillance and tracking of individuals or groups (including during demonstrations)” (European Parliament 2015).

Different kinds of drone surveillance, however, have to be taken into account. They depend on (i) the object or the area of surveillance, for example; whether or not people are in the area of a UAS operation; (ii) the subject performing the surveillance activity, such as a private guy, a journalist, a corporation, the police, or a civil servant in the performance of its public duties; and, (iii), the purposes that may restrict, for both moral and legal reasons, people’s right to privacy and some safeguards on data protection.

On this basis, we can further distinguish three different activities that fall under the notion of surveillance, that is, (i) monitoring and data gathering, regardless of what is monitored by and through UAS operations; (ii) investigation of specific or predefined targets; (iii) operatory functions, such as in legal enforcement operations, or for remote exploration work with the maintenance and repairs of countless facilities.

Several UAS surveillance and monitoring operations are of course morally sound. Wildfire monitoring (Songsheng 2019), rescue missions in risky areas, down to drones used for humanitarian aid in war zones, are among the examples. Also, civilian drones are used for surveillance operations in agriculture (Hell and Varga 2019), as well as monitoring transports and public infrastructures, such as harbours and dams, bridges and stations. In addition, UAS operations allow for new ways of monitoring animals’ behaviours, both for scientific research (Mufford et al. 2019) and for people’s safety, as occurs with shark monitoring alongside the Australian coasts.

In the urban context, drones are excellent tools for several activities in the business sector (for example, delivery), much as within smart city environments. They “provide the eye-in-the-sky alternative to ground-based monitoring, contributing to safety, early anomaly detection and possibly prediction, and improving everyday quality of life with little disruption of, and interference with, humans” (Pannozzi et al. 2019). Traffic monitoring (Garcia-Aunon, Roldan and Barrientos 2019), disaster recovery, and public park monitoring are only few of all possible uses of this technology, which are considered positive. The main risk is here to underuse our drones, thus creating opportunity costs “for what might be broadly described as the wrong reasons” (Floridi et al. 2018).

Yet, as usual, there is the other side of the coin, namely, the misuses of UAS technology. Even the sound use of UAS in smart city environments may turn out being problematic. The collection of data that drones make possible is pervasive and dynamic (Cavoukian 2012; Calo 2011). It is the difference between the fixed view of CCTVs monitoring a public park, or a train station, and the mobile view of drones, equipped with 3D resolution, monitoring the same public park, or station. Such surveillance and monitoring functions can have a chilling effect. People’s perception of how drones impact on their lives varies and is well documented in literature. Privacy is among the strongest concern (Walther et al. 2019; Rice et al. 2018; Grubestic and Nelson 2020). Under the drone’s eye, people are like the prisoner of Michel Foucault’s panopticon: “He is seen, but he does not see; he is an object of information, never a subject in communication.”

The pervasive and dynamic surveillance that drones make possible, often in very cheap ways, suggests three different kinds of problems. First, we may wonder about how the GDPR should be enforced in this context. Since people's activities, behaviours, or preferences can be further aggregated and organized for profiling them, either as a group, or as individuals (Pagallo 2017b), the attention should be drawn to the current state-of-the-art on strategies and measures as to how to preserve and enforce privacy and data protection by design and by default in UAS operations. Matters of data sharing, data integrity, and in some cases, the confidentiality of data are relevant for both data protection and telecommunication law.

The second problem regards the public purposes of such surveillance and monitoring UAS operations. The aim is to guarantee through the use of drones; public order, national security, the protection of health, and the rights and freedoms of others. The EU directive 2016/680 "on the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences", sets some important points. For example, Article 11 establishes some safeguards for "automated individual decision-making." Yet, data controllers are the "competent authorities" that determine the purposes and means of personal data processing in the criminal law field, whilst the data minimization principle simply disappears in the directive. What Article 4(1) (c) of the directive establishes is that data should not be "excessive in relation to the purposes for which they are processed." On top of that, as occurs with the GDPR, the directive does not apply to activities that fall outside the EU law, such as activities concerning national security or public order (Article 2(3)(a)). Correspondingly, the lawfulness of UAS operations for public purposes has often had to be determined on a single basis, that is, in relation to the law of the EU MSs.

