



# **Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations**

## **Final Report**



Rachel L. Finn and David Wright,  
Trilateral Research & Consulting, LLP

Laura Jacques and Paul De Hert,  
Vrije Universiteit Brussel

*November – 2014*



**EUROPEAN COMMISSION**

Directorate-General Enterprise and Industries

Directorate G— Aerospace, Maritime, Security and Defence Industries

Unit G5— G.5 Defence, Aeronautic and maritime industries

Contact: Jean-Pierre LENTZ, Policy Officer

E-mail: [Jean-Pierre.LENTZ@ec.europa.eu](mailto:Jean-Pierre.LENTZ@ec.europa.eu)

*European Commission*

*B-1049 Brussels*

**Study on  
privacy, data protection  
and ethical risks  
in civil Remotely Piloted Aircraft  
Systems operations**

Final Report

***Europe Direct is a service to help you find answers  
to your questions about the European Union.***

**Freephone number (\*):**

**00 800 6 7 8 9 10 11**

(\* ) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

## **LEGAL NOTICE**

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

More information on the European Union is available on the Internet (<http://www.europa.eu>).

Luxembourg: Publications Office of the European Union, 2014

ISBN 978-92-79-44126-4

doi: 10.2769/756525

© European Union, 2014

Reproduction is authorised provided the source is acknowledged.

*Printed in Belgium*

PRINTED ON ELEMENTAL CHLORINE-FREE BLEACHED PAPER (ECF)

PRINTED ON TOTALLY CHLORINE-FREE BLEACHED PAPER (TCF)

PRINTED ON RECYCLED PAPER

PRINTED ON PROCESS CHLORINE-FREE RECYCLED PAPER (PCF)

Image © Alexander Kolomietz, image # 72749828, Source: Fotolia.com

EXECUTIVE SUMMARY.....	10
1 INTRODUCTION .....	14
1.1 Privacy, data protection and ethical issues .....	15
2 METHODOLOGY.....	21
3 PRIVACY, DATA PROTECTION AND ETHICAL CONCERNS RELATED TO RPAS TECHNOLOGY....	23
3.1 Introduction and overview .....	23
3.2 Privacy issues associated with RPAS.....	24
3.2.1 The concept of privacy.....	24
3.2.2 RPAS in observation and surveillance activities .....	26
3.2.3 Privacy concerns related to visual photography and surveillance activities.....	30
3.2.4 Privacy concerns related to non-visual surveillance activities .....	37
3.2.5 Privacy concerns related to non- surveillance activities: chilling effect and property.....	40
3.2.6 Summary.....	40
3.3 Data protection issues associated with RPAS.....	41
3.3.1 The data protection risks inherent in RPAS technology .....	42
3.3.2 Summary.....	47
3.4 Ethical issues related to RPAS.....	47
3.4.1 Ethical concerns related to the use of RPAS.....	48
3.4.2 Summary.....	51
3.5 Conclusion.....	51
4 RPAS TECHNOLOGY AND EUROPEAN PRIVACY AND DATA PROTECTION LAW.....	53
4.1 Introduction .....	53
4.2 European law protecting the right to private life .....	54
4.2.1 Overview.....	54
4.2.2 Council of Europe law - Article 8 ECHR.....	54
4.2.3 European Union Law – Article 7 CFREU.....	64
4.2.4 Conclusion .....	64
4.3 The European law on personal data protection .....	65
4.3.1 General .....	65
4.3.2 Council of Europe Law (Article 8 ECHR and the Convention 108).....	66
4.3.3 The Fundamental Rights Charter (Article 8) and the Lisbon Treaty (Article 16) .....	67
4.3.4 The Data Protection Directive 95/46/EC .....	67
4.3.5 The Proposed General Data Protection Regulation .....	75
4.3.6 The Framework- Decision 2008/977/JHA.....	79
4.3.7 The Proposed Directive regulating data protection in the law enforcement sector .....	80
4.3.8 The e-Privacy Directive .....	80
4.3.9 The Directive 2006/24/EC on the retention of data.....	83
4.3.10 Conclusion .....	84

4.4	General Conclusion .....	84
5	RPAS TECHNOLOGY AND DOMESTIC PRIVACY AND DATA PROTECTION LAW .....	86
5.1	Introduction .....	86
5.2	Member States already using civil RPAS.....	87
5.2.1	The United Kingdom .....	87
5.2.2	France .....	93
5.2.3	Germany .....	99
5.2.4	Italy .....	104
5.2.5	Sweden .....	107
5.2.6	Denmark .....	112
5.3	Member State preparing RPAS regulations .....	117
5.3.1	Belgium .....	117
5.3.2	Conclusion .....	122
5.4	An overview of the current DPA positions and activities .....	123
5.4.1	The Czech Republic.....	123
5.4.2	Belgium .....	124
5.4.3	The UK.....	125
5.4.4	France .....	126
5.5	Third Countries .....	128
5.5.1	Switzerland .....	128
5.5.2	The United States.....	131
5.5.3	Conclusion .....	134
5.6	International soft-law measures.....	135
5.6.1	Recommended Guidelines for the Use of Unmanned Aircraft.....	135
5.6.2	Unmanned Aircraft System Operations Industry “Code of Conduct” .....	136
5.6.3	Drone Journalism Code.....	136
5.6.4	Conclusion .....	137
5.7	General Conclusion .....	137
6	CONSULTING WITH KEY STAKEHOLDERS.....	139
6.1	Industry analysis .....	139
6.1.1	Overview.....	139
6.1.2	Capabilities and applications .....	140
6.1.3	RPAS data collection .....	142
6.1.4	Industry perspectives on privacy and data protection.....	143
6.1.5	Consultations and regulations.....	145
6.2	DPA Analysis.....	147
6.2.1	Overview .....	147
6.2.2	Privacy, data protection and ethical issues .....	148
6.2.3	Consultations and regulations .....	155
6.3	Civil society organisation analysis.....	156
6.3.1	Overview .....	156

6.3.2	Privacy, data protection and ethical concerns .....	158
6.3.3	Consultations .....	163
6.4	Civil Aviation Authority analysis.....	164
6.4.1	Overview .....	164
6.4.2	RPAS regulations.....	165
6.4.3	CAA perspectives on privacy and data protection .....	166
6.4.4	Consultations and advice to RPAS users.....	169
6.5	Summary and conclusions .....	170
7	RPAS CAPABILITIES AND APPLICATIONS.....	173
7.1	Introduction .....	173
7.2	Commercial operators .....	174
7.2.1	Infrastructure inspection .....	174
7.2.2	Other visual services.....	176
7.2.3	Mapping.....	176
7.2.4	Earth observation .....	178
7.2.5	Precision agriculture .....	179
7.2.6	Novel services .....	180
7.3	Law enforcement and government operators .....	181
7.3.1	Surveillance of people .....	181
7.3.2	Civil protection.....	184
7.3.3	Regulatory enforcement.....	185
7.4	Journalists and filmmakers .....	186
7.5	Telecommunication providers .....	188
7.6	Private individuals using RPAS for household or personal uses .....	189
7.7	Summary.....	190
8	PRIVACY, DATA PROTECTION AND ETHICS IN RPAS SCENARIOS.....	194
8.1	Introduction .....	194
8.2	Commercial operators .....	197
8.2.1	Infrastructure inspection .....	197
8.2.2	Other visual services.....	202
8.2.3	Novel services .....	219
8.3	Law enforcement and government operators .....	224
8.3.1	Surveillance of people .....	225
8.3.2	Civil protection.....	230
8.3.3	Regulatory enforcement.....	235
8.4	Journalists and filmmakers .....	240
8.4.1	Filmmaking .....	240
8.4.2	Sensationalist journalism.....	245
8.5	Telecommunication providers .....	250
8.6	Private individuals.....	251
8.7	Summary.....	255

9	THE ADEQUACY OF CURRENT EU REGULATORY FRAMEWORKS.....	257
9.1	Introduction and overview .....	257
9.2	Current and emerging RPAS applications not covered by the current European privacy framework.....	257
9.3	Legal gaps in the current and proposed regulatory framework.....	260
9.4	Implementation and enforcement difficulties of the current Data Protection Directive 95/46/EC.....	272
9.5	Concluding observations.....	289
10	THE ADEQUACY OF CURRENT MEMBER STATE REGULATORY FRAMEWORKS .....	291
10.1	Introduction and overview .....	291
10.2	Member States already using civil RPAS.....	291
10.2.1	The United Kingdom .....	291
10.2.2	France .....	297
10.2.3	Germany .....	301
10.2.4	Italy .....	305
10.2.5	Sweden .....	310
10.2.6	Denmark .....	311
10.3	Member States preparing RPAS regulations .....	313
10.3.1	Belgium .....	313
10.4	Concluding Observations - The legal gaps remaining.....	317
10.4.1	Commercial operators.....	317
10.4.2	Journalists .....	319
10.4.3	State agencies.....	320
10.4.4	Private individuals (including recreational and private uses).....	321
10.4.5	Concluding Observations.....	321
11	COMPLEMENTARY MEASURES TO ASSIST IN ADDRESSING PRIVACY, DATA PROTECTION AND ETHICAL ISSUES .....	323
11.1	Introduction and overview .....	323
11.2	Legislative solutions.....	323
11.2.1	Commercial operators.....	324
11.2.2	State agencies.....	327
11.2.3	Journalists.....	328
11.2.4	Private individuals.....	329
11.3	Soft law measures: technological and voluntary solutions .....	329
11.3.1	Technological solution - Privacy by Design.....	329
11.3.2	Technological solution - Data Protection Impact Assessment .....	333
11.3.3	Technological solution - Surveillance Impact Assessment .....	338
11.3.4	Voluntary Solutions - Privacy Audits.....	339
11.3.5	Voluntary solution - Self-Regulations .....	342
11.3.6	Voluntary solution - Privacy Certification Schemes.....	346
11.3.7	Usage restrictions .....	349
11.4	Concluding remarks .....	351

12	RPAS REGULATION AND CIVIL AVIATION AUTHORITIES.....	352
12.1	Privacy and data protection issues addressed.....	352
12.2	General RPAS flight requirements.....	353
12.3	Summary.....	355
13	POLICY RECOMMENDATIONS FOR PRIVACY AND DATA PROTECTION ISSUES IN CIVIL RPAS.....	357
13.1	Introduction.....	357
13.2	Industry-specific recommendations.....	358
13.3	Raising awareness.....	359
13.4	Information and transparency protocols.....	362
13.5	Impact assessment and soft law measures.....	365
13.6	Monitoring good practice.....	368
13.7	Other recommendations.....	370
13.8	Summary.....	371
14	CONCLUSION.....	373
15	ANNEX A: RPAS CAPABILITIES AND APPLICATIONS.....	376
15.1	Introduction.....	376
15.2	Technical specifications.....	377
15.2.1	Size and weight.....	377
15.2.2	Control systems.....	380
15.2.3	Flight.....	383
15.3	Capabilities.....	385
15.3.1	Aerial photography and video streaming.....	385
15.3.2	Wide area surveillance.....	386
15.3.3	Geospatial analytics.....	387
15.3.4	Artificial intelligence and “smart drones”.....	387
15.3.5	Sampling and detection technologies.....	388
15.3.6	Telecommunications.....	388
15.3.7	Non-lethal weapons.....	389
15.4	Operators and applications.....	390
15.4.1	Classifying RPAS applications.....	390
15.5	Summary and conclusions.....	394
16	ANNEX B: REVIEW OF EUROPEAN AND NATIONAL RPAS SAFETY REGULATIONS.....	395
16.1	Introduction.....	395
16.2	EU Aviation Safety requirements.....	397
16.3	Requirements in European Member States.....	398
16.4	Summary and conclusions.....	410

## EXECUTIVE SUMMARY

The use of remotely piloted aircraft systems (RPAS) is rapidly expanding for a range of civil and commercial purposes. However, it is already apparent that existing RPAS capabilities and applications raise a number of privacy, data protection and ethical issues, some of which are recognised in the European RPAS Steering Group's *Roadmap*.<sup>1</sup> The purpose of this project is to support the development of harmonised and robust policies to enable the civil use of Remotely Piloted Aircraft Systems (RPAS) whilst addressing existing and potential privacy, data protection and ethical concerns. The project has resulted in a series of policy recommendations, in consultation with a range of relevant RPAS stakeholders (e.g., Data Protection Authorities (DPAs), Civil Aviation Authorities (CAAs), RPAS operators and civil society organisations, etc.), to support European innovation whilst protecting privacy, personal data and ethical safeguards. In order to construct these policy recommendations, the project was undertaken in two parts. Part I:

- identified the legislative instruments relevant to RPAS in Europe, Member States and third countries (including the positions of relevant DPAs),
- consulted with key stakeholders (RPAS industry representatives, Data Protection Authorities, Civil Aviation Authorities and civil society organisations) to examine their understanding of the risks RPAS pose to privacy, data protection and ethics, and
- conducted a privacy, data protection and ethical risk analysis of typical current and potential RPAS applications

In part II, the project:

- examined the adequacy of the existing legislative framework relevant to RPAS in Europe and Member States, and
- considered the extent to which CAAs might be mobilised to regulate privacy, data protection and ethical issues based on existing regulations.

### 1. Identifying the legislative framework

Chapters 3, 4 and 5 examine the relevant privacy, data protection and ethical issues associated with RPAS and identify the legislative framework relevant to RPAS. In Europe, the use of aerial technologies for photography, surveillance and other applications is covered by Article 7 (Respect for private life) and Article 8 (Data protection) of the Charter of Fundamental Rights of the European Union, 2000/C 364/01(CFREU), and by the Right to respect for private life of Article 8 European Convention on Human Rights. The use of RPAS for civil purposes must also conform to the obligations outlined in the Data Protection Directive 95/46/EC, when personal data is collected, processed or stored. In addition to these legislative mechanisms focused on privacy and data protection in Europe, national-level legislation related to privacy and data protection (particularly national laws which implement the Data Protection Directive) as well as national laws relevant to telecommunications, CCTV and police surveillance activities are also applicable to RPAS usage. The analysis of national laws focused on countries that allow RPAS missions, specifically, the UK, France, Germany, Italy, Sweden, Denmark and Belgium. This analysis finds that the law constructs five different groups of RPAS operators: commercial/corporate operators, journalists, police and government operators, telecommunications and Internet providers and natural persons using

---

<sup>1</sup> European RPAS Steering Group, *Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System*, June 2013. <http://ec.europa.eu/enterprise/sectors/aerospace/uas/>

RPAS for personal or household purposes. While privacy and data protection laws, as well as others, all apply to commercial/corporate RPAS operators, the other categories of operator may, in some circumstances, derogate from the obligations within these legal instruments.

## 2. Consultation exercises

Chapter 6 of the report presents the findings of a series of consultations with four different types of stakeholders associated with civil RPAS – industry representatives, Data Protection Authorities (DPAs), civil society organisations (CSOs) and Civil Aviation Authorities (CAAs). These consultations took the form of surveys as well as consultation exercises such as panels and workshops. The consultations reveal the urgency of taking policy action in this area. They demonstrate that experts such as DPAs and CSOs report that there are significant risks associated with current RPAS capabilities and applications, which are largely unrecognised by RPAS industry representatives. Therefore, more education is needed on all sides of the sector about the actual uses of RPAS, the potential privacy and data protection issues raised and ways of addressing these issues.

## 3. Privacy, data protection and ethical risk analysis

Chapters 7 and 8 of the report are comprised of the privacy data protection and ethical risk analysis of typical RPAS operators. In Chapter 7, the different RPAS users are linked with particular, typical applications, and the missions, technologies used, target and data collected for each type of mission is identified. In addition, each mission type that may collect personal data is associated with at least one typical mission scenario that RPAS operators specifically validated to ensure their realism. In relation to commercial usages, we examined infrastructure inspection, other visual services, mapping, earth observation, precision agriculture and novel services. In relation to police and governments, we examined surveillance of people, critical infrastructure protection and regulatory enforcement. Finally, we also constructed scenarios for journalists, filmmakers and private individuals.

These scenarios were the basis of individual risk analyses, based on the following privacy, data protection and ethical issues identified in Chapter 3.

*Table 1: Privacy, data protection and ethical issues relevant to RPAS*

<b>Privacy</b>	<b>Data protection</b>	<b>Ethical issues</b>
Chilling effect	Transparency	Safety
Dehumanisation of the surveilled	Data minimisation	Public dissatisfaction
Transparency and visibility, accountability and voyeurism	Proportionality	Discrimination
Function creep	Purpose limitation	
Bodily privacy	Consent	
Privacy of location and space	Accountability	
Privacy of association	Data security	
	Rights of access	
	Rights of correction	
	Third country transfers	
	Rights of erasure	

The risk analysis provides information on how each scenario scores in relation to each of these individual issues, and where appropriate, provides information on how RPAS operators can mitigate the risks posed within each of these individual elements. These risk reduction practices include:

- giving members of the public information about the activities being undertaken,
- minimising the amount of data that is collected,
- anonymising data that is collected,
- ensuring that the data is only used for the original purpose for which it was collected, eliminating or reducing the storage of personal data, and
- ensuring that data that is processed or stored is properly secured.

Providing information to members of the public, in particular, is a powerful risk reduction mechanism as it addresses privacy issues independent of the type of operation being undertaken, as well as potential data protection issues in operations that collect personal data.

#### **4. Adequacy of the regulatory framework**

In Chapters 9 and 10 we examine the adequacy of the European and Member State regulatory frameworks (identified in Chapters 4 and 5) for meeting the privacy, data protection and ethical risks associated with civil uses of RPAS. This report finds that the current European and Member State regulatory frameworks are largely adequate to address the privacy, data protection and ethical impacts of RPAS, primarily because they are technology neutral. Rights to privacy, as well as current data protection frameworks include provisions for addressing each of these risks. Instead, the real problem is educating the RPAS industry about their obligations, and enforcing the regulatory mechanisms that are in place. In addition, we further argue that the proposed amendments contained in the GDPR, particularly requirements to conduct a Data Protection Impact Assessment and to include privacy-by-design features in all data collection and processing activities, should contribute to reducing these gaps and encouraging more responsible RPAS practice. Nevertheless, we highlight particular good practice elements and very specific gaps present in each of these contexts.

#### **5. Recommendations**

We conclude that a combination of existing regulatory instruments and soft law measures such as Privacy Impact Assessments (PIAs) elements will assist RPAS operators in developing innovation applications and services by combining harmonised, technology-neutral regulations across Europe with a tailored impact assessment. In particular, they are organised under five main headings:

- Industry-specific recommendations for reducing risk (described above)
- Raising awareness of privacy and data protection requirements in the RPAS industry
- Enacting information and transparency protocols
- Conducting mandatory assessments of privacy and data protection issues for each type of operation (privacy impact assessments)
- Identifying stakeholders to monitor good practice in privacy and data protection.

Each of the key stakeholders involved in the RPAS eco-system has roles to play to meet these obligations. As such, under each of these broad recommendations, we include information specific to different stakeholder types. In addition, where possible, we provide suggested measures, options or steps to achieve each of these goals. Each of these policy

recommendations, and their specific sub-recommendations, represents improved practice in meeting privacy and data protection requirements. Taken together, these measures provide a comprehensive, good-practice package that encourages responsible use of RPAS in civil applications.

We conclude the report by highlighting a few, **key recommendations for specific types of stakeholder**.

First, we believe that the planned introduction of mandatory Data Protection Impact Assessments as part of the GDPR offers an opportunity for the European Commission to take the lead in ensuring that the RPAS industry takes their privacy and data protection obligations seriously. The RPAS industry must be supported to succeed in this endeavour. As such, we recommend that the European Commission support the development of a PIA framework for RPAS that can be evaluated by the Article 29 Working Party. This would follow established good practice in the RFID and smart meter sectors, and offer a robust and harmonised framework and methodology that would assist the RPAS industry in substantially meeting these obligations.