The third problem regards the governance of UAS. In addition to the enforcement of current rules in the public and private sector, we should consider people's role and expectations. Social cohesion and acceptability are crucial in this context. Drones offer the opportunity of re-imagining the physical, technological and human space of our lives, in such a way that all stakeholders should be involved in co-regulating the use of UAS technology as

regards (also but not only) design and urban planning, privacy concerns and anti-discrimination issues. In light of these three sets of problems, time is ripe to seek for some solutions.

5. PRIVACY PRESERVING STRATEGIES

This section examines the set of open issues concerning the enforcement of the GDPR in UAS operations, the lawfulness of UAS operations for public purposes, and the governance of UAS technology, in accordance with three privacy and data protection safeguarding strategies. Next, focus is on the principle of data protection by design; then, Section 5(b) dwells on the role of organizational measures; finally, Section 5(c) mechanisms of co-regulation. The aim is to strike a fair balance between privacy and data protection rights on the one hand and, on the other, the protection of further rights and freedoms of groups and individuals, much as the protection of public order and national security, etc.

5.1. PRIVACY BY DESIGN

The principle of privacy by design and by default is enshrined in Article 25 of the GDPR. Whether the latter will be a toothless or powerful mechanism to protect data subjects depends on how its rules are finally going to be interpreted and applied by the courts. A first approach is given by Ann Cavoukian. In 2012, she proposed seven Privacy by Design principles for UAVs, so that: (1) safeguards should be proactive and not reactive; preventative and not remedial; (2) privacy should be the default setting; (3) embedded into design; (4) privacy by design should accommodate, in Cavoukian's wording, "all legitimate interests and objectives in a positive-sum, or doubly enabling 'win-win' manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. It avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both"; (5) privacy by design should ensure a full lifecycle for data protection; (6) visibility and transparency have to be embedded into a privacy by design approach, allowing as far as possible openness of technological solutions and standards to be adopted; and (7) a user-centric approach should prevail in the design of algorithmic ecosystems (Cavoukian 2012).

Along the same lines, in the aforementioned Opinion 01/2015 on privacy and data protection issues related to the use of drones, the Working Party recommended:

Manufacturers and operators to embed privacy friendly design choices and privacy friendly defaults as part of a privacy by design approach and to involve a Data Protection Officer (where available) in the design and implementation of policies related to the use of drones and to promote the adoption of Codes of conduct that can help the various industry stakeholders and operators to prevent infringements and to enhance the social acceptability of drones. (Article 29 Data Protection Working Party 2015)

Privacy seals have been recommended as well. “Even though such schemes shall not excuse data controllers from knowledge of their data protection and privacy commitments, the participation of drone operators and manufacturers in a general privacy seal approach could be supported as a means towards accountability and compliance” (Article 29 Data Protection Working Party 2015; de Miguel Molina et al. 2018).

Likewise, the EDPS has provided recommendations for manufacturers, suggesting also the EU Commission to propose RPAS companies (i) to adopt different categories of sensors depending on the private sector buyers’ business objective; (ii) to set up data retention by design; (iii) to provide tools with data protection friendly functionalities such as the possibility to turn on and off sensors in flight, automatic masking of private areas, automatic detection and pixelation of faces; (iv) to configure by default any functionality provided by the devices to the most privacy-friendly settings; and, (v) to provide clear information to the user on privacy issues that may arise when using the device (European Data Protection Supervisor 2014 and Wright and Finn 2016).

Other examples of technological solutions for GDPR-abiding drones include encryption tools for video recording by drones, streamed in real-time to a remote control center (Akkaya et al. 2019). Another strategy concerns the set up of differential privacy tools for managing data protection risks raised by drones through the design of flight maps, with the aim of minimizing both drones movements and personal data collection. Such tools should allow UAS operators choosing the best air corridor for their drones,

much as public authorities in the phase of authorization of new operations, or national Data Protection authorities that have to control the lawfulness of personal data processing by UAS operations (Bassi et al. 2019; Kim, Ben-Othman and Mokdad 2019).

The adoption of security measures for protecting the integrity of personal data and their flow, pursuant to Article 21 of the GDPR, is also relevant and should be implemented taking into account the long list of cybersecurity requirements and telecommunications rules, for example; licensed frequencies, as an integrated and standardized system for linking together principles, rules, technological and organizational measures in a comprehensive privacy design strategy (Hoepman 2014).

This section has illustrated the manifold ways in which the rather vague terminology of Article 25 GDPR has materialized with many data protection by design-projects for the use of drones today. Some of these projects could be our tomorrow’s standards.

5.2. ORGANIZATIONAL MEASURES

In addition to the general requirement to adopt technological and organizational measures according to the data protection by design principle, the GDPR provides specific organizational rules to protect privacy and data protection rights. Mandatory organizational rules on DPIA, data processing records, data breach and audit procedures, with the appointment of a data protection officer and the so called data protection agreements are among the most relevant examples.

The main function of these rules is to complement the privacy by design principle with the responsibilities of controllers set up by Article 24 of the GDPR, and more generally, their duties under the accountability principle set up by Article 5. According to this latter principle, public legislation establishes the principles that must be followed by data controllers (Article 5(1)), as well as the goals that they should strive for. However, it is largely up to controllers on how they should attain such outcomes, under the supervision of public guardians. Self-regulation thus concurs to design the decisional and managerial activities that regard all the lifecycle of the personal data processing: gathering, storing, using, sharing, etc.

The first step for every GDPR-abiding drone is to make the different roles and corresponding activities and responsibilities of multiple subjects involved in UAS operations explicit. To start with, (i) who decides running an operation; (ii) who is the operator; and, (iii) the pilot. When processing personal data, such clarity is mandatory pursuant to Articles 26 and 28 of the GDPR on 'joint controllers' and 'processors' of personal data. Transparency and accountability in further fields of the law, for example, tortious liability and risk insurance, recommend similar solutions.

The second step regards, in many cases, a DPIA. As stressed above in Section 3, a DPIA is mandatory when new technologies are involved and a large-scale data processing occurs, as with many UAS operations. The assessment does not only regard the protection of personal data rights set up by Article 8 of the European Charter of Fundamental Rights (the Charter), but should include all privacy concerns raised by the drone's data processing in the broad meaning of Article 7 of the Charter. Both EU norms on civil aviation and drones, and the GDPR hinge on a risk-based approach that aims to attain both transparency and accountability. In the case of UAS operations, both Article 11 of Regulation 2019/947 and Article 35 of the GDPR shall be complementary.

As suggested by David Wright and Rachel Finn, drone manufacturers, in addition to drone operators, should be part of the DPIA release process:

They are best placed to design privacy-preserving technologies into a drone. They may not want to carry out a PIA. They may prefer to shift the responsibility to the operators, but manufacturers clearly have a role to play in the design of drones that may otherwise be used for privacy-intrusive applications. Manufacturers have a responsibility just like industries causing environmental impacts. Manufacturers should see and exploit the benefit of being able to say that their drones are privacy-friendly, that they have conducted an impact assessment. (Wright and Finn 2016)

From this latter point of view, the adoption of codes of conduct, the use of privacy seals, or of user-friendly communications with signal standardization are recommended.

The accountability principle should encourage the forces of the market to make business in a GDPR-abiding way.

Several privacy or data protection authorities worldwide have meanwhile released recommendations for how to make DPIAs for UAS operations. They include the EDPS, Article 29 Working Party (EDPS 2014; Article 29 Data Protection Working Party 2015), and the Canadian Privacy Commissioner Ann Cavoukian (Cavoukian 2012). Rules on the right to be informed, on communication to the National Data Protection Authority, on data controllers that should maintain a register of all data processing, apply to all personal data processing performed by drones. An exception has been inserted by Article 74(3-5) of Regulation (EU) 2018/1139, which provides for some specific data protection provisions on time-limited data storage, the right to information, and the possibility for MSs and EASA to "restrict the scope of the rights of the data subject to access, rectify and erase personal data included in the repository to the extent that it is strictly necessary to safeguard civil aviation safety, in accordance with Article 23 of Regulation (EU) 2016/679". This is a new legal reference for work on data protection by design and by default solutions, which were introduced above in Section 3.

5.3. CO-REGULATION AND CIVIC INVOLVEMENT FOR UAS URBAN OPERATIONS

Privacy and other societal concerns are at the core of public debates and conferences in the drone sector (EASA 2019c). They are a formidable hurdle for introducing drones in urban and populated areas. Both National Civil Aviation Authorities and EASA are working for a common agenda on how to tackle social involvement and communication.