Second, this report reveals that there is a clear need for industry and Data Protection Authorities to establish an ongoing dialogue. This dialogue would protect citizens' fundamental rights, and protect the emerging RPAS industry from legal liabilities. As such, it offers an opportunity for both stakeholders to improve practice in this area. However, the resources of DPAs are stretched, and many RPAS industry representatives are SMEs with similarly stretched resources. The EC can support this collaboration by hosting regulator workshops or convening and funding a regular working group on this issue.

Third, the European Commission needs to support awareness-raising activities targeted at the RPAS industry that clarify privacy and data protection requirements as well as publicise privacy-by-design features and practices that could mitigate the privacy and data protection risks associated with RPAS missions. This could include working with Member States to develop training courses and high-quality information materials in multiple languages for industry representatives. It could also include commissioning an information portal and forum to share information about RPAS legal obligations and risk mitigation measures.

Fourth, different stakeholders within the civil RPAS sector should work together to develop a national or cross-national information resource to enable citizens to identify the missions and operators associated with individual RPAS. These tools will meet transparency requirements for those missions that are collecting personal data, and will build public trust in relation to missions that are not collecting such data.

Finally, the European Commission should work with EASA, JARUS and other organisations to deploy CAAs as a natural gatekeeper for the civil RPAS sector. CAAs should be encouraged to issue aerial work permits and to ensure that legal obligations such as transparency tools or DPIA requirements have been conducted. This will require closer collaboration between CAAs and DPAs to enable them to mobilise their complementary competencies in this area.

# 1 INTRODUCTION

The deployment of Remotely Piloted Aircraft Systems (RPAS, actually an old 20<sup>th</sup> century technology<sup>2</sup>) entails many benefits for European manufacturing and operating industries and citizens. Although RPAS are not new, there have been significant recent advances in their relative size, weight, the payloads they carry and, consequently, the novel and emerging applications for which they may be used. These developments, particularly in the “civil” sphere (i.e., commercial, non-commercial and government non-military), yield several potential benefits for European industry and its citizens. Specifically, the European RPAS Steering Group argued that “the emerging technology of RPAS... can contribute to boost industrial competitiveness, promote entrepreneurship and create new businesses in order to generate growth and jobs.”<sup>3</sup> The Unmanned Aerial Vehicle Systems Association envisions potential civil or commercial applications of unmanned aircraft in the areas of security (including border patrol and policing), crop management, search and rescue, communications, infrastructural and environmental monitoring, surveying and disaster management.<sup>4</sup>

The non-military use of RPASs is already significant and extensive, for example, in law enforcement and policing activities; border patrols; global environmental monitoring and security related operations (GMES); fire services; traffic management and monitoring; fisheries protection; oil and gas pipeline surveying; coverage of large public events; agricultural management and crop monitoring; power line surveying; aerial photography, review and assessment of mines, quarries, dams, construction and building sites, and houses; critical infrastructure assessments in hazardous and non-hazardous environments; missing person searches, etc. As the *Roadmap* states, **“Being remotely piloted, RPA can perform tasks that manned systems cannot perform, either for safety or for economic reasons.”**<sup>5</sup> **This foregrounds the relative cheapness of using RPASs for many of the deployments, compared to conventional helicopters (though most operators foresee a mix of aircraft) and, significantly, the contribution that RPASs make to enhancing the health and safety of human beings tasked with dangerous jobs, e.g., in dealing with floods, disaster relief, volcanic eruptions, earthquakes, nuclear plant accidents.**

Police and government non-military uses are often the most controversial and least accepted by members of the public.<sup>6</sup> Early applications of RPAS by such authorities have included their use for aerial photography and surveillance by authorities in Europe and North America to:

- monitor crowds at events such as festivals<sup>7</sup>, protests<sup>8</sup> and sporting events<sup>9</sup>,

---

<sup>2</sup> The first unmanned aircraft was used by the US Navy in WWI. Quoted from Aviation Safety Unmanned Aircraft Programme Office, 2008, in McBride, Paul, “Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations”, *Journal of Air Law and Commerce*, Vol. 74, 2009, p. 628.

<sup>3</sup> European RPAS Steering Group, *Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System*, June 2013, p. 5. <http://ec.europa.eu/enterprise/sectors/aerospace/uas/>

<sup>4</sup> UAVS, “Civil or Commercial Applications”, 2011. <http://www.uavs.org/commercial>

<sup>5</sup> Directorate General Enterprise and Industry, “Remotely Piloted Aircraft Systems (RPAS)”, 24 September 2013. <http://ec.europa.eu/enterprise/sectors/aerospace/uas/>

<sup>6</sup> Enterprise and Industry Directorate General, *Tender Specifications: Study on privacy and data protection issues related to the use of civil RPAS*, 12 August 2013.

<sup>7</sup> Randerson, James, “Eye in the sky: police use drone to spy on V festival”, *The Guardian*, 21 Aug 2007. <http://www.guardian.co.uk/uk/2007/aug/21/ukcrime.musicnews>

<sup>8</sup> Hull, Liz, “Drone makes first UK ‘arrest’ as police catch car thief hiding under bushes”, *Daily Mail*, 12 Feb 2010.

- prevent anti-social behaviour<sup>10</sup>,
- detect marijuana cultivation<sup>11</sup>, and
- support police in pursuits and operations<sup>12</sup>.

Canadian police are responsible for the first photographs taken by an RPAS admitted as evidence in court after a local police force, in 2007, used a UAV to photograph a homicide scene<sup>13</sup>, suggesting that the information detected and/or recorded by RPAS may have forensic utility. These uses of visual photography payloads, the potential extension to other types of payloads (for example, thermal imaging cameras, communications relay and biometric identification), the decreasing size of RPAS devices and their use by commercial organisations and private individuals introduce privacy, data protection and ethical concerns that extend beyond analogies such as CCTV and police helicopter surveillance. This report examines the use of RPAS by these different stakeholders and argues that the risks associated with commercial uses of RPAS are significant; however, the risks associated with police and private, individual uses are the most problematic. As such, industry has an opportunity to lead the way by ensuring that commercial uses of RPAS adhere to robust privacy and data protection frameworks. Otherwise, the public may remain unconvinced about the use of RPAS, which may hinder the rollout of this technology and the associated economic and social benefits they are expected to introduce.

## 1.1 Privacy, data protection and ethical issues

It is already apparent that existing RPAS capabilities and applications raise a number of privacy, data protection and ethical issues, some of which are recognised in the RPAS *Roadmap*. In relation to privacy, evidence from RPAS development and deployment projects suggest that privacy and data protection issues are superseded by a focus on the technical capabilities of RPAS<sup>14</sup> and questions of safety (e.g., what kind of technical specifications are needed to avoid collisions in civilian airspace, how should regulators deal with the influx of inexperienced remote pilots, what technical requirements should be fulfilled before a national civil aviation association certifies a RPAS<sup>15</sup>, etc.). Safety issues are of paramount importance,

---

<http://www.dailymail.co.uk/news/article-1250177/Police-make-arrest-using-unmanned-drone.html#ixzz1JV7EKR1N> and Whitehead, John W., *Drones Over America: Tyranny at Home*, The Rutherford Institute, Charlottesville, VA, 28 June 2010.

[http://www.rutherford.org/articles\\_db/commentary.asp?record\\_id=661](http://www.rutherford.org/articles_db/commentary.asp?record_id=661)

<sup>9</sup> Eick, Volker, *The Droning of the Drones: The increasingly advanced technology of surveillance and control*, Statewatch Analysis, No. 106, 2009, p. 1. <http://www.statewatch.org/analyses/no-106-the-droning-of-drones.pdf>

<sup>10</sup> Randerson, op. cit., 2007.

<sup>11</sup> McCullagh, Declan, “Drone aircraft may prowl U.S. skies”, *CNET News*, 29 March 2006.

[http://news.cnet.com/Drone-aircraft-may-prowl-U.S.-skies/2100-11746\\_3-6055658.html#ixzz1JURmGB4a](http://news.cnet.com/Drone-aircraft-may-prowl-U.S.-skies/2100-11746_3-6055658.html#ixzz1JURmGB4a)

<sup>12</sup> Eick, op. cit., 2009, p. 4.

<sup>13</sup> “Canadian Police Push Limits of Civilian UAV Laws”, *Homeland Security News Wire*, 17 Feb 2011. <http://homelandsecuritynewswire.com/canadian-police-push-limits-civilian-uavs-laws>

<sup>14</sup> McCullagh, Declan, “Drone aircraft may prowl U.S. skies”, *CNET News*, 29 March 2006.

[http://news.cnet.com/Drone-aircraft-may-prowl-U.S.-skies/2100-11746\\_3-6055658.html#ixzz1JURmGB4a](http://news.cnet.com/Drone-aircraft-may-prowl-U.S.-skies/2100-11746_3-6055658.html#ixzz1JURmGB4a);

OPARUS, “Concept and Approach”, 2010, <http://www.oparus.eu/index.php/concept-a-approach>; Nevins, Joseph, “Robocop: Drones at Home”, *Boston Review*, Jan/Feb 2011.

<http://www.bostonreview.net/BR36.1/nevins.php>.

<sup>15</sup> See, for example, Joint Authorities for Rulemaking of Unmanned Systems (JARUS) – UAS Airworthiness Group, *Certification Specification for Light Unmanned Rotorcraft Systems (CS-LURS)*, Deliverable 1 (Version 0.1), 2012.

and the protection of individuals, animals and structures on the ground is a significant ethical issue. However, experts argue that privacy and data protection issues, as well as other ethical issues, are also significantly implicated by these technologies. In Europe, the use of aerial technologies for photography, surveillance and other applications is covered by Article 7 (Respect for private life) and Article 8 (Data protection) of the Charter of Fundamental Rights of the European Union, 2000/C 364/01(CFREU), and by the Right to respect for private life of Article 8 European Convention on Human Rights (ECHR, Rome, 4 November 1950). The report examines these legislative instruments and outlines how RPAS may impact these, and how RPAS operators may address these impacts.

The use of RPAS for aerial photography and other applications may also be covered by various secondary legislative EU instruments with regard to data protection, most notably the Data Protection Directive 95/46/EC. Data protection applies whenever personal data are processed, and applies during the monitoring of public space, especially if the images are recorded. The primary bottleneck for the applicability of data protection is that the footage needs to contain *personal data*<sup>16</sup>, that is, images of natural persons that are clear enough to lead to an identification, in order to fall under the scope of the Data Protection Directive. Consequently, any use of RPAS for aerial photography that captures members of the public and records the footage must comply with this instrument. This does not mean that the RPAS cannot operate, it simply means that operators must adhere to a number of specific controls. Notably, the protection of personal data requires that the processing of personal data is *legitimate* and *proportionate* to the aim it realises. Moreover, the data subject has the right to be informed about the processing, to access the data and to correct them. However, it would be difficult to inform individuals that RPAS surveillance is in operation, particularly as RPAS are often silent and may be practically invisible because of their small size or the altitude at which they fly. This makes it difficult to meet transparency and consent obligations, and consequently to meet data access obligations, if individuals are unaware that RPAS surveillance is occurring. The proposed General Data Protection Regulation (proposed GDPR), introduced in January 2012<sup>17</sup>, reiterates that data processing needs to be legitimate and proportionate (data minimisation), and strengthens the individual rights to be informed, access and correct one's data, and to object to their processing. Consequently, the proposed GDPR adds to the importance of finding ways to fulfil the requirements posed by the EU data protection legislation. The report provides more detail about the processing of personal information in relation to aerial photography and other applications, and it examines how the use of other payloads (e.g., thermal imaging, biometrics, etc.) might be impacted by data processors' obligations under the Data Protection Directive and the proposed GDPR.

In addition to these legislative mechanisms focused on privacy and data protection in Europe, national-level legislation related to privacy and data protection might also be applicable to RPAS usage. All European countries are required to abide by the Charter of Fundamental Rights of the European Union, and they are required to transpose the Data Protection Directive into appropriate national legislation. However, privacy laws may be weaker or stronger in some countries, and the transposition of the Directive into national laws has introduced some significant differences in the data protection regimes in different countries. Furthermore, some countries, such as France, have CCTV legislation that is applicable to the

---

<sup>16</sup> Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 June 2007.

<sup>17</sup> 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.

use of RPAS, while other countries (e.g., the UK) have laws covering police surveillance operations.

Finally, large-scale civil RPAS deployment introduces ethical or societal concerns including issues of safety, discrimination, function creep and anticipatory conformity. Safety is a primary consideration for individuals commenting on the possibility of large-scale deployments of RPAS, particularly as Bolkcom reports that the current accident rate for UAVs is 100 times that of manned aircraft.<sup>18</sup> This is because RPAS are often less-well maintained, and consequently less reliable, than traditional aircraft<sup>19</sup> and more subject to pilot error<sup>20</sup>, both of which increase risks to commercial aircraft and civilians on the ground.<sup>21</sup> Current civil deployments of RPAS often focus on persons and groups who are already marginalised in society, thus introducing risks associated with discrimination.<sup>22</sup> Civil uses of RPAS introduce issues associated with mission creep, whereby information collected for one purpose (e.g., traffic monitoring) is used for another purpose (e.g., detecting road tax evaders or dangerous driving). Other ethical impacts include the potential dehumanisation of the surveilled, where the distance between the controller of the RPAS and the surveilled diminishes the sense of moral responsibility for the actions of the RPAS (i.e., “gamification of reality”).<sup>23</sup> Additionally, conventional surveillance aircraft, such as helicopters, provide auditory notice that they are approaching and allow a person “to take measures to keep private those activities that they do not wish to expose to public view”.<sup>24</sup> In contrast, RPAS, and especially small RPAS, offer no such warning. This could lead to a self-governing or “chilling” effect, where individuals believe they are being watched, even when no RPAS are in operation.<sup>25</sup> Finally, function creep refers to the possibility that a system originally acquired for one purpose, is expanded to fulfil additional purposes, where, for example, RPAS originally used to inspect infrastructure at a chemical plant ends up being used to film workers. Each of these ethical issues could lead to public discomfort with the use of RPAS, which would need to be overcome in order to allow innovation and economic opportunities in this area.

This report will discuss each of these issues in detail. Given this framework above, this report uses the following schema in relation to privacy, data protection and ethical issues:

### ***Privacy***

- Chilling effect
- Dehumanisation of the surveilled
- Transparency and visibility, accountability and voyeurism

---

<sup>18</sup> Bolkcom, Christopher, *Homeland security: unmanned aerial vehicles and border surveillance*, Congressional Research Service report for Congress, 28 June, 2004.

<sup>19</sup> Dunlap, Travis, “Comment: We’ve Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search”, *South Texas Law Review*, Vol. 51, No. 1, Fall 2009, pp. 173- 204.

<sup>20</sup> *The Economist*, “Unmanned aircraft: The fly’s a spy”, 1 November 2007.  
[http://www.economist.com/displaystory.cfm?story\\_id=10059596](http://www.economist.com/displaystory.cfm?story_id=10059596)

<sup>21</sup> Electronic Privacy Information Center, *Unmanned Planes Offer New Opportunities for Clandestine Government Tracking, Spotlight on Surveillance*, August 2005.  
<http://epic.org/privacy/surveillance/spotlight/0805/>

<sup>22</sup> Finn and Wright, op. cit., 2012

<sup>23</sup> Wall, Tyler, and Torin Monahan, “Surveillance and violence from afar: The politics of drones and liminal security-scapes”, *Theoretical Criminology*, Vol. 15, No. 3, 2011, pp. 239-254.

<sup>24</sup> McBride, op. cit., 2009, p. 659.

<sup>25</sup> Foucault, Michel, *Discipline and Punish: The Birth of the Prison*, Vintage, New York, 1977.

- Function creep
- Bodily privacy
- Privacy of location and space
- Privacy of association

#### ***Data protection***

- Transparency
- Data minimisation
- Proportionality
- Purpose limitation
- Consent
- Accountability
- Data security
- Rights of access
- Rights of correction
- Third country transfers
- Rights of erasure

#### ***Ethical issues***

- Safety
- Public dissatisfaction
- Discrimination
- Illegal intrusions into wildlife

Given the framework above, the report will also describe the legislative instruments relevant to the use of RPAS in Europe, as well as in a select set of European and non-European countries. Thus, it will identify for RPAS operators the privacy, data protection and ethical issues they should consider, and the specific legal instruments with which they must comply.

The introduction of new and harmonised European regulations is important to harness the benefits of RPAS, whilst protecting citizens' fundamental rights and meeting ethical obligations. However, Finn and Wright have argued that "current regulatory mechanisms do not adequately address privacy and civil liberties concerns because UASs are complex, multimodal surveillance systems that integrate a range of technologies and capabilities".<sup>26</sup> Given this complexity, a range of regulatory instruments might be necessary to attend to the potential benefits and challenges of civil RPAS deployment across Europe. Regulation might happen either on the level of EU and/or national regulatory instruments or by creating guidelines, especially with regard to soft regulatory mechanisms, such as privacy by design, privacy impact assessments and surveillance impact assessments.

Some Member State and third-country national legislation might also point to effective ways in which to regulate the civil deployment of RPAS. For example, the UK Civil Aviation Authority, which regulates the use of RPAS in UK airspace, has explicitly advised that:

---

<sup>26</sup> Finn and Wright, op. cit., 2012, p. 185.

*Aircraft operators and pilots should be aware that the collection of images of identifiable individuals (even inadvertently) when using surveillance cameras mounted on a Small Unmanned Surveillance Aircraft may be subject to the Data Protection Act.<sup>27</sup>*

They warn operators that they must comply with data protection legislation and point them to the Information Commissioner's Office, the UK national data protection authority, for more information. This system indicates one method through which the concerns and jurisdictions of the national DPA and CAA have been interlinked. Another example is the German Civil Aviation Act and the Regulation on Aviation which stipulate that authorisation to use RPAS is dependent on the operator's assurance that the operation will not violate fundamental rights.<sup>28</sup> Beyond Europe, the US has introduced several measures that would restrict the use of RPAS to law enforcement authorities who obtain a warrant or those who file a "data collection statement" indicating how the drone would be used and how the operator would minimise the collection of personal information.<sup>29</sup>

The purpose of this project is to support the development of harmonised and robust policies for the civil use of Remotely Piloted Aircraft Systems (RPAS) that address existing and potential privacy, data protection and ethical concerns. This report will identify the capabilities and applications associated with RPAS and present a series of typical RPAS scenarios and associated risks to privacy, data protection and ethics. The report also presents the findings of a series of consultations with four different types of stakeholders associated with civil RPAS – industry representatives, Data Protection Authorities (DPAs), civil society organisations (CSOs) and Civil Aviation Authorities (CAAs). These consultations took the form of surveys as well as consultation exercises such as panels and workshops. The consultations reveal the urgency of taking policy action in this area. They demonstrate that experts such as DPAs and CSOs report that there are significant risks associated with current RPAS capabilities and applications, which are largely unrecognised by RPAS industry representatives. Therefore, more education is needed on all sides of the sector about the actual uses of RPAS, the potential privacy and data protection issues raised and ways of addressing these issues. As such, the report also provides a privacy and data protection impact matrix for the civil use of RPAS that maps privacy, data protection and ethical risks onto RPAS scenarios. This will serve as an educational instrument for many RPAS stakeholders to bring these differing perspectives into better alignment.