However, public efforts on standards, on models of compliance, or recommendations may be not enough. We can learn a lot from the social perception on the use of civilian drones. As suggested by some scholars:

Although participants frequently expressed discomfort with making strong recommendations due to lack of knowledge, participants expressed numerous recommendations reflecting desires for drones to be used for the 'greater good' and for the use of multi-way communication

processes when making decisions about the regulation of drones. (Walther et al. 2019)

Community involvement cannot be ignored (Resnik and Elliott 2019). Consultations with stakeholders and forms of participation can increase awareness of social benefits as well as the best practices and recommended behaviors for diminishing risks for safety and privacy. Municipalities, smart city experiments and companies who daily run drones for their activities must be part of the process. Public authorities and the forces of the market have an important role in designing best practices and making clear how drones behave in various situations and satisfy human needs. The creation of experimental areas is where people interact with drones, and thus looks at smart ways to address people's concerns and expectations.

The first special zone for the test of drones was established in Antwerp in January 2019.¹ Similarly, the experiments of the City of Turin, Italy, are noteworthy.² The Piedmont capital launched a City Lab for testing innovative technologies such as self-driving cars and drones within some areas of the town. Among the experiments with drones, the most relevant instance of the City Lab is so far, the monitoring of a public park within the city center. These forms of experimentation should allow us to further clarify the content of rules and standards for privacy friendly UAS operations over the next few years. Social acceptability and cohesion play a crucial role for a sound governance of this technology.

6. CONCLUSIONS

This paper has examined the impact of UAS technology on people's rights to privacy, personal data protection, and surveillance. On the one hand, the analysis assessed the most relevant provisions of the GDPR in this context, in order to stress that several crucial issues, such as business opportunities, behavior monitoring, and free flow of data in UAS operations, remain open. On the other hand, we scrutinized how this technology has affected the very notion of surveillance. Drones have an invisible, or non-detectable, mobile view that can access multiple

locations, following persons smoothly across fences or through windows for long periods. In addition to sound applications of UAS technology, such as in public parks, or through traffic monitoring in cities, with disaster recovery, or medicals delivery, this paper has shed light on more problematic and even troubling uses of drones, for example, the chilling effect that follows a new form of Foucault's panopticon.

These different kinds of concerns brought about by drones were thus examined in connection with the different fields under stress, i.e. Articles 7 (privacy) and 8 (data protection) of the EU Charter of Fundamental Rights, much as national legislations on public order and national security, the protection of health, and of the rights and freedoms of others. This paper has proposed a threefold approach to this complex legal framework and its open problems, in order to properly tackle some of the legal challenges of UAS technology.

First, focus was on privacy by design and data protection measures. The aim is to embed legal safeguards into UAS. Work on encryption tools for video recording by drones, and the design of tools for managing data protection risks raised by drones through personalized flight maps, illustrated how designing GDPR-abiding drones is feasible.

Second, the attention was drawn to the long list of organizational rules provided by the GDPR, in order to strike a fair balance between legal safeguards and business interests, fruitful applications of UAS operations and risks for privacy, personal data protection, and new forms of mass surveillance. The GDPR's principle of accountability (Article 5) illustrates how top-down forms of legal regulation (Article 5 (1)) have to be complemented with legal mechanisms of coordination and bottom-up approaches (Article 5 (2)).

Third, the role of social norms, acceptability, and cohesion were under scrutiny. Although public authorities, municipalities, and companies running drones on a daily basis have an important role in the governance of UAS, for example, designing standards and defining best practices, community involvement cannot be ignored. People

¹ <https://www.portofantwerp.com/en/drones-port-area>

² <https://www.torinocitylab.it/en/>

should understand how drones may behave in various situations and nevertheless, they have to have a say on whether UAS operations satisfy human needs. Regulators should pay attention to how they can ensure alignment with societal values, for example, through manifold forms of participatory mechanisms, in order to strengthen their understanding of the public opinion through a dialogue between all parts affected.

Finally, this paper illustrated some of the ways in which this is feasible, as shown by the experiments on 'special zones' for the use and test of drones in Antwerp and Turin.