This report finds that the current European and Member State regulatory frameworks are adequate to address the privacy, data protection and ethical impacts of RPAS. This is because both the Data Protection Directive and the GDPR contain specific, technology neutral principles to which that anyone who collects, processes or controls personal data must adhere (unless the data is collected by a natural person and processed for household or personal use). Additionally, each EU Member State has translated the DPD into their own national legislation that maintains the principles outlined in the DPD. As such, these regulatory frameworks are also adequate. However, the report also finds that there is a significant gap in the awareness of RPAS manufacturers and operators with respect to their obligations and that

---

<sup>27</sup> Civil Aviation Authority, "Unmanned Aircraft and Aircraft Systems", no date.  
<http://www.caa.co.uk/default.aspx?CATID=1995>

<sup>28</sup> Voisin, Gabriel, "Drones: Privacy implications across the EU", Bird & Bird, 15 July 2013.  
<http://www.twobirds.com/en/news/articles/2013/global/drones-privacy-implications-across-the-eu>

<sup>29</sup> Thompson, Richard M., "Drones in Domestic Surveillance Operations", *Congressional Research Service*, 3 April 2013, p. 1.

there is a lack of enforcement of these obligations. We argue that the proposed amendments contained in the GDPR, particularly requirements to conduct a Data Protection Impact Assessment and to include privacy-by-design features in all data collection and processing activities should contribute to reducing these gaps and encouraging more responsible RPAS practice. We specifically argue against introducing RPAS-specific legislation, as such legislation will likely not adequately address the varied, dynamic and exponential technologies and data practices that can be linked with RPA platforms.

We conclude that a combination of existing regulatory instruments and soft law measures such as Privacy Impact Assessments (PIAs) elements will assist RPAS operators in developing innovation applications and services by combining harmonised regulations across Europe with a tailored impact assessment. In particular, the project has resulted in a series of policy recommendations, in consultation with a range of relevant RPAS stakeholders (e.g., Data Protection Authorities, Civil Aviation Authorities, RPAS operators and civil society organisations, etc.), to support European innovation whilst protecting privacy, personal data and ethical safeguards. These policy recommendations are separated by different types of stakeholders, and are focused on five key bullet points:

- Industry-specific recommendations for reducing risk
- Raising awareness of privacy and data protection requirements in the RPAS industry
- Enacting information and transparency protocols
- Conducting mandatory assessments of privacy and data protection issues for each type of operation (privacy impact assessments)
- Identifying stakeholders to monitor good practice in privacy and data protection.

Each stakeholder group has a role to play in assisting the RPAS industry in meeting obligations around privacy, data protection and ethics. The policy recommendations focus on actions or steps these individual policy members can take. Each of these policy recommendations, and their specific sub-recommendations, represents improved practice in meeting privacy and data protection requirements. Taken together, these measures provide a comprehensive, good-practice package that encourages responsible use of RPAS in civil applications.

## 2 METHODOLOGY

In order to provide an overview of RPAS capabilities and applications, the privacy, data protection and ethical issues associated with RPAS and the regulatory environment currently applicable to RPAS, this report uses a combination of desk research and consultation exercises with a range of stakeholder groups. The desk research tasks include an examination of RPAS capabilities and applications, the European laws relevant to RPAS, a select set of Member State laws relevant to RPAS and third country laws relevant to RPAS. These reviews used academic journal articles, research reports and other grey material, policy documents, industry publications and media materials to examine these issues in depth. With specific reference to the national contexts examined, partners have selected a sub-set of countries within and outside Europe upon which to focus. The countries that were selected - the UK, France, Germany, Belgium, Luxembourg and Italy in Europe and Switzerland and the USA outside of Europe – conform to countries that either have prepared or are preparing regulations for the use of RPAS in civil air space. Therefore, the purpose of these selections is to provide information for RPAS users in contexts that would be useful for them, as well as to use the country reports as data to identify and analyse good practice in addressing privacy and data protection issues whilst enabling the use of RPAS for civil applications.

The consultation exercises provide supplementary material to these discussions. These consultation exercises included two types of consultations – face-to-face consultations and an on-line survey consultation. These consultations gathered information about how different stakeholder categories understand the risks associated with privacy, data protection, ethics and the civil use of RPAS. Both the face-to-face and survey consultation exercises targeted four stakeholder groups with varying levels of success: RPAS industry representatives, Data Protection Authorities, civil society organisations and Civil Aviation Authorities. The face-to-face consultations included a panel discussion with civil society organisations during an event called “Privacy Camp” that is organised in conjunction with the annual *Computers, Privacy and Data Protection Conference* in Brussels and two separate workshops. The first workshop was an event organised by DG Enterprise that included representatives from the Data Protection Authorities of 18 of the 28 European Member States and the European Data Protection Supervisor. The second workshop was a project-organised event that included speakers and representatives from industry, civil society organisations, Data Protection Authorities and policy-makers.

In relation to the survey, partners utilised the following methodology. The questionnaire was distributed to all four categories of stakeholder through specific and pertinent channels. First, the consortium relied upon a series of contact lists already in partners’ possession as a result of work in other projects. These lists were expanded and developed in relation to each of the four stakeholder categories. The consortium followed a specific method for identifying additional stakeholders. First the consortium relied upon existing organisations, such as industry associations and the Article 29 Working Party to build contacts. Where the consortium had existing direct contacts with these authorities, these contacts were telephoned in order to ensure that the consortium contacted the most relevant person(s) of the organisation. Where the consortium lacked directly named contacts, organisations were also contacted to identify the relevant persons.

In order to complete the survey, the consortium began the process by sending each individual on the contact list a targeted e-mail advising him or her that the questionnaire will be following shortly. The consortium used SurveyMonkey to draft and host the questionnaires,

and once the survey was ready the consortium circulated a link to the survey via e-mail. A second e-mail reminder followed this after one week and a third after two weeks. This strategy is known to increase survey response rates as outlined in the survey research literature.<sup>30</sup> As a result of these tasks, the consortium is confident that it reached as many English-speaking representatives of these specific stakeholder categories as would be interested in filling out the survey.

While some of the questions were common to all stakeholder groups, as described above, the survey also examined different issues in relation to different stakeholder categories. For example, the survey for industry representatives examined the current and future capabilities and applications of RPAS, by asking industry about the devices they design, manufacture and operate as well as their customers (e.g., law enforcement, commercial, etc.). It also examined the extent to which industry representatives felt that these current and future applications raised privacy and data protection issues, and what, if any, activities they have undertaken to address these issues. The DPA questionnaire capitalised on DPAs legal expertise to enquire what legal frameworks related to privacy, data protection or RPAS-related issues (i.e., CCTV, communications surveillance) were relevant to RPAS. Both the DPA survey and the CSO survey also examined what specific aspects of privacy, data protection and ethics might be impacted by visual surveillance by RPAS (the most common application) as well as future RPAS capabilities. Finally, the CAA questionnaire examined the current regulatory framework of RPAS, CAAs' knowledge of privacy and data protection legislation and how well they felt that they were positioned to examine privacy and data protection issues alongside their other responsibilities.

Due to the relative novelty of using RPAS for civil applications, these consultations are exploratory in nature. Both the face-to-face consultations and the survey consultation occurred with a non-representative set of self-selected individuals. Despite this lack of representativeness, the consultation exercises provided significant insight into the approaches of these different stakeholder categories and their understandings of the inter-relationships between privacy, data protection and ethics.

---

<sup>30</sup> See, for example, Aldridge, Alan, and Jen Levine, *Surveying the social world: principles and practice in survey research*, Open University Press, Buckingham, 2001; De Vaus, David, *Surveys in Social Research*, Allen and Unwin, London, 1990 and Hoinville, Gerard, and Roger Jowell, *Survey Research Practice*, Heinemann, London, 1978.

## **3 PRIVACY, DATA PROTECTION AND ETHICAL CONCERNS RELATED TO RPAS TECHNOLOGY**

### **3.1 Introduction and overview**

The last few years have demonstrated the potential advantages of RPAS technology for civil applications by governmental authorities (such as law enforcement agencies), commercial operators (enterprises offering RPAS services), corporate operators (enterprises using RPAS internally for their own needs, either a big company like SNCF or the self-employed like a farmer) and individuals<sup>1</sup>, as well as a potential for economic growth within the European market<sup>2</sup>. However, existing and potential RPAS capabilities and applications raise a number of privacy, data protection and ethical issues. In relation to privacy, evidence from projects involving the development and deployment of RPAS suggests that privacy and data protection issues are superseded by a focus on the technical capabilities of RPAS and questions of safety. Thus, primary concerns relating to the civil use of RPAS include questions pertaining to the kind of technical specifications that are required to avoid collisions in civilian airspace, how regulators ought deal with the influx of inexperienced remote pilots, and what technical requirements should be fulfilled before a national civil aviation association certifies a RPAS.

Nonetheless, the European Commission, which supports the emergence of the RPAS sector, remains aware of the privacy, data protection and ethical challenges that the integration of RPAS in Europe is likely to generate. As aviation safety, data protection and privacy all fall under the jurisdiction of the European Commission, the Commission has published the following three publications in this area: a Staff Working document; a Roadmap; and a Communication identifying the actions that should be taken in the areas of regulation, research and the societal impact of RPAS. Under this last expression “societal impact”, the Commission refers to the privacy, data protection and ethical challenges raised in the context of the RPAS technology. These societal issues raised by the existing RPAS capabilities require identification and attention. Additionally, novel and emerging RPAS capabilities as well as the decreasing size and weight of RPAS might introduce new privacy, data protection and ethical issues.

This chapter is devoted to the identification and study of the impacts that the existing and potential RPAS in civil (commercial/corporate, governmental, private, journalistic) applications may have upon societal concerns, particularly privacy, data protection and ethical issues. This chapter is, therefore, divided into three sections: Section 2 will address privacy issues, Section 3 will examine data protection issues, and Section 4 will focus on ethical issues.

---

<sup>1</sup> Volovesky, Uri, “Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study”, *Law & Security Review*, Vol. 30, 2014, p. 306.

<sup>2</sup> European Steering Group, “Roadmap for the integration of civil RPAS into the European Aviation System”, European Commission, Brussels, 20.06.2013.

## 3.2 Privacy issues associated with RPAS

As discussed in Chapter 1, civil RPAS serve in rescue missions, in the performance of crop dusting, and in delivering humanitarian aid. However, they are and will likely continue to be used by law enforcement agencies, commercial organisations and civilians around the world for more controversial objectives, such as “illegal” immigration, covert surveillance, sensationalist journalism and voyeurism “with all the civil and human rights implications than those missions entail”.<sup>3</sup> Privacy concerns not only relate to the RPAS as an aircraft, but also to the payload or software with which the drone is fitted (e.g. CCTV, thermal cameras, GPS, Automated Number Plate Recognition). The level of impact of this new technology on individual privacy is complex as it comprises several factors. The degree of impact depends on the purpose for which drones are used, as well as the extent and type of personal information that RPAS may capture, the type of operator, the context and location of the RPAS, as well as the type of technology equipment they carry. For instance, privacy concerns related to the use of a RPAS equipped with a facial recognition sensor in the context of a crime investigation are not the same as those occurring when a RPAS fitted with a CCTV camera is used to monitor pipelines.

Despite these recognised difficulties, this Section will identify the main existing and potential privacy concerns which result from the different capabilities of RPAS. After a brief description on the concept of privacy we will examine the ways in which the capabilities of RPAS may impact the nature of “surveillance” moving forwards. This includes the use of RPAS for aerial photography by commercial and corporate operators not interested in the activities of individuals. Further, we will identify the privacy issues specific to RPAS’ use in observation and surveillance contexts, including aerial photography and visual surveillance (sub-section 3), non-visual surveillance and other information gathering practices that may impact individuals (sub-section 4) and the privacy issues that arise in contexts that do not impact individuals, including professional and recreational uses (sub-section 5).

### 3.2.1 The concept of privacy

The term “privacy” has its origins in the Latin word “*privatus*” which means “separate”. Although there is no universal definition of the concept of privacy, it may be defined as “the presumption that individuals should have an area of autonomous development, interaction and liberty, namely a “private sphere” with or without interaction with others, free from state intervention and from excessive unsolicited intervention by other uninvited individuals”.<sup>4</sup>

This “exoteric concept without precise objectively discernable boundaries”<sup>5</sup>, as defined by Brendan Gogarty and Meredith Hagger, embraces different components, although this categorization has long been contentious among scholars. Traditionally, the legal doctrine identified four dimensions of privacy: bodily privacy, information privacy, privacy of

---

<sup>3</sup> Nevins, Joseph, “Drones at home, Robocop”, *Boston Review*, January/February 2011, pp. 32-37; Stanley, Jay, and Catherine, Crump, *Protecting Privacy From Aerial Surveillance, Recommendations for Government Use of Drone Aircraft*, ACLU, 2011, p. 11.

<sup>4</sup> La Rue, Frank, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40, 17 April 2013, pp 6-7.

<sup>5</sup> Gogarty, Brendan, and Meredith, Hagger, “The Laws of Man Over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air”, *Journal of Law, Information and Science*, Vol. 19, 2008, p. 73.

communication and location privacy. Recently, Finn, Wright and Friedewald have argued for an expansion to seven types of privacy by taking into account emerging technologies. In their view, privacy encompasses the following aspects:

- Privacy of the person: refers to the right to keep bodily functions and body characteristics private and to protect against body searches like DNA test;
- Privacy of behaviour: is the ability of the individual to behave in public, semi-public or one's private space without undue observation and interference by others;
- Privacy of personal communication: relates to the protection of emails, telephone communications, SMS, and any other form of communication;
- Privacy of data and image: also known as data protection, encompasses the type of information which is protected by the right to the protection of personal data;
- Privacy of thoughts and feelings: relates to the freedom of individuals to keep their thoughts or feelings private;
- Privacy of location and space: encompasses the right of individuals to move in their "home" and other public or semi-public places without being identified, tracked or monitored;
- Privacy of association, including group privacy: concerns freedom of people to associate with others.<sup>6</sup>

The notion of "privacy" is protected by laws that afford protection under "the right to privacy" or "the right to private life". The first appearance of the right to a private life in the legal doctrine is generally attributed to the lawyers Samuel Brandeis and Louis Warren who defined it as being "*the right to be let alone*".<sup>7</sup> However, the concept of privacy has constantly evolved according to different factors of social, legal and scientific nature.<sup>8</sup> Whereas the right to private life in relation to the RPAS technology is analysed later in this contribution, it is noteworthy that the right to private life is recognised as a fundamental right and enshrined in many international conventions, European texts, and domestic laws. On an international level, the right to private life is dealt with by Article 17 and 23 of the International Covenant on Civil and Political Rights (ICCPR).<sup>9</sup> At the European level, the right to private life is consecrated in the texts of two distinct European organisations, the European Convention of Human Rights (Article 8)<sup>10</sup> of the Council of Europe, and the

---

<sup>6</sup> Finn, Rachel L., David Wright, and Michael Friedewald, "Seven types of Privacy", in Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (Eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, pp. 4-5.

<sup>7</sup> Brandeis, Louis, and Samuel Warren, "The Right to Privacy", *Harvard Law Review*, Vol. 4, No. 5, 1890, pp. 193-220.

<sup>8</sup> Docquir, Benjamin, *Le droit de la vie privée*, Larcier, Bruxelles, 2008, p. 28.

<sup>9</sup> **Article 17:** 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.

**Article 23:** 1. The family is the natural and fundamental group unit of society and is entitled to protection by society and the State. 2. The right of men and women of marriageable age to marry and to found a family shall be recognized. 3. No marriage shall be entered into without the free and full consent of the intending spouses. 4. States Parties to the present Covenant shall take appropriate steps to ensure equality of rights and responsibilities of spouses as to marriage, during marriage and at its dissolution. In the case of dissolution, provision shall be made for the necessary protection of any children.

<sup>10</sup> **Article 8:** 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

European Charter of fundamental rights (Article 7)<sup>11</sup> of the European Union. The European Court of Human rights, competent to condemn States which violate the Convention, has developed comprehensive jurisprudence regarding the interpretation of Article 8 of the European Convention of Human Rights. An in-depth study of the right to private life in line with the European and domestic legal framework will be the subject of the latter chapters of this deliverable. This discussion examines the privacy issues that may arise when drones are used in surveillance and non-surveillance contexts. The following discussion includes “aerial photography” in its definition of surveillance, given the potential to capture images of members of the public in some RPAS contexts and applications.

### 3.2.2 RPAS in observation and surveillance activities

This section discusses two main questions that require consideration when discussing surveillance operated by RPAS operators in a civilian context. First, we explain the origin of the RPAS as a surveillance tool and the actors associated with this surveillance operated by drones. Secondly, we attempt to answer the following crucial question: “Will RPAS bring a new dimension to the nature of surveillance or prove to be just another tool?” When answering this question, we examine the different features of drones that could be transformative in terms of surveillance as we compare them to the traditional surveillance devices (CCTV systems and helicopters).

#### ***Who is carrying out surveillance?***

Although drones have primarily developed in the context of military operations, non-military RPAS are increasingly used in the civil sphere through policing and security measures. The first civil uses of RPAS were for global security activities that represent the civil variation of their military observation and intelligence missions.<sup>12</sup> Therefore, the first non-military uses of RPAS were undertaken by governmental authorities, particularly police and intelligence agencies (to investigate on marijuana cultivation, to monitor protests and gatherings on public places, to control borders against illegal immigration and for investigation and prosecution of crimes). Today, police surveillances drones are already operating in Europe, U.S. and India.<sup>13</sup> For example, in the Netherlands, police have stated “drones have been used about a hundred times for law enforcement purposes in 2012”.<sup>14</sup> In April 2014, this use became official when the Dutch Parliament enacted a law allowing law enforcement authorities to use drones for video surveillance of the country's citizens.<sup>15</sup> There has also been speculation that surveillance drones outfitted with thermal imaging were deployed during the Olympics Games of London 2012 and Sochi 2014 to ensure the smooth conduct of the games.

---

<sup>11</sup> **Article 7:** *Everyone has the right to respect for his or her private and family life, home and communications.*

<sup>12</sup> Geffray, Edouard, “Drones, Innovations, vie Privée et Liberté Individuelles”, *La lettre innovation et prospective de la CNIL*, No. 6, 2013.  
[http://www.cnil.fr/fileadmin/documents/La\\_CNIL/publications/DEIP/LettreIP6.pdf](http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/LettreIP6.pdf).

<sup>13</sup> Gutwirth, Serge, Raphael Gellert, Rocco Bellanova, Michael Friedewald, Philip Schutz, David Wright, Emilio Mordini and Silvia Venier, *Legal, Social, Economic and Ethical Conceptualisations of Privacy and Data Protection (Deliverable 1- project)*, European Commission, Brussels, 2012, p.88.

<sup>14</sup> Schermer, Bart, “An Eye in the Sky: Privacy Aspects of Drones”, *Leiden Law Blog*, 2013.  
<http://leidenlawblog.nl/articles/an-eye-in-the-sky-privacy-aspects-of-drones>

<sup>15</sup> Gijzemijter, Martin, “Dutch Authorities Now Allowed to Film Citizens Using Drones”, 2014.  
<http://www.zdnet.com/dutch-authorities-now-allowed-to-film-citizens-using-drones-7000028019/>

Turning away from the public sector, we observe that the business sector, including companies, corporate actors and professionals, such as journalists, are increasingly becoming “users of surveillance” for commercial benefits or purposes connected to governmental outsourcing. For example, drones may be used to monitor a competitor for corporate espionage, or in the observation of celebrities for sensationalist press articles. Citizens also seem interested in the monitoring capabilities of drones (such as to protect their own property), and it is likely that a number of these recreational activities are ethically questionable. While the use of RPAS by governmental authorities is a focus of the relevant privacy literature, it is the anticipated RPAS use by private sector and citizens that will likely pose the greatest threat to privacy, especially as the use of surveillance and observation by sectors of society are less either not even regulated.<sup>16</sup>

### ***Do RPAS change the nature of surveillance?***

When compared to other forms of surveillance, some policy makers and law enforcement authorities would say that RPAS are “just another tool in the toolbox”<sup>17</sup>, “technologically neutral”<sup>18</sup> and that they are not different from a range of traditional surveillance systems, such as aerial surveillance led by helicopters or visual surveillance operated through CCTV systems<sup>19</sup>.

This common argument that RPAS technology does not contribute anything new in terms of surveillance does not address the current complexity of RPAS systems. Compared to *CCTV systems*, a RPAS comprises the unique ability to be equipped with a variety of advanced sensors, to process different types of images and information and to undertake different types of surveillance (i.e., physical surveillance, surveillance of communications, dataveillance, tracking, body surveillance). Mounted with these sense-enhancing technologies which “greatly magnify the human capacity to observe”<sup>20</sup>, drones can not only capture footages which reveal “far more than the naked eye”<sup>21</sup> but also recognise faces, intercept electronic communications or even detect “abnormal behaviours” and identify human targets<sup>22</sup>. Moreover, while CCTV systems are fixed, transparent and confined to public places<sup>23</sup>, RPAS “offer new angles for visual surveillance”<sup>24</sup>, can monitor in locations which do not require an access to the premises and, thus, can be operated in strict secrecy. They also “may be

---

<sup>16</sup> Against this background, the use of “surveillance and monitoring activities” refers to all types of surveillance (physical surveillance, dataveillance, communication surveillance, sousveillance, lateral surveillance, aerial surveillance)<sup>16</sup> operated by all types of actors (law enforcement authorities, journalists, corporations and individuals such as neighbour, voyeur, stalker, citizen-paparazzi).

<sup>17</sup> Cited in Nevins, Joseph, “Drones at Home, Robocop”, *Boston Review*, January/February 2011, pp. 32-37.

<sup>18</sup> Nevins, op. cit., 2011.

<sup>19</sup> Finn, Rachel L., and David Wright, “Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications”, *Computer Law & Security Review*, Volume 28, Issue 2, April 2012, pp. 184–194.

<sup>20</sup> Calo Ryan, M., “Robots and Privacy”, in Patrick Lin et al. (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics*, MIT Press, Cambridge, 2012, pp. 187-202.

<sup>21</sup> Stanley and Crump, op. cit., 2011.

<sup>22</sup> Electronic Privacy Information Center (EPIC), *Comments of the EPIC to the FAA on Unmanned Aircraft System Test Site Program*, Docket No. FAA—2013—0061, 2013, p. 3.

<sup>23</sup> Finn, Rachel L., and David Wright, “Privacy and data protection issues related to use of civil RPAS”, European Data Protection Authorities meeting, European Commission, Brussels, 28 February 2014.

<sup>24</sup> Wright, David, “Drones: Regulatory challenges to an incipient industry”, *Computer & Law Security Review*, Vol. 30, 2014, p. 227.

deployed without any delay”<sup>25</sup> “to observe and follow individuals, something that is very difficult, if not impossible, when using fixed CCTV systems”<sup>26</sup>.

Besides the numerous “new surveillance technologic payloads” with which it can be endowed, the RPAS in itself has new surveillance potentials that manned aircraft like helicopters would not be able to provide. Unlike *police helicopters* that have “clear auditory signal and are relatively recognizable and identifiable”.<sup>27</sup> One author observes “it is difficult to put visible police decals on a Raven for instance. So a drone may be used by the police, intelligence agencies, or even private entities, resulting in much uncertainty for those observed”<sup>28</sup>.

In addition to the aforementioned characteristics that make a RPAS a unique tool for covert surveillance,<sup>29</sup> we can also expect a change in the duration and breadth of the observation. If surveillance is characterised by its sporadic nature and is limited to specific zones for now, solar-power RPAS will soon be able to “stay in the air forever”.<sup>30</sup> Therefore, as noted by John Villanesor:

*[T]oday, no government body is actively and publicly promoting a plan to establish a permanent high-altitude surveillance drone presence above American cities. But because it will soon be inexpensive and easy to do so, and because the information gathered will be considered as useful and valuable, it will inevitably happen by the end of the decade.*<sup>31</sup>

In addition to threat of being constantly monitored, the advanced technology of the sensors will allow to cover very wide zones. For example, a technical adviser for Air Force intelligence, surveillance and reconnaissance capabilities suggests that there are plans within America to use MQ-9 Reapers with sensors able to “film an area with a four-kilometre radius underneath the Reaper during both day and night operations from 12 angles... even if a vehicle drives out of the view of the full-motion video sensor, it will still be within Gorgon Stare’s range (the name of the program). Even if 12 squinters run in 12 directions, Gorgon Stare could dedicate one angle to each one”.<sup>32</sup> With regard to the increase in the scale of surveillance due to new technologies, Murakami Wood also notes “the ubiquity of surveillance is not only about how much surveillance occurs, but also the way in which it is becoming less and less obvious as it increases in quantity”.<sup>33</sup>

---

<sup>25</sup> International Working Group on Data Protection in Telecommunications, “Working Paper on Privacy and Aerial Surveillance”, Berlin, 2-3 September 2013, p.5.

<sup>26</sup> Schermer, op. cit., 2013.

<sup>27</sup> Finn and Wright, op. cit., 2014.

<sup>28</sup> Schermer, op. cit., 2013.

<sup>29</sup> Calo Ryan, M., “The Drone as a Privacy Catalyst”, *Stanford Law Review*, Vol. 64, No. 29, December 2011. [http://www.stanfordlawreview.org/sites/default/files/online/articles/64-SLRO-29\\_1.pdf](http://www.stanfordlawreview.org/sites/default/files/online/articles/64-SLRO-29_1.pdf)

<sup>30</sup> Prigg, Mark, “The Silent Spy Drone that Could Stay in the Sky Forever”, *The Daily Mail*, 17 July 2012. <http://www.dailymail.co.uk/sciencetech/article-2174976/The-silent-spy-drone-stay-sky-forever.html>

<sup>31</sup> Villanesor, John, “Observations from above: Unmanned Aircraft Systems and Privacy”, *Harvard Journal of Law & Public Policy*, Vol. 36, No. 2, 2013, pp. 458-517.

<sup>32</sup> DarkGovernment, “Reaper Sensors Called Gorgon Stare”, *DarkGovernment news online* no date. <http://www.darkgovernment.com/news/reaper-sensors-called-gorgon-stare/#sthash.eIqOpPBz.dpuf>

<sup>33</sup> Wood, David Murakami, “Vanishing Surveillance: Why Seeing What is Watching Us Matters”, *Office of the Privacy Commissioner of Canada*, Toronto, 2011.

The foregoing suggests that RPAS are an extremely effective vehicle for anyone seeking to conduct monitoring activities. An article in the *Economist* states, “UAVs can peek much more easily and cheaply than satellites and fixed camera can”.<sup>34</sup> Indeed, becoming increasingly cheaper than any other surveillance systems means that any cost barrier to permanent use of aerial surveillance and on the excessive police presence is going to disappear, and that a shift in the actors of surveillance will appear.<sup>35</sup> Although law enforcement agencies in multiple countries are deploying RPAS, the civil use of drones will be utilised by organisations other than governments and their agencies. Thus, due to the affordability of RPAS and their potential payloads, the RPAS technology tends to reinforce the recent phenomenon of “privatization of surveillance”.<sup>36</sup> Chris Schlag, and Ryan Calo observe that “many privately owned companies already use or have expressed interest in obtaining drones for security, loss prevention” and to “survey property, secure premises or monitor employees”.<sup>37</sup> Moreover, some media agencies, such as *National Geographic*, have acquired drones to collect private information, to follow and photograph celebrity events or “to cover unfolding police activity or traffic stories”.<sup>38</sup> The Electronic Privacy Information Centre has also claimed that Google Inc. has “deployed street-level drones in other countries to supplement the images of Street View”.<sup>39</sup> In addition to commercial organisations, small professional entities such as “private detective agencies, lawyers, bail bondsmen, insurance companies and others have all staked a claim in the development of affordable drone technology”.<sup>40</sup> Finally, even individuals seem attracted to this “lucrative paparazzi industry”.<sup>41</sup> Thus, recreational drones that are marketed with cheap sensors will certainly increase lateral surveillance (individuals-to-individuals surveillance) as well.<sup>42</sup>

On the question of whether drones will change surveillance, this evidence suggests that drones will in fact change the nature of surveillance. ACLU and EPIC have arrived at the same conclusion stating “Drones present a unique threat to privacy. Drones are designed to undertake constant, persistent surveillance to a degree that former methods of surveillance were unable to achieve”<sup>43</sup>, and that “UAVs could actually be “transformative” in the manner in which they conduct surveillance<sup>44</sup>”. Surveillance by states is the most commonly discussed form of surveillance, and it is also the subject of many articles and reports in this area<sup>45</sup>.

---

<sup>34</sup> “Unmanned Aircraft: The Fly’s a Spy”, *The Economist*, 2007.

[http://www.economist.com/displaystory.cfm?story\\_id=10059596](http://www.economist.com/displaystory.cfm?story_id=10059596).

<sup>35</sup> EPIC Org., “Domestic Unmanned Aerial Vehicles (UAVs) and Drones 2013”,

<http://epic.org/privacy/drones/> Also see Courtland, Erin, “Drones in Canada – Will the Proliferation of Domestic Drone Use in Canada Raise New Concerns for Privacy?”, *OPC Research Reports*, March 2013.

<sup>36</sup> EPIC Org., op. cit., 2013.

<sup>37</sup> Schlag, Chris, “The New Privacy Battle: How the Expanding Use of Drones Continues to Erode Our Concept of Privacy and Privacy Rights”, *Pittsburgh Journal of Technology Law and Policy*, Vol. 13, No. 2, 2013, p. 11.

<sup>38</sup> Calo, op. cit., 2012.

<sup>39</sup> EPIC Org., “Domestic Unmanned Aerial Vehicles (UAVs) and Drones 2013”, 2013.

<http://epic.org/privacy/drones/>

<sup>40</sup> Schlag, Chris, op. cit., 2013.

<sup>41</sup> Calo, op. cit., 2011, p. 30.

<sup>42</sup> De Hert, Paul, “Drones: Fair Information Principles to Constitutional Principles? A Right to Bear Arms to Shoot Certain Drones Out of My Air”, *Belgian Unmanned Aircraft System Association Meeting*, BEUAS Brussels, 2013.

<sup>43</sup> EPIC Org., “Domestic Unmanned Aerial Vehicles (UAVs) and Drones 2013”, <http://epic.org/privacy/drones/>

<sup>44</sup> Courtland, Erin, *Drones in Canada – Will the proliferation of domestic drone use in Canada raise new concerns for privacy?*, OPC research reports, March 2013.

<sup>45</sup> Villasenor, John, “Observations from above: Unmanned Aircraft Systems and Privacy”, *Harvard Journal of Law & Public Policy*, Vol. 36, No.2, 2013, pp. 458-517.

Recently, Statewatch issued a report regarding the European Commission involvement in the RPAS technology. In that report, the civil liberties watchdog estimates that the European Commission has budgeted 315 million Euros for the deployment of drones used mainly for surveillance missions by European law enforcement authorities.<sup>46</sup> The way that societies are policed is undergoing transformation, and commercial actors and individuals are also becoming users of the observation and monitoring capabilities of the RPAS technology both in terms of business and leisure pursuits. While state surveillance by drones must continue to be vetted through the imposition of warrants for operation, and other legal restrictions, “neighbour monitoring” and “surveillance marketing” are new forms of surveillance and the scale of this surveillance also requires the attention of policy makers.

### 3.2.3 Privacy concerns related to visual photography and surveillance activities

In this section we take a closer look at visual photography, video streaming and surveillance which is conducted via high resolution cameras, thermal imaging cameras and infrared cameras. This differs from non-visual imaging and surveillance such as surveillance monitored through the means of other sensors (such as microphones, automated number plate recognition, GPS sensors, communication relay systems, facial recognition, etc.). We divided the examination of the privacy impacts of drones between visual and non-visual surveillance because on one hand, the principal payload of most drones is cameras<sup>47</sup>, and, on the other hand, we will see that visual photography and surveillance is typically intrusive and affects many dimensions of privacy<sup>48</sup>.

When RPAS technologies are mounted with visual payloads (high-resolution, thermal imaging or infrared cameras) privacy-related issues arise in relation to the following: function creep, chilling and panoptic effects, dehumanization of the surveilled at the hands of the surveillants, transparency, visibility, accountability and voyeurism.

#### ***Function creep***

Scholars such as Joseph Nevins, Roger Clarke and Erin Courtland have particularly emphasised their fear of “function creep”<sup>49</sup> in the case of RPAS. This occurs when “RPAS are purchased for specific, restricted operational uses but come to be used for more common, controversial reasons”.<sup>50</sup> For instance, when a RPAS is purchased by the police for monitoring crowd gatherings, but it is also used to detect people who have not paid for parking. In the private sector, an example could include a data processing operation that is launched for a specific marketing purpose, but the collected information is later used for other purposes or resold to other data processors, such as insurance companies or public authorities.

---

<sup>46</sup> Hayes, Ben, Chris Jones and Eric Töpfer, *Eurodrones Inc.*, Statewatch/Transnational Institute, Amsterdam, 2014. [http://www.tni.org/sites/www.tni.org/files/download/011453\\_tni\\_eurodrones\\_inc\\_br\\_3e.pdf](http://www.tni.org/sites/www.tni.org/files/download/011453_tni_eurodrones_inc_br_3e.pdf); Waterfield, Bruno, “EU spent £320 million on surveillance drone development”, *Telegraph online*, February 2014. <http://www.telegraph.co.uk/news/worldnews/europe/eu/10632262/EU-spent-320-million-on-surveillance-drone-development.html>

<sup>47</sup> This is due to the affordability and accessibility of visual payloads on the market, for example, Go-pro.

<sup>48</sup> Wright, David, “Drones: Regulatory Challenges To An Incipient Industry”, *Computer & Law Security Review*, Vol. 30, 2014, p. 228.

<sup>49</sup> “Function Creep is what occurs when an item, process, or procedure designed for a specific purpose ends up serving another.”: see [www.functioncreep.blogspot.be](http://www.functioncreep.blogspot.be)

<sup>50</sup> Statewatch, “Commission Wants Drones Flying in European Skies by 2016”, *Statewatch News Online*, September 2012. <http://www.statewatch.org/news/2012/sep/eu-com-drones.htm>

Another associated function creep risk is created when drones' operator powers expand beyond those required to meet the stated aims of a drone's activity.<sup>51</sup> An example of this is when real estate companies that initially use drones for filming houses that they have to sell, decide also to film people, houses, backyards and cars around the neighbourhood to portray the financial standing of residents of an area. In the law enforcement sector, Canadian police use drones for taking aerial pictures and videos of traffic collisions or crime scenes. Imagine that upon analysing the footage, they discover a number of cars on the other side of the road disobeying the speed limit. The high-quality video allows them to read the number plates of the offending cars, and they use the data to issue tickets.<sup>52</sup> Another example of function creep is given by Tom Barry, senior analyst at the Center for International Policy in Washington. He explained that the United States Department of Homeland Security recently purchased some civil RPAS destined to be used by the U.S. Custom and Border Protection to operate as instruments of "border security" but that those same RPAS were rapidly engaged in the "war on drugs".<sup>53</sup>

### ***Chilling and panoptic effect syndrome***

The term "chilling effect" refers to a decrease in the legitimate exercise of civil liberties and rights, such as freedom of assembly or freedom of expression, because individuals are discouraged from participating in social movements or public dissent activities for fear of being surveilled.<sup>54</sup> This "chilling effect" is often observed in situations where people are under generalised covert surveillance, "to protect themselves from the negative effects of intrusions, individuals must assume they are being observed and attempt to adjust their behaviour accordingly".<sup>55</sup> Robyn Dawes, renowned American psychologist, is among a number of psychologists that have reached the same conclusion as that reached by scholars in the area of surveillance, namely that "people who are being observed tend to behave differently, and make different decisions, than if they are not being watched".<sup>56</sup> Studies by scientists at Newcastle University have proven that "merely hanging up posters of staring human eyes is enough to significantly change people's behaviour".<sup>57</sup> In his study of the risks of surveillance on democratic societies, Professor Anthony Giddens refers to the "self-censorship" effect of surveillance from citizens in their speeches, actions and beliefs.<sup>58</sup>

---

<sup>51</sup> Nevins, Joseph, "Drones at Home, Robocop", *Boston Review*, January/February 2011, pp. 32-37; Stanley, Jay, and Catherine, Crump, *Protecting Privacy From Aerial Surveillance, Recommendations for Government Use of Drone Aircraft*, ACLU, 2011, p. 11.

<sup>52</sup> Draganfly Innovations Inc., "Draganflyer X6 UAV RC Helicopter Assists Police at Traffic Accident Scene", 28 December 2009. <http://www.rctoys.com/pr/2009/12/28/draganflyer-x6-uac-rc-helicopter-assists-police-at-traffic-accident-scene/> See also Courtland, op. cit., 2013, p. 6.

<sup>53</sup> Barry, Tom, "Homeland Security Drones Mission Creep from Border Security to National Security", *Borderlines Blog*, March 2013. <http://borderlinesblog.blogspot.be/2013/03/homeland-security-drones-mission-creep.html>

<sup>54</sup> YourDictionary, "Chilling Effect. (n.d.)" <http://law.yourdictionary.com/chilling-effect>

<sup>55</sup> Finn, Rachel L., David Wright and Michael Friedewald, "Seven types of Privacy", in Gutwirth, S., Leenes, R., de Hert, P., Pouillet, Y. (Eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, p. 16.

<sup>56</sup> van der Linden, Sander, "How the Illusion of Being Observed Can Make You a Better Person," *Scientific American*, 2011. <http://www.scientificamerican.com/article.cfm?id=how-the-illusion-of-being-observed-can-make-you-better-person>

<sup>57</sup> Ibid.

<sup>58</sup> Richards, Neil M., cited in Giddens, Anthony, "The Dangers of Surveillance", *Harvard Law Review*, Cambridge, 2013, pp. 19-49.

Philosophers such as Jeremy Bentham and Michel Foucault were already well aware of the idea that people adjust and even correct their own deviant behaviour when they know they are being observed. The work of these two philosophers, working in different contexts, contributed to the formation of panoptic theories of surveillance.<sup>59</sup> This theory explains that for example, designing a prison in a way that prisoners cannot see the guards, one can observe a self-disciplining effect amongst the prisoners who never know whether they are being watched.<sup>60</sup> By being hidden, the watcher increases its power over the watched. This can however, produce positive results such as in the context of disassembling a criminal group. However, it can also lead to great abuses and domineering behaviour by the watcher.

The choice to undertake overt observation with the aim of generating adapted behaviours of people being watched has been criticised. Roger Clarke will soon issue an article about drones' impact on the behavioural privacy<sup>61</sup> in which it emphasises that behavioural privacy is the dimension of privacy that is the most affected by the visual surveillance application of drones.<sup>62</sup> He also insists “the deterrent value in relation to serious forms of misbehaviour is limited” while “the primary deterrent effect that is likely to be achieved is the chilling of lawful social, economic, cultural and political behaviours”.<sup>63</sup> Clarke argues further that “the feeling that ‘they know all about you anyway’ can lead the persons-at-risk to result in hyper-vigilance or even to paranoia”.<sup>64</sup>

As described in Chapter 3, in the near future, CCTV systems and drones equipped with specific cameras will be also able to utilise “smart surveillance” algorithms to detect abnormal behaviours.<sup>65</sup> Once certain behaviours are spotted in a public place, these “smart” systems would then be able to alert the police. So, there is some chance that in addition to the systematic monitoring of behaviours, civilians may be under permanent surveillance. Subsequently, the “chilling effect” as we now understand it, may too become more pronounced.