7. REFERENCES

1. Article 29 Data Protection Working Party. 2015. *Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones*. Adopted on 16 June, 2015, WP 231.
2. Akkaya, K., Baboolal, V., Saputro, N., Uluagac, S., and Menouar, H. 2019. "Privacy-Preserving Control of Video Transmissions for Drone-based Intelligent Transportation Systems." In: *2019 IEEE Conference on Communications and Network Security (CNS)*. doi: 10.1109/CNS.2019.8802665.
3. Bassi, E. 2019. "European drones regulation: Today's legal challenges." In: *2019 International Conference on Unmanned Aircraft Systems*. ICUAS. Atlanta, GA (USA): IEEE, pp. 443-450.
4. Bassi, E., Bloise, N., Dirutigliano, J., Piero Fici, G.P., Pagallo, U., Primatesta, S., and Quagliotti, F. 2019. "The Design of GDPR-Abiding Drones Through Flight Operation Maps: A Win-Win Approach to Data Protection, Aerospace Engineering, and Risk Management." *Minds and Machines* 29 (4): 579-601.
5. Budinska, I. 2019. "On Ethical and Legal Issues of Using Drones." In: N. Aspragathos, P. Koustoumpardis, V. Moulianitis (eds.), *Advances in Service and Industrial Robotics. RAAD 2018. Mechanisms and Machine Science*, vol 67. Springer: Cham, pp. 710-717.
6. Calo, R. 2011. "The drone as privacy catalyst." *Stan. Law Rev. Onl.*, 64: 29-33, December 2011. <http://www.stanfordlawreview.org/online/drone-privacy-catalyst>.
7. Cavoukian, A. 2012. *Privacy and Drones: Unmanned Aerial Vehicles*. Ontario, Canada: Information and Privacy Commissioner.
8. Clarke, R. 2014. "The regulation of civilian drones' impacts on behavioural privacy". *Comp. Law and Sec. Rev.*, 30 (3): 286-305.
9. EU: *Charter of Fundamental Rights of the European Union*. (2000)
10. EU: *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*.
11. EU: *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*.
12. EU: *Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91*.
13. EU: *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems*.
14. EU: *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircrafts*.
15. European Union Aviation Safety Agency (EASA). 2018. *Opinion 01/2018 "Introduction of a regulatory framework for the operation of unmanned aircraft systems in the 'open' and 'specific' categories"*.
16. European Union Aviation Safety Agency (EASA). 2019a. *Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Commission Implementing Regulation (EU) 2019/947*. 9 October 2019.
17. European Union Aviation Safety Agency (EASA). 2019b. *Opinion 05/2019, Standard scenarios for UAS operations in the 'specific' category*. RMT.0729, release on November, 07, 2019.
18. European Aviation and Safety Agency (EASA). 2019c. *Regulators and industry unite in need to address societal concerns on drones*. Press release, 10 Dec. 2019. <https://>