This is especially so for the case of drones that are undetectable from the ground. In that situation, citizens will have no means of knowing what payload is used, or whether the drone is mounted with a camera or a recognition sensor, and nor will they be capable of detecting who the pilot is and who they represent, i.e. a hobbyist, a marketing company, or a law enforcement agency. Thus, even if commercial and professional uses of RPAS do not carry out visual photography of persons or engage in surveillance, their mere presence and the inability to identify what their purpose and payload may be will contribute to a panoptic effect.

---

<sup>59</sup> Calo, Ryan M., “People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship”, *Penn State Law Review*, Vol. 114, No. 3, 2010, p. 809.

<sup>60</sup> Bentham, Jeremy, “Panopticon”, in Monatgu, Basil, *Opinions of Different Authors Upon the Punishment of Death*, London, 1886; Foucault, Michel, *Discipline and Punish: the Birth of the Prison*, Vintage, New York, 1977.

<sup>61</sup> Behavioural privacy refers to the freedom of the individual to behave as he or she wishes without undue observation or interference from others. Clarke, Roger, “The Regulation of Civilian Drones’ Impacts on Behavioural privacy”, *Computer Law & Security Review*, Vol. 30, No. 3, 2014, p. 1.

<sup>62</sup> Clarke, op. cit., 2014; Wright, op. cit., 2014, p. 228.

<sup>63</sup> Clarke, op. cit., 2014, p.4.

<sup>64</sup> Ibid.

<sup>65</sup> INDECT is the European Commission project studying how to detect “automatically” abnormal and suspicious behaviours from CCTV images, audio or data exchanged on Internet.

### ***Dehumanisation of the surveilled at the hands of the surveillants***

As underlined by Professor Ryan Calo, RPAS “represent the cold, technological embodiment of observation”.<sup>66</sup> Pilots can be kilometres away from their target when they are operating drones in surveillance missions or for direct marketing actions. What this means is that pilots are physical and psychologically removed from the act of observation or information collection. For example, up until now, to operate a corporate espionage mission, some employees of a company had to be engaged by the competitor firm. With the use of drones, a commercial company can easily monitor its competitor firm by flying over the site of its competitor, recording footage through the window. Therefore, being physically and psychologically removed from activities means that some activities, such as corporate espionage, may proliferate with the deployment and the use of drones in civil society.

In keeping with this idea that being physically removed transcribes into a psychological or even moral detachment from the activity, Roger Clarke explains: “the fact that the pilot is remote from its target, this causes a detachment from physical reality [that] weakens the constraints of conscience, and loosens at least some of the psychological and social constraints that apply in metaspace”.<sup>67</sup> For instance, press agencies and police forces may be just as tempted to take footage of a celebrity party as taking footage of a criminal gang meeting with mobile cameras, especially as they no longer have to be physically present to obtain the footage. It is easy to comprehend how the disappearance of the once present logistical barrier of having to be present to photograph will engender legal action following voyeuristic pursuits or legal cases involving nuisance actions against journalists and neighbours. A scenario involving drones that are equipped with cameras to ensure the safety of police officers during an operation also poses the risk that the use of such “safe” methods of surveillance be systematically extended.<sup>68</sup> These concerns are shared by Calo, who illustrates the subtle evolution of dehumanisation created by drone technology:

*Today’s police have to follow hunches, cultivate informants, subpoena ATM camera footage; journalists must ghost about the restaurant or party of the moment. Tomorrow’s police and journalists might sit in an office or vehicle as their metal agents methodically search for interesting behaviour to record and relay.*<sup>69</sup>

All these examples support the premise that RPAS that monitor with little or no human intervention will lead to an increase in the trend of automated law enforcement without a decrease in the risks of bugs or software errors related to automated programs.<sup>70</sup> The dangers of such errors are particularly relevant when the data collected by drones is adduced as evidence before a court.

Finally, the soon-to-be highly accessible drones and camera equipment means that all members of society may proclaim themselves as a surveillant, society protector or even private detective. The effect of this will be an increase in surveillance activities “from everyone on everyone”.

---

<sup>66</sup> Calo, op. cit., 2011.

<sup>67</sup> Clarke, op. cit., 2014.

<sup>68</sup> Clarke, op. cit., 2014.

<sup>69</sup> Calo, M. Ryan, “Robots and Privacy”, in Patrick Lin et al. (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics*, MIT Press, Cambridge, 2012, pp. 187-202.

<sup>70</sup> Clarke, op. cit., 2014, p. 4.

### ***Transparency and visibility, accountability and voyeurism***

Monitoring activities with RPAS is mostly a covert exercise during which drones remain undetected to individuals on the ground, and undertaken on the basis of a single perspective. This context is likely to lead to different abuses, and errors.<sup>71</sup>

Following the revelation of scandals implicating PRISM and other NSA secret programs, there is little trust in the merits of covert governmental surveillance programs. This is also the case in the private sector where trust in the confidentiality and privacy policies of companies like Google have been under criticism.

The drone appears to be the new perfect candidate for blanket surveillance activities because of its capability to be invisible, to capture images, sounds and to intercept phone calls and texts. Aside from increasing covert surveillance, which raises transparency issues that are inherent to this kind of surveillance, RPAS uses in overt surveillance or even for any other activities not related to surveillance, will also raise transparency concerns. The risks are so great that policy makers are currently debating a way to impose a duty on surveillants to inform the public of their activities and thereby, safeguard the transparency requirements of relevant legal frameworks.

The fact that RPAS are usually undetectable, together with the type of subject matter usually under surveillance, raises questions concerning the willingness of those carrying out surveillance to respect their duties to inform the public and to obtain the requisite consent. It also raises questions as to the enforceability of these legal duties.<sup>72</sup> The resultant lack of transparency increases the risks of errors committed by the law enforcement authorities or other operators. Moreover, when electronic or human errors or even abuses occur, it is very difficult for individuals to detect them since much surveillance is conducted from a single perspective and within a limited context.<sup>73</sup> As emphasised by Clarke:

*many cases of mistaken identity arise, fuelling rumours and innuendo. Moreover, images and video recordings, particularly when taken from above the object being observed, and especially when presented by government agencies, are invested with importance that it may or may not merit. In turn, refutation of unjustified accusations is very challenging in the 'court of public opinion' and even in courts of law.*<sup>74</sup>

In addition to transparency, RPAS also raise issues associated with accountability. “In case of infringements to their right to private life, individuals do usually expect to identify a legal or physical entity to be responsible for damages they suffered”.<sup>75</sup> However, as the surveillance will be mostly anonymous and capable of being carried out by anyone with a drone and attachments, the ability to detect those responsible for the surveillance is diminished. The European RPAS Steering Group has accepted that “it is really complex to monitor and control RPAS, [...] through licensing or registration systems that would ensure that they are used in a

---

<sup>71</sup> Clarke, op. cit., 2014.

<sup>72</sup> Belgian Privacy Commission, ‘La Commission vie privée répond aux questions fréquemment posées concernant les drones’. <http://www.privacycommission.be/fr/news/la-commission-vie-priv%C3%A9e-r%C3%A9pond-aux-questions-fr%C3%A9quemment-pos%C3%A9es-concernant-les-drones>

<sup>73</sup> Ibid.

<sup>74</sup> Clarke, op. cit., 2014, p. 4.

<sup>75</sup> European RPAS Steering Group, “Roadmap for safe RPAS integration into European Air System - Annex 3 A study on the societal impact of the integration of civil RPAS into the European Aviation System”, 2013. [http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap-annex-3\\_en.pdf](http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap-annex-3_en.pdf)

lawful and legitimate way”.<sup>76</sup> The accountability problem is compounded by the fact that drones can be operated by automatic software, and/ or that they can be hacked and intercepted in flight.<sup>77</sup> For example, a drone that was hacked whilst it was filming an athletic competition recently injured an athlete.<sup>78</sup> It may be expected that police investigations will remain open, and individuals without compensation if accountability cannot be placed on those responsible for damage caused by surveillance activities. The lack of accountability mechanisms ultimately have a wider effect on democracy: “The inevitable coupling of UAVs,[...] combined with insufficient accountability mechanisms, is a recipe both for the normalization of previously unacceptable levels of policing and for official abuse”<sup>79</sup>.

Furthermore, the use of RPAS by private individuals is likely to disturb privacy as drone operators engage in voyeuristic behaviours and/ or harassment. Clarke explains that the widespread availability of drones means that they “empower pilots and/or operators of on-board facilities to engage in voyeurism, harassment, stalking, and even acts of gratuitous violence”.<sup>80</sup> Compared to other visual technologic means, Clarke emphasises also the fact that RPAS allow to their operators (paparazzi and voyeurs) to engage in surreptitious observation for longer periods<sup>81</sup>. With regard to recreational RPAS, Courtland raises an important point by emphasising that recreational drone pilots do not need a licence to operate<sup>82</sup>. Civil drones, or their technological accompaniments, are not subject to authorisation which means “there is going to be an issue with stalking, harassment, and other crimes using drones by individuals”, as explained by Amie Stepanovich, director of the Domestic Surveillance Project at the Electronic Privacy Information Center. Imagine “a testosterone-packed teenager directing his drone to watch the object of his affection (or lust) sunbathing in the supposed privacy of her backyard”.<sup>83</sup> Whereas some countries put restriction on the use of drones by private for recreational application, private companies such as the French firm Parrot continues to sell its second generation recreational drone, equipped with a front camera able to shoot in 720p HD at 30 frames per second. Since 2010, the Parrot Company has already sold more than one half-million of its first model remotely piloted via a Smartphone and equipped with two cameras.<sup>84</sup> Therefore, some private operators cross the border between permitted and prohibited use.

---

<sup>76</sup> Ibid.

<sup>77</sup> Clarke, op. cit., 2014, p. 4.

<sup>78</sup> Radulova, Lillian, “Woman Athlete Suffers Head Injuries After Hackers Took Control of Drone Filming Race and Made It Crash”, *Mail Online*, 8 April 2014. <http://www.dailymail.co.uk/news/article-2599269/Australian-triathlete-injured-crashing-drone-pilot-loses-control.html#ixzz33lbkaHDq>

<sup>79</sup> European RPAS Steering Group, op. cit., 2013.

<sup>80</sup> In its recommendations to the US government, the American Civil Liberties Union referred to a case involving the following set of facts: “In 2004 a couple making love on a dark night time rooftop balcony, where they had every reason to expect they enjoyed privacy, were filmed for nearly four minutes by a New York police helicopter using night vision. Rather than apologize, NYPD officials flatly denied that this filming constituted an abuse, telling a television reporter: “this is what police in helicopters are supposed to do, check out people to make sure no one is... doing anything illegal”. This raises the question of whether privacy protections for individuals might be necessary when the “voyeur” is able to see the individual in real time, whilst simultaneously downloading that footage to a social network.

<sup>81</sup> Wright, op. cit., 2014, p. 228.

<sup>82</sup> Courtland, op. cit., 2013, p. 7.

<sup>83</sup> Ibid.

<sup>84</sup> Marival, Julien, ‘Interpellé pour avoir fait voler un drone autour de la tour Eiffel’, *Metronews*, Paris, 2014. <http://www.metronews.fr/paris/interpelle-pour-avoir-fait-voler-un-drone-autour-de-la-tour-eiffel/mnbt!piGVaaVzEKSZs/>

Finally, presenting many advantages for news reporting, RPAS has revolutionised the journalistic world but also the paparazzi sector. Consequently, the Reuters Institute for the Study of Journalism has issued a report identifying the journalistic issues and advocating for a specific regulatory framework for the journalism sector.<sup>85</sup> Meanwhile, the US Federal Aviation Administration is currently examining “improper operations of drones by journalists”. One such case under review concerns “an off-duty employee of a local TV station flew a drone over the scene of a car crash, where a victim's body had been left exposed”.<sup>86</sup> Although professionals have ethical rules set up to govern the profession, there is little to deter “citizen journalists, YouTubers with a Phantom quadcopter or the paparazzi”<sup>87</sup> from behaving inappropriately.<sup>88</sup> Matthew Waite, founder of the Drone Journalism Lab, concurred with the importance of establishing a firm distinction between paparazzi photographers and serious journalists when stating:

*Put drones in the hands of the paparazzi and I agree with most people's discomfort. But put a drone in the hands of a serious journalist and I'll argue that you have an ideal early adopter of the technology, one that can help guide society into a post-drone world, where flying robots large and small become vastly more commonplace... I'm not claiming that codes of ethics are all perfect or deal with drones specifically. My point is that they exist. And many of them would easily apply to drones without much creativity. And there is broad agreement that professional journalism is ethical journalism.*<sup>89</sup>

This section demonstrates that even though commercial RPAS operators and operations may not specifically engage in visual surveillance of people, they are implicated in a wider trajectory that raises significant privacy issues. Furthermore, the inability of individuals to directly identify who is operating the RPAS in question, the payload(s) with which it is equipped and the purpose for which it is being used contributes to a generalised privacy impact, whereby individuals are pushed to behave as though they are being observed since they are not able to identify whether observation is taking place. In Germany, specifically, this impact of surveillance has been identified and legislated against<sup>90</sup>, making RPAS operators potentially legally implicated in the use of technology that has broad potential privacy impacts.

---

<sup>85</sup> Goldberg, David, Mark Corcoran and Robert, G. Picard, “Report - Remotely Piloted Aircraft Systems & Journalism Opportunities and Challenges of Drones in News Gathering”, *Reuters Institute for the Study of Journalism*, 2013.

<sup>86</sup> Collins, Katie, “Police, Paps and Privacy: The Challenges of Drone Journalism”, *Wired online*, February 2014. <http://www.wired.co.uk/news/archive/2014-02/12/drone-journalism-legal-and-privacy>

<sup>87</sup> Ibid.

<sup>88</sup> Relevantly, if the European Union retains the competence to establish rules governing professional use of RPAS for journalists, then Member States must establish rules governing private uses. In this regard, we can expect that strict regulations on professional use of RPAs would provide a clear signal about what is acceptable use, and it would provide a model for states to set their own regulations.

<sup>89</sup> Waite, Matthew, “Journalists: Good Early Drone Adopters”, *Aljazeera online*, 11 December 2013. <http://m.aljazeera.com/story/20131123125221676178>

<sup>90</sup> Jóri, A, “Data protection law – An Introduction”, *dataprotection.eu*, 6 April 2007. <http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.SecondGeneration>

### 3.2.4 Privacy concerns related to non-visual surveillance activities

Today, in addition to visual payloads, RPAS can also be fitted with GPS devices, microphones and recognition software such as automated license plate readers. Tomorrow's drone sensors technologies will multiply. Chapter 3 finds that facial recognition, "soft" biometric, biological and chemical sensors and lethal and non-lethal weapons are already on the list of the technologies that the next drones-generation will carry. In addition to scientific research on sensors, engineers are also developing RPAS that are less visible thanks to nano and biomimetic innovations.<sup>91</sup> While non-visual payloads raise some of the same privacy issues (function creep, accountability and transparency) as visual payloads, they also raise additional threats that require examination. In this section, we, therefore, discuss concerns about the right to life, lack of respect for the bodily integrity, privacy location and space, and association privacy.

#### **Concerns about bodily privacy**

Amongst the non-visual payloads that can be mounted on RPAS, biometric (facial recognition, fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent) and "behaviometric"<sup>92</sup> sensors are the most likely to damage the right to privacy. The privacy of the person, and especially bodily privacy<sup>93</sup>, will certainly be affected by RPAS which facilitate "the use of biometric data [for] verification and identification of individuals"<sup>94</sup> on the basis of facial patterns, fingerprints, iris scans, forearm veins. Whereas there is presently little evidence to inform or identify the new uses that public and private sectors may develop from this association of surveillance technologies, some are concerned that this will lead to more intrusive observation or tracking of individuals.<sup>95</sup>

Policy-makers are also concerned about the interactions between RPAS and biometric technologies and capabilities. For instance, in the United States, Richard M. Thompson II, a legislative attorney, declared in his Report for the U.S. Congress "In the near future, law enforcement organisations might seek to outfit drones with facial recognition or soft biometric recognition which can recognize and track individuals based on attributes such as height, age, gender, and skin color".<sup>96</sup> In the European Union, the Dutch Minister for Safety and Justice has recently answered questions about potential use of drones, specifically not excluding the potential to equip drones with facial recognition sensors in the future. He stated, "Since I am not able to foresee all future purposes for which a Raven [another drone] or Scan Eagle will be used, I do not want to rule out the fact that there will come a time when they are fitted with

---

<sup>91</sup> Rosenblum, Andrew, "Drone Robotique, Recette Pour un Drone 100 % Autonome" *Courrier International*, 17 January 2013. <http://www.courrierinternational.com/article/2013/01/17/recette-pour-un-drone-100-autonome> See also Davis, Josh, "Biomimetics: It Looks Like a Bird, It Acts Like a Bird, But It's Not a Bird", *Technology Trends*, 2013. <http://www.etacg.com/technology-trends/animals-as-inspiration-for-technological-advancement>

<sup>92</sup> Refers to a persons' behaviour studied in line with their biometric characteristics (such as voice, retina): Volovesky, op. cit., 2014, p. 314.

<sup>93</sup> The right to keep bodily functions and body characteristics private: Finn, Rachel, L. and David Wright, "Privacy and Data Protection Issues Related to Use of Civil RPAS, *European Data Protection Authorities meeting, European Commission*, Brussels, 28 February 2014.

<sup>94</sup> Volovesky, op. cit., 2014, p. 314.

<sup>95</sup> Volovesky, op. cit., 2014, p. 314.

<sup>96</sup> Thompson II, Richard M., "Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses", *CRS Report for Congress*, April 2013, p. 4; Dillow, Clay, "Army Developing Drones that Can Recognize Your Face from a Distance", *POPSCI*, 2011.

cameras capable of facial recognition. Any violations of privacy resulting from that, are, in itself, not a valid reason to rule it out in advance”.<sup>97</sup>

The security sector, crime prevention programs and even social networks such as Facebook and LinkedIn, are already using biometric analysis.<sup>98</sup> Furthermore, access to biometric data for many commercial organisations can be beneficial for profiling. Specifically, some retail organisations are already using biometrics to identify or profile customers.<sup>99</sup> We can, therefore, easily imagine that drones equipped with biometric sensors will be used by the commercial sector to increase their marketing actions and reduce their staff costs. One example would be the utilisation of small drones in luxury shops that act as personalised sales representatives that are fitted with “behaviometrics” (facial, iris, voice) and connected to a database containing customer files (names, former purchases, etc.). This drone would act as a sales representative and personalise the sale by recognising the customer and recommending items similar to those previously purchased by the customer.

### ***Concerns about privacy of location and space***

Mounted with Global Positioning System (GPS), Automatic Number Plate Recognition (ANPR) or even a video camera transmitting in real time, RPAS can infringe *privacy of location and space*. Privacy of location and space “encompasses the right of individuals to move in their “home” and other public or semi-public places without being identified, tracked or monitored”.<sup>100</sup> It is clear that by recording images of a person or of a vehicle in public places, RPAS allow their operator to locate individuals in particular places and at particular times, and also enables operators to reveal a person’s movements. A comprehensive record of a person’s movements can in turn reveal sensitive personal data such as “familial, political, professional, religious and sexual details” (*United States vs. Jones*, 2012).<sup>101</sup> Furthermore, when connected with other analytics software like facial recognition or automatic number plate recognition (ANPR), pedestrians and vehicles may be tracked. If this device rests in the hands of a stalker, a thief or even a parent worrying for his/her child, these devices may result in a multitude of privacy breaches, as well as inflict injury on the surveillance subject. In the commercial sector, drones fitted with GPS devices could benefit delivery companies. Amazon and Dominos pizza have already placed advertisements on YouTube which suggest that deliveries will be affected more efficiently with the use of drones. So, equipped with a GPS, drones used in this context can gather location data corresponding to the addresses of their customers.

In the law enforcement sector, while many US Police Officers expressed their will to use drones associated with GPS and ANPR,<sup>102</sup> others, such as the U.S. Senator Rand Paul, fear the consequences of drones with tracking capabilities.

---

<sup>97</sup> Dutch Parliament, “Aanhangsel van de Handelingen. Vragen gesteld door de leden der Kamer, Met de Daarop Door de Regering Gegeven Antwoorden”, *Tweede Kamer*, 31 April 2014  
<http://www.tweedekamer.nl/kamerstukken/kamervragen/detail.jsp?id=2014D11452&did=2014D11452>

<sup>98</sup> Volovesky, op. cit., 2014, p. 314.

<sup>99</sup> Finn, Rachel L., and Kush Wadhwa, “The Ethics of ‘Smart’ Advertising and Regulatory Initiatives in the Consumer Intelligence Industry: A Critical Review of Digital Red-Lining, Exploitation and Other Ethical Impacts”, [forthcoming] 2014.

<sup>100</sup> Finn, Wright, and Friedewald, op. cit., 2013, p. 16.

<sup>101</sup> Ibid.

<sup>102</sup> St. Louis Police Chief, Sam Dotson, wants to employ drones to go after suspects on the run: “This is a way we can monitor the individual, back off, not chase him at high speeds and when it’s safe for the officers and safe for the community, move in and make an arrest”. Also see Ruane, Jessica, “Could Spy Drones e the

*Flying over our homes, farms, ranches and businesses and spying on us while we conduct our everyday lives is not an example of protecting our rights. It is an example of violating them. . . . When I have friends over for a barbecue, the government drone is not on the invitation list. We should not be treated like criminals or terrorists while we are simply conducting our everyday lives. We should not have our rights infringed upon by unwarranted police-state tactics.*<sup>103</sup>

In addition to privacy of location, drones will also interfere with some private spaces. This intrusion in our private sphere is discussed by Calo in that robots “introduce new points of access to historically protected spaces”.<sup>104</sup> So, there exists a real risk of being filmed in private spaces such as one’s own backyard. Calo describes another risk related to privacy of space as one that arises when a drone is hacked and used against its own operator. For example, an intelligence agency or a commercial company engaging in corporate espionage could acquire software to infiltrate drones to capture images, GPS traces or even to turn on microphones or cameras in order to access, alter or delete any information stored.<sup>105</sup>

### ***Concerns about associational privacy***

Finn, Wright and Friedewald also point out the potential risks that RPAS do not respect the association privacy of individuals. The privacy of association refers to “the freedom of people to associate with others”.<sup>106</sup> RPAS combined with sensors, such as GPS, could evoke concerns such as operators tracking their targets and thereby identifying a target’s group membership/s, affiliation/s and other private group activities. Further, a relevant example in the commercial sector would be that, following the rumour of a fusion between competitors, a corporate spy utilises a drone fitted with a camera and a GPS tracker to identify which competitor company they will associate with for future innovations. It should be noted that these concerns are also heightened when RPAS are equipped with a visual payload such as a camera. For example, a local aircraft enthusiast purchases a drone to curb anti-social behaviour in his neighbourhood. He films teenagers’ hanging out in his neighbour’s front garden, and sometimes uses the drone to follow young people home and identify where they live. The drone is small and very quiet, and the teens are often unaware that they are being filmed.

Thus, RPAS fitted with payloads other than photography equipment and visual sensors raise privacy issues unique to those capabilities. Therefore, individuals operating RPAS for non-visual imaging purposes must take account of different and/or additional privacy issues. This suggests that as the capabilities of RPAS proliferate, users and operators will have to be well educated about potential privacy infringements in order to ensure compliance with relevant legal and ethical obligations.

---

Future of Crime Fighting?”, *Pando*, 31 January 2014. <http://pando.com/2014/01/31/could-spy-drones-be-the-future-of-crime-fighting/>

<sup>103</sup> Ryand, Paul, “Don’t let drones invade our privacy”, *CNN Online*, 2012. <http://www.cnn.com/2012/06/14/opinion/rand-paul-drones/>

<sup>104</sup> Calo, Ryan M., “Robots and Privacy”, in Patrick Lin et al. (Eds.), *Robot Ethics: The Ethical and Social Implications of Robotics*, MIT Press, Cambridge, 2012, pp. 187-202.

<sup>105</sup> La Rue, Frank, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council, A/HRC/23/40, 17 April 2013, pp.6-7, [http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40\\_EN.pdf](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf)

<sup>106</sup> Finn, Wright and Friedewald, op. cit., 2013.

### 3.2.5 Privacy concerns related to non-surveillance activities: chilling effect and property

As discussed above, in addition to imaging and other information gathering applications, RPAS have demonstrated potential capabilities for applications other than those that may be conceptualised as surveillance. RPAS that are used for recreational purpose or for commercial activities like crop dusting are much less invasive than RPAS used for surveillance purposes. Nevertheless, privacy concerns can still be identified in relation to these uses.

As with the case of drones used for monitoring, inspection or information gathering purposes, we can expect a “chilling effect”. Since people do not know who is operating the drone, what its capabilities are and what types of payloads it is carrying, they may behave as if they are under observation irrespective of the extent of that observation or whether the information gathered about them is subsequently used. As noted above, this implicates civil users of RPAS in wider privacy discussions, regardless of whether their operations have impacts on individuals.

Besides privacy threats, civil RPAS, by virtue of their capacities of “peering inside high-level windows and through solid barriers, such as fences, trees, and even walls”<sup>107</sup> will undoubtedly erode the status of the right to private property. So, regardless of whether drones are fitted with payloads to monitor or not; we can already predict situations where there may be grounds for legal action for breaches of property law resulting from improper uses of drones.<sup>108</sup> Relevantly, the effectiveness of laws prohibiting harassment, stalking, or nuisance are compromised by the complexity involved with identifying a drone’s operator.

### 3.2.6 Summary

The purpose of this section was to identify and describe the different privacy issues related to the use of civil RPAS in commercial, governmental and domestic applications. We observed that RPAS are and will be used for monitoring activities by a wide variety of operators. Whereas it is clear that law enforcement will use them for criminal investigations and other surveillance missions, private actors such as corporates and journalists may also use them for corporate espionage, tracking celebrities and other observation activities. Furthermore, we saw that some individuals will envisage the use of drones as a new tool for private monitoring activities including the protection of their own property, as well as more sinister (voyeuristic) pursuits. Second, we analysed whether RPAS technology produces a change in the nature of surveillance. We answered this question in the affirmative, because any operator may easily undertake surveillance via RPAS, and because this widespread surveillance engenders a privatisation of the surveillance. Furthermore, RPAS also change the nature of surveillance because of the inherent capabilities of RPAS that were not features of former surveillance technologies such as helicopters, and traditional CCTV systems. These factors make RPAS technologies a unique tool for targeted observations and ubiquitous surveillance.

In the third and fourth sub-sections, we examined privacy concerns according to the type of payload with which the drone is equipped. The fourth sub-section concerns the privacy issues related to drones fitted with visual payload while the fifth section covers those when drones

---

<sup>107</sup> The Electronic Privacy Information Center (EPIC. Org.), “Domestic Unmanned Aerial Vehicles (UAVs) and Drones”. <http://epic.org/privacy/drones/>

<sup>108</sup> Ilya Somin, “Private Drones and Private Property Rights”, *Volokh*, 2012. <http://www.volokh.com/2012/02/19/private-drones-and-private-property-rights/>

are equipped with non-visual payloads. We observed that the different privacy dimensions are impacted differently according to if the drone is used in a visual or non-visual surveillance application. This analysis has shown that RPAS technology associated with visual payloads including high-tech, thermal imaging and infra-red cameras are more privacy intrusive than RPAS associated with other sensors. This is for a number of reasons. The main reason is that with visual payloads, drones affect almost all types of privacy (bodily privacy, behaviour privacy, image and information privacy, location and space privacy, and association privacy). Furthermore, RPAS fitted with visual sensors allow their operators to film live and take footage of objects and individuals in private and public places, which in turn raises privacy issues, such as a chilling effect or panoptic syndrome, that do not arise in the context of non-visual surveillance. Another reason is that visual payloads are cheaper and easier to purchase than other sensors. Therefore, all types of drone operators, including government agencies, corporates, journalists and private users, may easily access such technologies.

In the fourth sub-section, we remarked that non-visual sensors mounted on RPAS that are used for information gathering applications may also affect different dimensions of privacy of an individual (bodily privacy, privacy of information, privacy of location and space and privacy of association). In non-visual surveillance, recognition sensors and GPS devices are certainly the most privacy intrusive devices when they are associated with drones. Finally, the fifth sub-section demonstrates that there are also privacy considerations surrounding RPAS usage by professional and hobbyists because the RPAS can be used for purposes subsequent to surveillance. The erosion of the status of private property is certainly one of the main issues.

### **3.3 Data protection issues associated with RPAS**

As mentioned in Section 2 above, drone operators process, use and store personal information they capture via the help of sensors mounted on RPAS. Whereas it is evident that photograph is the type of personal data which is the most frequently collected by drones, biometric data, and location data are also personal data able to be captured by drones' operators. Since personal data is collected, a specific dimension of privacy is concerned, the privacy of personal information. Contrary to the other dimensions of privacy, the privacy of personal information is protected by a specific right, the data protection right.

This third Section is devoted to the examination of these different elements. In a first stage, we will define the concept of data protection and its relationship with the right to privacy. In a second stage, we will examine the data protection risks that the RPAS sensors may raise in their civil applications. In relation to data protection risks, the discussion of this chapter is confined to generalised data protection risks, rather than specific risks and principles treated in the data protection legislation that will be examined in Chapter 5 (i.e., proportionality, transparency, etc.).

#### *3.3.1 The concept of data protection*

The concept of "Protection of Personal Data" appeared with the emergence of the computer age during the 1960s and 1970s. The right to privacy was no longer sufficient to address the

issues posed by emerging technologies.<sup>109</sup> The right to protection of personal data emanated from the rights of privacy and autonomy, but responded to the specific need to protect citizens from abuses by the public and private sectors in the processing, use, storage and disclosure of citizens' personal data.<sup>110</sup> Since its formal recognition, "data protection laws have therefore been characterised as regulatory reactions to technological developments".<sup>111</sup> In order to balance the powers of the data collectors and the data subjects, and to balance the need for collection, use and dissemination of collected information and its impact on the liberties and rights of individuals, the right to data protection constantly evolves according to the technological developments.<sup>112</sup>

Although data protection and privacy share certain characteristics and interplay, they are often described as being "twins, but not identical".<sup>113</sup> The privacy right is broader than the data protection right but we will see later that unlike privacy protection rules, "data protection rules are not prohibitive: they organise and control the way personal data are processed".<sup>114</sup> Privacy tends to protect the intimacy of the person and the secrets of each individual, while data protection is more business-like, it is not only a personal right but also a *corpus juris* for companies.

Data protection is already the subject of a wealth of academic literature, as well as a multitude of legal instruments around the world. In this contribution, we will first identify the data protection risks surrounding the RPAS technology when drones are used for the purpose of collecting personal information and then, in latter chapters we will examine the European and national data protection framework relating to RPAS applications.

### 3.3.2 *The data protection risks inherent in RPAS technology*

For many years, individuals' information has been a currency and tool for control by companies and states. Collected and processed for all types of purposes (profiling, marketing, immigration, anti-terrorism, etc.), personal data are collected by all types of actors (companies, states, individuals). Amongst drone's equipment, main of them will allow to collect personal data (biometric data, images, sounds, location data, sensitive data, etc.). Due to their aerial capabilities, RPAS technology is more likely to result in incidental collections of personal data than other types of processors and, thus, more likely to infringe the fundamental data protection right. These concerns have been confirmed by the Article 29

---

<sup>109</sup> De Hert, Paul and Vagelis Papakonstantinou, "The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters – A Modest Achievement However Not the Improvement Some Have Hoped for 2009", *Computer Law & Security Review*, Vol. 25, 2009, pp. 403-40; Boehm, Franziska, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, Springer, Berlin, 2012, p. 19.

<sup>110</sup> Ibid.

<sup>111</sup> European Commission, "Legal Analysis of a Single Market for the Information Society. New Rules for a New Age? The Future of Online Privacy and Data Protection, Brussels, 2009, p. 3.  
file:///Users/annadonovan/Downloads/Singlemarket-legalanalysis.pdf

<sup>112</sup> de Terwangne, Cécile, *Le Manuel Vie privée et données à caractère personnel*, Politeia, Brussels, 2013.

<sup>113</sup> European Commission, op. cit., 2009, p. 4; Hustinx, Pierre, "Data Protection in the European Union", *Privacy & Informatie*, 2005, p. 62-65; De Hert, Paul and Eric Schreuders, "The Relevance of Convention 108", *Council of Europe Conference on Data Protection, Warsaw, proceedings 33 & 42, 19-20 November 2001*.

<sup>114</sup> European Commission, op. cit., 2009, p. 4; Gutwirth, Serge and Mireille Hildebrandt, "Profiling the European Citizen", *Computers, Privacy and Data Protection Conference*, 17 January 2009.  
www.cpdconferences.org, p. 4.

Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Art.29WP), which has recently issued a “Response to a Questionnaire from the European Commission regarding the data protection issues related to RPAS”.<sup>115</sup> In its response, the Art.29WP confirmed the potential data protection breaches related to civil drones, stating that:

*There is unquestionably a real need to focus on the threats that an uncontrolled proliferation of drone applications could bring about for individuals’ fundamental rights and freedoms. From a data protection point of view, what is relevant is not so much the use of RPAS as such, but mainly the different technologies they can be equipped with (i.e. high-resolution cameras and microphones, thermal imaging equipment, or devices to intercept wireless communications) and the subsequent collection and processing of personal data that may take place.*<sup>116</sup>

As is the case with privacy issues, it is complex to identify and enumerate each current and potential data protection risk presented by the civil use of drones. This is because the data protection issues arise depending on the type of payload attached to the drone, and may also vary subject to the quantity of the data collected, the type of personal data collected (sensitive or not), the type of collector, and the purpose of the collection and processing. Thus, certain types of processing operations will be more likely to breach the data protection laws and fundamental civil rights than others.

However, unlike our observation with privacy issues related to RPAS technologies, the RPAS technology does not present any new data protection issues that have not already been raised in relation to other existing technologies. This is because, although RPAS technology in itself is new, the payloads that can be fitted to the drones 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.

Later in this contribution, we will analyse the data protection principles and the adequacy of these when applied to the use of the RPAS technology. In this regard, we will also identify the legal data protection issues that the RPAS technology may arise. In the present section, we focus on the general data protection risks inherent in RPAS technology. These risks are the invisible feature of the data collection, the potential for indiscriminate and mass collecting of data, disclosure and the hijacking of drones’ content, profiling, and de-individualisation and discrimination.

### ***The invisible feature of the data collection***

The inherent nature of the RPAS technology is that the collection of personal data will mostly take place without the knowledge of the data subject. In the context of RPAS technology, there exists what has been referred to as a “double invisibility”.<sup>117</sup> First, photographic technologies (high resolution, night vision) developed for RPAS are able to film and take

---

<sup>115</sup> Article 29 Working Party, Response to a Questionnaire from the European Commission regarding the data protection issues related to RPAS, Ref. Ares3737090, Brussels, 16 December 2013, p.1.  
[http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131216\\_reply\\_to\\_rpas\\_questionnaire.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131216_reply_to_rpas_questionnaire.pdf)

<sup>116</sup>Ibid.

<sup>117</sup> Fossoul, Virginie, “RFID et biométrie: Etat des lieux”, in Docquir, B A. Puttemans (Eds.), *Actualités du droit de la vie privée*, Bruylant, Brussels, 2008, p. 149-150.

photographs from a distance that the subject concerned is not aware of the capture of images. Second, the transfer of data between the RPAS and the collector ordinarily takes place in an invisible way and at a distance from the data subject. For example, photographic and cinematographic images collected by drones are generally transmitted online. The same occurs with snippets of intercepted communications. Hence, it is easy for any drone operator to covertly process personal data.<sup>118</sup>

This double invisibility poses problems for the enforcement by an individual of their rights. This is because the data subjects are rarely aware that their data is being collected and processed in the first place. The Art.29WP has observed the “enforcement concern about the transparency principle” where drones collection is invisible when it stated:

*The increasingly powerful techniques drones may be equipped with would allow collecting personal data through high resolution image and video recordings as well as storing and, if necessary, transferring such data to the relevant ground station. Data subjects would hardly be aware of this kind of processing as it is difficult to notice RPAS, because of their small size and the altitude of operation. Furthermore, it is difficult, if not impossible, even for individuals noticing such devices, to know who is observing them, for what purposes and how to exercise their rights.*<sup>119</sup>

Thus, there arise many situations when personal information will be collected by drones in the absence of the data subject’s knowledge or consent. The subsequent usage, storage or re-sale by a commercial company to another is a plausible eventuality of the data. Thus, it is apparent that data protection rules are likely infringed even in the most generic cases.

### ***The indiscriminate and mass collection of information***

Being mobile, civil drones can capture massive amounts of data in an indiscriminate way. This indiscriminate character of RPAS technology was also emphasised by the President of The Rutherford Institute when he stated “the logical aim of technologically equipped police who operate as technicians must be control, containment and eventually restriction of freedom”.<sup>120</sup> The Belgian Privacy Commission concurs, stating when “they cannot distinguish the subjects and elements filmed, the collection is susceptible to operate without any criterion and without a prior selection of information which is relevant to carry out a specific purpose”.<sup>121</sup> This is illustrated by the example of an operator who uses a commercial RPAS fitted with a high definition camera to examine 100m high power lines in a rural area. In order to fulfil its mission, this RPAS captures and records images of the towers and power lines, as well as a few residential gardens visible in the background. It is clear that in many situations some personal information of individuals will be incidentally collected by RPAS when the material is not adapted to the mission. This capacity to process and store massive amounts of data in an indiscriminate manner is contrary to the data protection principles.<sup>122</sup> Generally, the data protection principles require that data be processed for a well-defined purpose, and that

---

<sup>118</sup> Ibid.

<sup>119</sup> Article 29 Working Party, op. cit., 2013, p.1.

<sup>120</sup> Whitehead, John W., “Drones Over America: Tyranny at Home”, *njtoday online*, 30 June 2010. <http://njtoday.net/2010/06/30/drones-over-america-tyranny-at-home/>

<sup>121</sup> Belgian Privacy Commission, op. cit., 2009.

<sup>122</sup> Ibid.

the processing is not excessive to the purpose pursued, or that it could be obtained and processed by less intrusive technological means.

Furthermore, drones used for surveillance purposes bring to mind PRISM and other similarly controversial surveillance programs. Specifically, images and video captured by drones can be stored and analysed at a later date for future purposes.<sup>123</sup> An example of this is where police using an RPAS to take HD footage of a road accident in dangerous conditions but later uses this footage to identify drivers to issue speeding tickets and other traffic infringements.<sup>124</sup> We can also predict similar unlawful uses of data within the private sector. For example, a mapping company that films a neighbourhood and transmits this live footage to a company that discovers a celebrity hosting a party. This footage may be sold to a tabloid in breach of a number of privacy and data protection laws. As discussed in relation to the finality principle, the fact that drones are capable of storing massive volumes of many types of data in an indiscriminate way, RPAS operators are likely to collect more data than necessary to the purpose of the initial collection. This leads to a breach of the principles of data proportionality and minimisation.