- www.easa.europa.eu/newsroom-and-events/press-releases/regulators-and-industry-unite-need-address-societal-concerns.
19. European Data Protection Supervisor. 2014. *Opinion of the European Data Protection Supervisor 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 2014.
 20. European Parliament, Directorate General For Internal Policies – Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs. 2015. *Privacy and Data Protection Implications of the Civil Use of Drones, In-depth Analysis*.
 21. Finn, R. L. and Donovan, A. 2016. "Big data, drone data: Privacy and ethical impacts of the intersection between big data and civil drone deployments." In: B. Custers (ed.). *The Future of Drone Use. Opportunities and Threats from Ethical and Legal Perspectives*. The Hague: Asser Press, pp. 47-70.
 22. Finn, R. L. and Wright, D. 2016. "Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organisations". *Computer Law & Security Review*, 32: 577–586.
 23. Floridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, Ch., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., and Vayena, E. 2018. "AI4People - An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations." *Minds and Machines*, 28 (4): 689-707.
 24. Garcia-Aunon, P., Roldan, J.J., and Barrientos, A. 2019. "Monitoring traffic in future cities with aerial swarms: Developing and optimizing a behavior-based surveillance algorithm." *Cognitive Systems Research*, 54: 273-286. <https://www.sciencedirect.com/science/article/pii/S1389041718303279>.
 25. Grubestic, T.H. and Nelson, J.R. 2020. *UAVs and Urban Spatial Analysis. An Introduction*. Springer: Cham.
 26. Hell, P.M. and Varga, P.J. 2019. "Drone Systems for Factory Security and Surveillance." *Interdisciplinary Description of Complex Systems*, 17 (3-A): 458-467. <https://doi.org/10.7906/indecs.17.3.4>.
 27. Hoepman, J.H. 2014. "Privacy Design Strategies." In N. Cuppens-Boulahia et al. (eds.) *ICT Systems Security and Privacy Protection*. SEC 2014. *IFIP Adv. in Inform. and Comm. Techn.*, 428: 446-459. Berlin – Heidelberg: Springer.
 28. Kim, H., Ben-Othman, J. and Mokdad, L. 2019. "UDiPP: A Framework for Differential Privacy Preserving Movements of Unmanned Aerial Vehicles in Smart Cities." *IEEE Transactions on Vehicular Technology*, 68 (4): 3933-3943.
 29. Marin, L. and Krajčiková, K. 2016. "Deploying Drones in Policing Southern European Borders: Constraints and Challenges for Data Protection and Human Rights." In A. Završnik (ed.) *Drones and Unmanned Aerial Systems. Legal and Social Implications for Security and Surveillance*. Cham: Springer International, pp. 101-127.
 30. de Miguel Molina, M., Santamarina Campos, V., Segarra Oña, M.V., and de Miguel Molina, B. 2018. "Regulation, Co-Regulation and Self- Regulation of Civil Unmanned Aircrafts in Europe." *World Ac. of Science, Eng. and Techn. Intern. J. of Law and Pol. Sc.*, 12 (5): 498-501.
 31. Mufford, J.T., Hill, D.J., Flood, N.J., and Church, J.S. 2019. "Use of unmanned aerial vehicles (UAVs) and photogrammetric image analysis to quantify spatial proximity in beef cattle." *Journal of Unmanned Vehicle Systems*, 7 (3): 194-206. <https://doi.org/10.1139/juvs-2018-0025>.
 32. Pagallo, U. 2017a. "From Automation to Autonomous Systems: A Legal Phenomenology with Problems of Accountability." In: *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence*. IJCAI-17. pp. 17-23.
 33. Pagallo, U. 2017b. "The Group, the Private, and the Individual: A New Level of Data Protection?" In L. Taylor, L. Floridi and B. van der Sloot (eds.). *Group Privacy: New Challenges of Data Technologies*. Dordrecht: Springer, pp. 159-173.
 34. Pagallo, U., Casanovas, P., and Madelin, R. 2019. "The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data." *The Theory and Practice of Legislation*, 7 (1): 1-25, DOI: 10.1080/20508840.2019.1664543.
 35. Pannozzi, P., Valavanis, K.P., Rutherford, M.J., Guglieri, G., Scanavino, M. and F. Quagliotti. 2019. "Urban Monitoring of Smart Communities Using UAS." In: *2019 International Conference on Unmanned Aircraft Systems*. ICUAS. Atlanta, GA (USA): IEEE, pp. 866-873. doi: 10.1109/ICUAS.2019.8798310.
 36. Resnik, D.B. and Elliott, K.C. 2019. "Using Drones to Study Human Beings: Ethical and Regulatory Issues." *Sci Eng Ethics* 25: 707–718. <https://doi.org/10.1007/s11948-018-0032-6>.
 37. Rice, S., Tamilselvan, G., Winter, S.R., Milner, M.N., Anania, E.C., Sperlak, L., and Marte, D.A. 2018. "Public perception of UAS privacy concerns: a gender comparison." *Journal of Unmanned Vehicle Systems*, 6: 83-99. <https://doi.org/10.1139/juvs-2017-0011>.
 38. Songsheng, L. 2019. "Wildfire early warning system based on wireless sensors and unmanned aerial vehicle."

Journal of Unmanned Vehicle Systems, 7:76-91. <https://doi.org/10.1139/juvs-2018-0022>.

39. Walther, J., Pytlik Zillig, L., Detweiler, C., and Houston, A. 2019. "How people make sense of drones used for atmospheric science (and other purposes): hopes, concerns, and recommendations." *Journal of Unmanned Vehicle Systems*, 7:219-234. <https://doi.org/10.1139/juvs-2019-0003>].
40. Wright, D. and Finn, R. 2016. "Making Drones more Acceptable with Privacy Impact Assessment." In: B. Custers (ed.). *The Future of Drone Use. Opportunities and Threats*