### ***Disclosure and the hijacking of RPAS' content***

Two elements inherent in drone's technology increase the risks that personal data of individuals captured via RPAS are disclosed, their Wi-Fi connection (mostly to transmit information) and their use by private individuals. First, data collected by RPAS that is directly or indirectly transmitted through wireless communication represents a situation where drones process personal data in a manner that poses security risks to the data collected.<sup>125</sup> Indeed, RPAS technology is not a reliable method of ensuring confidentiality of the data as data security and integrity can be endangered by modes of transmission such as satellites, Wi-Fi, and other broadcast technologies. These modes of transmission also increase the potential risk of hacking. As a matter of fact, various newspapers have recently published articles about how it is easily for hackers to hijack a RPAS, to take control of it, of its photographic capabilities and of its content.<sup>126</sup> The CNIL, the French Data Protection Authority has, for instance, evoked that during the "DronesGames", a team of developers from the company Groupon hacked an AR drone and used it to take photographs of the public, apply a facial recognition algorithm and tweet the footage with the name of the person when they are identified.<sup>127</sup> CNN has also recently published an article describing how drones may be hacked to tap into smartphones with Wi-Fi settings, and for the purpose of accessing personal information including credit card information, usernames and passwords.<sup>128</sup> Unfortunately, victims of such crimes are rarely compensated due to the difficulties associated with

---

<sup>123</sup> Schermer, Bart W., "The Limits of Privacy in Automated Profiling and Data Mining", *Computer Law & Security Review*, Vol. 27, 2011.

<sup>124</sup> Finn and Wright, op. cit., 2012, pp. 184–194.

<sup>125</sup> Fink, Erica, "This Drone Can Steal What's on Your Phone", *CNNMoney*, 20 March 2014. <http://money.cnn.com/2014/03/20/technology/security/drone-phone/>

<sup>126</sup> Greenberg, Andy, "Flying Drone Can Crack Wifi Networks Snoop on Cell Phones", *Forbes*, 28 July 2011. <http://www.forbes.com/sites/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/>; Gallagher, Ryan and Rajeev Syal, "Met police using surveillance system to monitor mobile phones", *Guardian*, 30 October 2011. <http://www.theguardian.com/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance>

<sup>127</sup> Geffray, Edouard, "Drones, innovations, vie privée et libertés individuelles", *La lettre innovation et prospective de la CNIL*, No.6, Paris, 2013, p. 4.

<sup>128</sup> Fink, op. cit., 2014.

identifying a hacker in such situations where hackers are physically located at a great distance from the drones, and often from the location where the crime is committed.

Secondly, private use being unregulated in terms of data protection, the access of such gathering information technology by individuals will necessarily increase abuses and disclosure concerns. Risks of misuses by private operators are further reinforced by the “drone it yourself” phenomenon. By “drone it yourself” we refer to the practice of several private operators purchasing different kind of technologies (RPAS, sensors, software, etc.) and making their own sense-enhancing drones.<sup>129</sup> One trend is to buy a drone and to equip it with a GoPro camera.<sup>130</sup> What will happen when recognition sensors such facial recognition will be cheaper and accessible on the market to all?

### ***Profiling, de-individualisation and discrimination***

“Profiling” is “the process of discovering correlations between data in databases that can be used to identify and represent a human or nonhuman subject (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group of a category”.<sup>131</sup> Profiling practices are used mainly by the private sector in the process of direct marketing, but can also be utilised by the public sector for a range purposes such as anti-terrorism.<sup>132</sup> In the commercial sector, profiling allows commercial entities to use different types of data relating to their customers to determine their consumption profiles. However, “misuse or abuse of profiling may have negative consequences for individuals and society as a whole”.<sup>133</sup> In some circumstances, profiling may provoke discrimination or de-individualisation concerns.<sup>134</sup>

The first use of drones for profiling took place when the American army used military drones for profiling terrorists. This profiling highlighted the potential for drones to carry out profiling task in non-military scenarios. However, such use can end in abuses of personal rights of the data subject. For example, a leading retailer deploys drones mounted with camera and GPS to take footage of the houses, backyards and cars of its customers. After matching information collected from the footage (car brands, house sizes and types etc.) with the addresses and names of its clients, the company may quite easily perform targeted advertising. Further, the extraction and combination of the collected data may result in discrimination against individuals with particular characteristics.<sup>135</sup> Furthermore, by reading this data and subsequently grouping customers, the customer loses its individual identity. Bart W. Schermer comments on this form of profiling as potentially leading to stigmatisations of group members and even damage to societal cohesion.<sup>136</sup>

Besides de-individualisation risks, the combination of data collected by drones with other data files may produce data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health

---

<sup>129</sup> Geffray, op. cit., 2013, p. 4.

<sup>130</sup> For example, La Drone Shop, “Go Pro, Be a Hero”, no date. <http://www.ladroneshop.com/fr/26-gopro>

<sup>131</sup> Schermer, op. cit., 2011, p.45.

<sup>132</sup> Ibid.

<sup>133</sup> Schermer, op. cit., 2011, p.45.

<sup>134</sup> Ibid.

<sup>135</sup> Finn and Wadhwa, op. cit., [forthcoming] 2014.

<sup>136</sup> Schermer, op. cit., 2011, p.45.

or sex life” and health data<sup>137</sup>. These types of data are considered “sensitive data” under European law and its collection and processing is heavily restricted.

### 3.3.3 Summary

Whereas this section had not for scope to examine the legal data protection issues that the RPAS technology may raise as these latter will be latter discussed, it aims to identify and examine data protection risks inherent in RPAS technology. The main difficulty observed in this study is that data protection risks related to the collection of data through the means of drones depends upon different elements and circumstances of that collection. However, four main areas of concern have been identified. These are: the enforcement of data subject rights in the face of the invisible collection and processing of data by RPAS; the risk of breaches that indiscriminate processing may produce in light of the data protection principles, particularly the principles of purpose limitation, proportionality and data minimisation; the hacking of drones and their content; and the profiling of customers for commercial gain may lead to de-individualisation and discrimination issues.

## 3.4 Ethical issues related to RPAS

The term ethics originates from the Greek word “*ethos*”, meaning “character” or “habit” and from the Latin word “*mores*”, signifying customs.<sup>138</sup> Ethics is a branch of philosophy that rationally assesses what is good and wrong for the individual, personally, and in an individual’s relationships with others (for society).<sup>139</sup> It also refers to “well-founded standards of right and wrong that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, or specific virtues”.<sup>140</sup> Some ethical principles are manifested in laws, and particularly, in codes of conduct. However, this is not always the case if the law is partially based on ethical principles of a society as, “many acts that would be widely condemned as unethical are not prohibited by law”.<sup>141</sup>

Relevantly, ethical concerns surround the use of RPAS in civil applications. Major ethical concerns of RPAS application are identified as safety, public dissatisfaction, discriminatory targeting and illegal intrusion in wildlife.

---

<sup>137</sup> European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, Article 8.

<sup>138</sup> Legal Information Institute, “Ethics: An Overview”, *Cornell University Law School online*, no date. <http://www.law.cornell.edu/wex/ethics>; Gutwirth, Serge, Raphael Gellert, Rocco Bellanova, Michael Friedewald, Philip Schutz, David Wright, Emilio Mordini and Silvia Venier, *Legal, Social, Economic and Ethical Conceptualisations of Privacy and Data Protection (Deliverable 1-Prescient project)*, European Commission, Brussels, 2012, p. 16.

<sup>139</sup> *Ibid.*

<sup>140</sup> Velasquez, Manuel, Claire Andre, Thomas Shanks, S.J., and Michael J. Meyer, “Issues in Ethics”, *Santa Clara University online*, Vol. 1, No.1, 1987. <https://www.scu.edu/ethics/practicing/decision/whatisethics.html>

<sup>141</sup> Legal Information Institute, op. cit.

### 3.4.1 Ethical concerns related to the use of RPAS

#### *Safety*

The examination of the potential safety risks that civil RPAS cause falls outside of the scope of this deliverable.<sup>142</sup> However, it ought to be noted that “safety is a primary consideration for individuals commenting on the possibility of large-scale deployments of RPAS”<sup>143</sup>, particularly as Bolkcom reports that the current accident rate for UAVs is 100 times that of manned aircraft<sup>144</sup>. This is because RPAS are often less maintained, and consequently less reliable, than traditional aircraft<sup>145</sup>, and more susceptible to pilot error<sup>146</sup>. Both these issues increase risks to commercial aircraft, and civilians on the ground.<sup>147</sup> Physical dangers and injuries may be the result not only of a deficiency of the mechanism, inadequate maintenance, or use or misuse by its operator, but also as a result of cyber-attacks.<sup>148</sup> However, unlike to the privacy challenges caused by the civil use of RPAS technology, the EASA and many Civil Aviation Authorities of the Member States have already adopted aviation rules and proposals including numerous security provisions.<sup>149</sup> As there is a close and direct connection between the safety of UAVs and the preservation of the right to privacy, some safety rules may engender a beneficial effect on the privacy of citizens. We refer, for instance, to the safety regulations prohibiting the flight of drones over densely populated areas. Such safety regulations “significantly interferes with the ability of UAVs to collect information on individuals located in those area; fewer flights, in turn, lessen potential infringements of individuals’ right to privacy”.<sup>150</sup>

In certain cases, safety concerns become also intertwined with ethical concerns. It is, *inter alia*, the case when RPAS are mounted with lethal and non-lethal weapons. Meredith Hagger and Brendan Gogarty opine:

*UVs are not strictly weapons, insofar as they may have a range of uses and carry a variety of on-board systems which have non-military utility. Conversely, they are extremely capable weapons platforms and are increasingly being designed to take place of manned fighter craft.*<sup>151</sup>

In its report on civil RPAS, ACLU, the American civil liberties watchdog, explains that American RPAS manufacturers are already selling the idea to law enforcement agencies “the

---

<sup>142</sup> For more information about safety issues see Clarke, op. cit., 2014, pp. 263-285.

<sup>143</sup> Gutwirth, et al., op. cit., 2012, pp. 184–194.

<sup>144</sup> Bolkcom, Christopher, “Homeland Security: Unmanned Aerial Vehicles and Border Surveillance”, *Congressional Research Service Report for Congress*, 28 June 2004.

<sup>145</sup> Dunlap, Travis, “We’ve Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search”, *South Texas Law Review*, Vol. 51, No. 1, Fall 2009, pp. 173-204.

<sup>146</sup> “Unmanned Aircraft: The fly’s a spy”, *The Economist*, 2007 <http://www.economist.com/node/10059596>

<sup>147</sup> EPIC Org., “Unmanned Planes Offer New Opportunities for Clandestine Government Tracking, Spotlight on Surveillance”, *EPIC*, 2005. <http://epic.org/privacy/surveillance/spotlight/0805/>

<sup>148</sup> Clarke, op. cit., 2014, pp. 263-285.

<sup>149</sup> For example in the national laws of Austria, Czech Republic, Denmark, France, Germany, Ireland, Italy, Poland, Sweden and the United Kingdom.

<sup>150</sup> Volovesky, op. cit., 2014, p. 310.

<sup>151</sup> Gogarty, Brendan and Meredith Hagger, “The Laws of Man Over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air”, *Journal of Law, Information and Science*, Vol. 19, 2008, p. 73.

option of arming these remote controlled aircraft with non-lethal (for now) weapons like rubber bullets, Tasers, and tear gas”.<sup>152</sup> These uses have been examined in detail in Chapter 3. However, within the European Union, the Members of the European Parliament (hereinafter, the MEPs) have recently adopted a resolution on armed drone usage expressing “grave concern over the use of armed drones outside the international legal framework”.<sup>153</sup> Furthermore, with regard to the potential use of civil drones mounted with weapons in the framework of surveillance or criminal investigation, the competence belongs to the Member States. Therefore, the MEPs have urged in their resolution that “the Council (Member States Representatives) to adopt an EU common position on the use of armed drones”.<sup>154</sup>

### ***Public dissatisfaction with RPAS***

Since the use of RPAS by the U.S in the war against terrorism,  
*there has been an on-going debate around the ethics of using remotely piloted vehicles in combat operations. They have been blamed for significant losses of life on the ground in combat zones, the removal of soldiers from the human consequences of their actions.*<sup>155</sup>

Although, people may support the use of RPAS in some civilian contexts such as for the detection and the monitoring of natural disasters, search and rescue missions<sup>156</sup>, citizens and particularly NGO’s are well aware that the design of military drones and the development of the military technologies associated (payloads) permits their dazzling development and their use in the civilian sphere and vice-versa<sup>157</sup>. This is strengthened further by the fact that some former military drones are re-used for civilian applications. In addition, the recent revelations about American surveillance programs ‘spying’ on citizens beyond U.S. borders heightens the level of mistrust members of the public hold in governments, as well as in major corporate players such as Google, where misuse of RPAS technologies are concerned. Hence, collection of data via the aid of drones in the framework of surveillance programs will likely face some opponents.

Furthermore, as described in the European Commission Roadmap related to RPAS and societal impacts, people expect that “RPAS have an ethical behaviour comparable with the humans, respecting some commonly accepted rules”.<sup>158</sup> While the public today expects that their privacy will not be undermined by the deployment of civil drones, scholars in the field do not agree on the evolution of these privacy expectations in relation to the emergence of privacy intrusive technology such as civil drones. On one hand, authors like Clarke explain by the following example how public expectation will remain the same regardless of the evolution of privacy intrusive technologies:

*a person in a quiet corner of a public park, or amid a large and noisy audience at a sport or entertainment event, might well be included in a general photo of the park or in a ‘crowd shot’ at the venue; whereas they reasonably have a strong expectation*

---

<sup>152</sup> Stanley, Jay and Catherine Crump, op. cit., 2011.

<sup>153</sup> European Parliament, Joint Motion for a Resolution on the use of armed drones ([2014/2567\(RSP\)](#)), 25 February 2014.

<sup>154</sup> Ibid.

<sup>155</sup> Gutwirth, et al., op. cit., 2012, p. 96.

<sup>156</sup> International Working Group on Data Protection in Telecommunications, op. cit., 2013.

<sup>157</sup> Volovesky, op. cit., 2014, p. 310; Hayes, Ben, Chris Jones and Eric Töpfer, op. cit., 2014.

<sup>158</sup> European RPAS Steering Group, op. cit., 2013, p. 44.

*that they will not be targeted with a zoom lens or a directional microphone. Technological development continually expands the capacity of other parties to invade private space, but it does not change the underlying human need, nor the reasonableness of the expectation.*<sup>159</sup>

On the other hand, authors like Calo and Nevins argue that drones could operate to shift privacy expectations and engender “the normalization of previously unacceptable levels of policing and... official abuse”. This shift could “operate to dampen constitutional privacy guarantees” or “disturbing implications for civil and human rights”.<sup>160</sup> In term of policy regulation, the difference of theory is very important as it implies that, in the first case, policy makers have to reinforce their privacy policies in order to assure the same level of privacy regardless of the technological innovation. In the second case, which seems unfortunately more realistic, policy makers and drones operators could benefit from this “shifting privacy expectation” phenomenon to allow for the gradual increase in the use of intrusive drones in the European airspace.

### ***Discriminatory targeting***

In Great Britain, it is well known that camera operators focus on disadvantaged neighbourhoods, resulting in a disproportionate collection of information relating to particular categories of individuals.<sup>161</sup> This discrimination concern has been confirmed by a sociological study concerning the way CCTV systems are operated: “Black people were between one and a half and two and a half times more likely to be monitored than one would expect from their presence in the population”.<sup>162</sup> Stanley and Crump, authors of the ACLU report, argue that problems may arise from the fact that “The individuals operating surveillance systems bring to the job their existing prejudices and biases”.<sup>163</sup> In the same range of idea, Coleman and McCahill explain that the use of this kind of technology often “reinforces existing social positions, particularly positions of marginalization along lines of race, class, gender, sexuality and age”.<sup>164</sup> Whereas most of the CCTV systems are fixed, drones fitted with a camera act as mobile CCTV systems. Therefore, if we can already identify the occurrence of discrimination in “simple observation”, we may presume that discriminatory behaviours correlate with the use of devices technologically designed for target monitoring, such as RPAS technologies. In terms of application, it has already been observed that the use of drones for border control faces such ethical concerns, particularly racial discrimination issues.<sup>165</sup>

### ***Illegal intrusion in wildlife***

With the recent advances in Nano-Biomimetic technologies – technologies recreating the traits and abilities of biological systems in the form of materials and machines – new potential surveillance capabilities are expected. This surveillance would be completely undetectable.

---

<sup>159</sup> Clarke, op. cit., 2014, p. 2.

<sup>160</sup> Nevins, Joseph, “Drones and the Dream of Remote Control in the Borderlands”, 2012. <https://nacla.org/>. See also Calo, “Robots and Privacy,” op. cit., 2012; European RPAS Steering Group, op. cit., 2013, p. 44.

<sup>160</sup> Clarke, op. cit., 2014, p. 2.

<sup>160</sup> Nevins, op. cit., 2012; Calo, “Robots and Privacy”, op. cit., 2012.

<sup>161</sup> Finn and Wright, op. cit., April 2012, pp. 184–194; Stanley and Crump, op. cit., 2011, p. 12.

<sup>162</sup> Ibid.

<sup>163</sup> Stanley and Crump, op. cit., 2011.

<sup>164</sup> Finn and Wright, op. cit., April 2012, pp. 184–194.

<sup>165</sup> The use of drones to monitor borders is beyond the scope of this research project.

Josh Davis, author in *Technology Trends*, observed that the association between biomimetic and RPAS technologies displays the following: “if you see a biomimetic drone, chances are you will just dismiss it as an animal, remaining completely unaware of the disadvantageous predicament you have just been forced in to”.<sup>166</sup> He also explains “the United States Air force is currently developing [bug like drones](#) designed to eliminate specific targets. When completed, these aerial drones will have the ability to fly, hover, and perch their way through almost any area”.<sup>167</sup> This “biomimetic-drone” is viewed as the future for the military sector, and it follows that this technology will be subsequently utilised by the private sector. The effect of this technology is a drone with greater surveillance capabilities, which will operate more ubiquitously, and invisibly, than before. Thus, we can expect an escalation of the privacy and ethical problems described above, and some scientists have already demonstrated that this illegal intrusion on wildlife will cause irreversible harm.<sup>168</sup> It is noteworthy that even if drones are not yet associated with biomimetic technology, some parks have already prohibited RPAS from flying over because the way they affect the fauna.<sup>169</sup>

### 3.4.2 Summary

This final section discussed the ethical concerns related to the civil use of RPAS technologies. Among these issues are security risks, especially those identified in relation to drones with weapon capabilities, the concern that civil drones are still associated with “military drones” in light of civilian deaths they cause in war zones, and the issue of emerging distrust between states and citizens. An examination of these issues also demonstrates the concerns relating to discrimination as drones, much like CCTV systems, may target some citizens more than others. Finally, we examined how wildlife could also be affected by the use of drones whether these latter take the appearance of animals by association of RPAS technology with the nano-biomimetic technology.

## 3.5 Conclusion

This analysis of the current and future privacy, data protection and ethical risks related to RPAS technology has demonstrated how the civil uses of drones may pose challenges for the fundamental rights and liberties of citizens. Numerous reports of watchdog associations have particularly pointed out concerns around the use of governmental drones in the context of visual surveillance operations. However, this study has shown that other civil applications and other types of RPAS operators may also flirt with the limits of what is “acceptable” in terms of privacy, data protection and ethics.

Therefore, the results of this analysis have thrown up many questions in need of further investigation. In light of the lack of European rules, do some Member States have rules governing the uses of RPAS? Do the right to privacy and existing data protection legislation apply to RPAS technology? If such is the case, are they sufficient to address the issues described above in a proactive way? Do they cover all types of application and all types of operators? Being so privacy intrusive and able to create such privacy violations, would it be

---

<sup>166</sup> Wood, op. cit., 2011, p. 13.

<sup>167</sup> Davis, op. cit., no date.

<sup>168</sup> Wood, op. cit., 2011, p. 13.

<sup>169</sup> Bolesse, Cécile, ‘Les Drones Sont Désormais Interdits de Séjour Dans le Yosemite Park’, *net.com editorial*, 2014. <http://www.01net.com/editorial/619252/les-drones-sont-desormais-interdits-de-sejour-dans-le-yosemite-park/>

logical to prohibit some civil applications? Should we prevent manufacturers from selling RPAS (with particular capabilities or payloads) to certain types of operators? Under which legal basis should we judge a person that is flying his drone mounted with a camera near the window of a female? Should we permit employers to use them for monitoring workers on a work site? Are there existing technologic means allowing operators to anonymise information?

Although this chapter attempted to measure the extent of the privacy impacts of the RPAS technology, it raises more questions than it answers. The next chapters of this report will examine these outstanding interrogations while at the same time fully respecting the realistic and pragmatic balance between offering a full privacy protective legal framework to European citizens and allowing that RPAS technology offers all the economic advantages already recognised.

## 4 RPAS TECHNOLOGY AND EUROPEAN PRIVACY AND DATA PROTECTION LAW

### 4.1 Introduction

The operations of RPAS are regulated in Europe by the European Aviation Safety Agency (EASA) and the national Civil Aviation Authorities (CAAs). These latter decide which drone's applications are permitted, enact aviation and safety rules and grant permits to governmental, commercial and individual operators<sup>1</sup>. More than one thousand RPAS permits have already been granted by the EASA and several CAAs (Austria, Czech Republic, Denmark, France, Germany, Ireland, Italy, Poland, Sweden and the United Kingdom).

Besides safety, we have seen in the previous chapter how RPAS operating in civil contexts may pose some privacy and data protection challenges. Such privacy risks surrounding the RPAS technology require a comprehensive privacy and data protection legal framework. However, although no privacy or data protection legislative instruments specific to RPAS technology exists at national or European levels, some elements of existing privacy and data protection law are applicable to the use of RPAS in civil contexts. Given this applicability it is necessary to examine these existing instruments in detail to clarify how RPAS operators might meet their legal obligations under these frameworks. Such an examination would also enable an identification of gaps where policy-makers may need to enact specific rules strictly adapted to drones.

Some stakeholders have already considered this question. Some stakeholders advocate for a regulation by analogy, arguing that the existing privacy and data protection regulatory framework is enough, while others suggest the adoption of specific regulation for RPAS.<sup>2</sup> The European RPAS Steering Group seems to take an intermediary position, holding that “part of the existing regulatory framework may be applicable to the use of RPAS and the existing case law on data collection and handling may provide guidance in the drafting and implementation of regulation specific to RPAS”.<sup>3</sup> It can be said that, the Commission does not oppose the use of drones, but rather foresees their integration into the current regulatory framework. The Commission funded research into RPAS technology and innovation in 2009. More recently, it has undertaken several initiatives to put in place a strong privacy and data protection framework for application to drone usage. On 8 April 2014, the Commission issued a Communication entitled “A new era for aviation – Opening the aviation market to the civil use of RPAS in a safe and sustainable manner”. The Commission intends to assess how to make RPAS applications compliant with data protection rules. It intends to consult experts

---

<sup>1</sup> Some specific aviation and safety regulations governing RPAS have already been enacted by the European Aviation Safety Agency (EASA), responsible for the RPAS above 150kg and the national Civil Aviation Authorities (CAA's), responsible for governmental RPAS and those lighter than 150kg.

<sup>2</sup> European RPAS Steering Group, Roadmap for safe RPAS integration into European Air System - Annex 3 A study on the societal impact of the integration of civil RPAS into the European Aviation System, 2013, [http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap-annex-3\\_en.pdf](http://ec.europa.eu/enterprise/sectors/aerospace/files/rpas-roadmap-annex-3_en.pdf)

<sup>3</sup> Hesselink, Henk, *ULTRA Unmanned Aerial Systems in European Airspace – Deliverable 3: Identification of Social Dimension*, 2013, p.58.

and relevant stakeholders, to increase awareness to protect fundamental rights of European citizens, and to promote measures under national competence.<sup>4</sup>

Chapter 12 and Annex B demonstrate that, at the national level, some Member States have already adopted aviation rules governing civil RPAS while others have drafted proposals that are awaiting adoption.<sup>5</sup> Few Member States have added some specific privacy and data protection provisions in their aviation legislation regulating the use of RPAS and its payloads.<sup>6</sup> Nevertheless, several national data protection authorities (DPA) such as in France and in Belgium have officially declared that the operators of drones must respect the national privacy and data protection legal framework.

Against this background, the present chapter will identify the existing European privacy and data protection laws and will assess the applicability of such legal texts to the different type of RPAS applications. It will provide a detailed analysis of the scope and principles provided by those laws through an examination of, first, the regulations governing the right to private life (Section 2), and second, the relevant provision of the data protection legislation (Section 3).

## **4.2 European law protecting the right to private life**

### *4.2.1 Overview*

In this first section, we study how the right to private life is regulated under European Union law, and examine whether principles forming the basis of this legislative protection could extend to regulate the use of RPAS technology in European airspace. In that regard, we discuss the main instruments that explicitly recognise the right to private life, namely the European Convention of Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (CFREU).

First, we focus on law of the Council of Europe and in particular, we analyse Article 8 of ECHR as the accepted “historic driver” of the development and expansion of the right to private life in Europe.<sup>7</sup> We also examine the positive and negative obligations flowing from this article in its horizontal application. That study is complimented by a review of relevant case law involving a number of surveillance operations led by the law enforcement sector, and the way in which those operations interfere with Article 8. In addition, a discussion of jurisprudence of the European Court of Human Rights regarding visual-surveillance leads to the identification of a number legal principles that could be relevant to regulation of RPAS-conducted surveillance. We also briefly examine the relevance of Article 7 of the CFREU.

### *4.2.2 Council of Europe law - Article 8 ECHR*

#### ***General – The wording of Article 8***

The Article 8 of the ECHR provides:

---

<sup>4</sup> European Commission, Communication of 4 April 2014 A new era for aviation – Opening the aviation market to the civil use of RPAS in a safe and sustainable manner, Brussels, 04.04.2014, p. 8.

<sup>5</sup> See Chapter 4 of this deliverable. Austria, Czech Republic, Denmark, France, Germany, Ireland, Italy, Poland, Sweden and the United Kingdom.

<sup>6</sup> See Chapter 4 of this deliverable. French and Germany.

<sup>7</sup> Docquir, Benjamin, *Droit de la vie privée*, Larcier, Brussels, 2008, p. 37.

1. *A person has a right to respect for their private and family life, home and communications.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*<sup>8</sup>

Article 8 is divided into two parts. The first paragraph enunciates the precise rights that guaranteed by the State including the right to respect for private life, family life, home and correspondence.<sup>9</sup> The second paragraph outlines a limitation to the respect of those rights<sup>10</sup>, providing that “it may be acceptable to interfere with Article 8 rights in certain circumstances”<sup>11</sup>.

However, the meaning of the private life, and the four rights enumerated in Article 8 do not adequately address the contemporary view of what “private life” today entails. The Strasbourg Court dealt with this issue by recognising an evolving interpretation of each of these rights by giving these concepts a broad definition.<sup>12</sup> For example, the concept of “home” includes a hotel room, a room in a guesthouse, as well as professional premises.<sup>13</sup> Relevantly, the court also found that Article 8 comprises a right to personal data protection. The Court held that “private life is a broad concept which is incapable of exhaustive definition”.<sup>14</sup> In other words, the protective scope of the right to private life is not limited to any particular area of life because it extends to the protection of personal autonomy (i.e., the possibility of self-determination with regard to one’s body, sexual orientation, relations with others, construction of one’s own identity, etc.) in the broadest sense.

Nevertheless, the right to private life is limited by Article 8(2) which requires that that right is not absolute and must be balanced with other liberties and general interests, such as the freedom of expression. However, interference with an Article 8 right must fulfil the three conditions listed in par. 2, namely that the interference is legitimate and justified, and “in accordance with the law”, and/ or the pursuit of a legitimate aim “necessary to a democratic society”. It is also left to the discretion of Member States to determine whether an interference with an Article 8 right is justified according to Article 8(2).<sup>15</sup> In making such a determination, a state court will ordinarily apply the following three steps analysis:

---

<sup>8</sup> Council of Europe, European Convention on Human Rights, Rome, .04.11.1950, Article 8.

<sup>9</sup> Kilkelly, Ursula *The right to respect for private and family life – A guide to the implementation of Article 8 of the European Convention on Human Rights. Human Rights Handbook 1*, Council of Europe, Strasbourg, 2003, p. 6.

<sup>10</sup> De Hert, Paul, “L’Article 8 CEDH”, in Cécile de Terwangne (Eds.), *Le Manuel Vie privée et données à caractère personnel*, Politeia, Brussels, 2013, p. 1.

<sup>11</sup> Kilkelly, *op. cit.*, 2003, para 6.

<sup>12</sup> Docquir, Benjamin, “Le droit de la vie privée : aperçu général et règles de proportionnalité” in B., **Docquir and A. Puttemans** (Eds.), *Actualités du droit de la vie privée*, Bruylant, Bruxelles, 2008, p. 6.

<sup>13</sup> *Ibid.*, p. 10.

<sup>14</sup> European Court of Human Rights (“ECtHR”), *Costello-Roberts v. the United Kingdom*, Judgment of 25 March 1993, no. 13134/87, para. 36.

<sup>15</sup> Akandji-Kombe, Jean-François, *Positive obligations under the European Convention on Human Rights. A guide to the implementation of the European Convention on Human Rights. Handbook 7*, Council of Europe, Strasbourg, 2007, p. 36.

- *Is the interference in accordance with the law? The legality requirement (accessibility and foreseeability)*

Article 8(2) stipulates firstly that interference to private life has to be “in accordance with the law”. According to the jurisprudence of the Court, this latter expression means, first of all, that a surveillance measure needs to have a legal basis in domestic legislation.<sup>16</sup> As a surveillance measure may seriously threaten an Article 8 right, the ECtHR prescribes that in order for the surveillance measure to be lawful, the national rule must be particularly clear, precise and detailed.<sup>17</sup> In addition, the European Court has added to its criterion two sub-criteria of accessibility and foreseeability. Accessibility requires that “the law which prescribes an interference with a right under Article 8 must be publicly accessible”.<sup>18</sup> Citizens must have access to the information on the subject and circumstances of the right that may be interfered with. Foreseeability requires that “the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence”.<sup>19</sup>

- *Is the interference in the pursuit of a legitimate aim?*

According to Article 8, a legitimate aim refers exhaustively to “national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.<sup>20</sup>

- *Is the interference necessary in a democratic society?: the necessity and proportionality requirements*

This last condition requires that States demonstrate not only that the interference respond to a “pressing social need”, but also that the interference is “proportionate to the legitimate aim pursued”.<sup>21</sup>

Therefore, the Court will only condemn a State for violation of Article 8 if the state concerned has interfered with a right to private life recognised by the court as being protected by Article

---

<sup>16</sup> ECtHR, *Malone v. the United Kingdom*, application no. 8691/79, Judgment of 2 August 1984, pp. 27-28, para. 67 (“*Malone v. the UK*”); ECtHR, *Huwig v France*, application no. 11105/84, Judgment of 24 April 1990, para. 28 (“*Huwig v. France*”); ECtHR, *Kruslin v France*, application no. 11801/85, Judgment of 24 April 1990, pp. 16-21, paras. 27 & 30-36 (“*Kruslin v. France*”); ECtHR *Khan v the United Kingdom*, application no. 35394/97, Judgment of 12 May 2000, pp. 6-7, para. 26 (“*Khan v. the UK*”).

<sup>17</sup> *Kruslin v France*, pp. 16-21, para. 36; *Huwig v. France*, para 35; De Hert Paul, Galetta Antonella, “The Legal Perspective. A Report Presenting a Review of the Key Features Raised by Legal Perspectives of Surveillance and Democracy. Deliverable D2.3 to EU Project IRISS (FP7-SSH-2011-2)”, 2013. <http://irissproject.eu/wp-content/uploads/2013/04/Legal-perspectives-of-surveillance-and-democracy-report-D2.3-IRISS.pdf>.

<sup>18</sup> The Council of Europe, *ECHR Online*, 1950, Article 8. <http://echr-online.com/art-8-echr/introduction#In> accordance with the law - accessible

<sup>19</sup> *Malone v. the United Kingdom*, supra note 147, para 67; *Kruslin v. France*, para 30; ECtHR, *Weber and Saravia v. Germany*, application no. 54934/00 admissibility decision, para 93 of 29 June 2006, para. 93 (“*Weber and Saravia v. Germany*”).

<sup>20</sup> The Council of Europe, op. cit., 1950, Article 8, para 2.

<sup>21</sup> Justice, *Freedom from Suspicion Surveillance Reform for a Digital Age*, Justice online, London, 2011, p. 35.

8(1) and, that the state cannot justify its interference by complying with the requirements of Article 8(2). However, as discussed below, when an interference is found in a surveillance measure, the ECtHR has developed specific requirements that public authorities must satisfy. However, the Strasbourg Court has competence to condemn only states for violation of individual rights under the Convention (vertical relationships), and thus domestic legislation protecting violations between private individuals and corporations (horizontal relationships) may be heard before national courts.<sup>22</sup>

### ***Positive and negative obligations and the vertical effect of the ECHR***

Adding to the complexity of Article 8, is the negative obligation arising from the wording of Article 8, and a positive obligation recognised by ECtHR case law.<sup>23</sup> In *Airey v. Ireland*, the court found that: “although the object of Article 8 (art. 8) is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life”.<sup>24</sup> Moreover, the negative obligation requires that states do not interfere in the private life of individuals unless the conditions of par. 2 are met, while the positive obligation entails that states ensure the protection of individual’s private life by setting up protective measures.<sup>25</sup> As is the case with interferences, the Court allows states a wide margin of appreciation regarding to both types of obligations.<sup>26</sup> The concept of positive obligations transposes the States obligation to be active in the protection of the Human Rights. In the context of Article 8, which is undoubtedly the most important area for the development of positive obligations<sup>27</sup>, the ECtHR imposes this obligation on states with the view that they may be held responsible for the consequence of the actions of corporate bodies even if those actions are not bound by human rights norms<sup>28</sup>.

As its title suggests, the European Convention of Human Rights has always been devoted to protect citizens against the interference by public authorities in their enjoyment of human rights. This is the reason why Article 8(2) is stipulated to protect individuals only from the interference of states and the ECtHR only examines the implementation of the convention by states (individuals-states, vertical relationships). However, violations of human rights do not only come from public authorities, but also from private parties and individuals. In this regard, rights of the convention, including Article 8 have been recognised as containing a horizontal effect.<sup>29</sup> Furthermore, the Convention has direct effect in national legal systems.<sup>30</sup> So, on one hand, Article 8 ECHR protects citizens from the interference of states but also

---

<sup>22</sup> Docquir, op. cit., 2008, p.9; De Hert, op.cit., 2013, p.1.

<sup>23</sup> Boehm, Franziska, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, Springer, Berlin, 2012, p. 26.

<sup>24</sup> ECtHR, *Airey v. Ireland*, application no. 6289/73, Judgment of 9 October 1979, Series A no. 32, p. 17, para. 32 (“*Airey v. Ireland*”).

<sup>25</sup> Franziska, op. cit., 2012, p. 26.

<sup>26</sup> *Ibid.*, p. 26.

<sup>27</sup> Akandji-Kombe, Jean-François, *Positive obligations under the European Convention on Human Rights. A guide to the implementation of the European Convention on Human Rights. Handbook 7*, Council of Europe, Strasbourg, 2007, p. 20.

<sup>28</sup> Edwards, Richard A., “Big Brother Watch, Private Investigators and the ECHR”, *Euro Rights Blog*.

<http://www.eurorights.org.uk/post/45610626019/big-brother-watch-private-investigators-and-the-echr>

<sup>29</sup> Sepulchre, Vincent, *La protection juridictionnelle des droits de l’homme en Belgique*, Kluwer, Brussels, 2007, pp.41-42.

<sup>30</sup> *Ibid.*

from private parties and other individuals in their enjoyment of private life rights. On the other hand, a breach of Article 8 of the Convention will be dealt with by a national judge, or in an action against a State before the Strasbourg Court.<sup>31</sup>

### *Article 8 of the ECHR case law on visual surveillance*

#### a) General

As Chapter 3 demonstrates, the observation and surveillance applications of RPAS engender privacy concerns. The ECtHR has produced a wealth of jurisprudence related to Article 8 and surveillance activities operated by law enforcement authorities with the core of its case law concerning the interception of communications and wiretapping.<sup>32</sup> In this section we examine the approach adopted by the ECtHR in its surveillance case law. The study of the surveillance case law of the ECtHR will allow us to draw out some principles that are applicable to RPAS technology when this technology is used by law enforcement agencies for monitoring activities. Subsequently, we examine the case law concerning non-visual surveillance.

#### b) Private sphere

Notably, the right to private life applies differently subject to the sphere in which the individual operates. The private sphere covers the intimate aspect of a human being's personality. This is considered a totally private sphere. It is delineated from the public sphere by physical boundaries, such as the home, personal relationships (family and friends), and by selected fields of information (personal, sensitive, or embarrassing information).<sup>33</sup> Article 8 of the ECHR applies to this sphere and any intrusion from outside will be considered as interference. Therefore, the use of drones to monitor someone within this private sphere will undoubtedly interfere with Article 8(1).

#### c) Public places

With respect to the meaning of public places, the Venice Commission defines a public area as:

*[...] at place which can be in principle accessed by anyone freely, indiscriminately, at any time and under any circumstances. Public areas are open to the public. In principle anyone at anytime can have the benefit of this area.*<sup>34</sup>

In public areas, individual privacy is similar to the concept of a non-privacy because:

*when entering a public space or staying there implies that one is conscious that one will be at least seen, even recognized, and that one's behaviour may be scrutinized by*

---

<sup>31</sup> Sepulchre, op. cit., 2007.

<sup>32</sup> Galetta, Antonella and Paul, De Hert Paul, "Complementing the Surveillance Law Principles of the Court of Strasbourg with its Environmental Law Principles. An Integrated Technology Approach to a Human Rights Framework for Surveillance", *Utrecht Law Review*, Issue 1, Vol.10, January 2014, p. 59.

<sup>33</sup> Nissenbaum, Helen, "Toward an Approach to Privacy in Public: Challenges of Information Technology", *Ethics & Behavior*, Vol. 7(3), 1997, p. 207.

<sup>34</sup> Venice Commission, *Opinion on Video Surveillance In Public Places by Public Authorities and the Protection of Human Rights*, Council of Europe, Strasbourg, March 2007, p. 3.

*anyone on this public sphere, one may draw one's own conclusions with respect to these elements and decide to adapt one's behaviour accordingly.*<sup>35</sup>

This acknowledges that “any human being moving in public areas may well expect a lesser degree of privacy”.<sup>36</sup> So, individuals can still hold privacy expectations, and thus, “they should not expect to be deprived of their rights and freedoms including those related to their own private sphere and image”.<sup>37</sup> Therefore, Article 8(1) may also be applied in public areas if the individual concerned could reasonably expect a certain degree of privacy.

With reference to the aforementioned considerations, the Court uses the “reasonable expectation of privacy” test to determine whether the right to private life (Article 8(1)) of an individual in a public place has been interfered with. Further, if the Court has confirmed that the “reasonable expectation of privacy” criterion is important, other elements must be taken in consideration:

*There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily a conclusive factor.*<sup>38</sup>

#### d) Public places: case law

The following cases examine the elements that the ECtHR or the CoE Commission have established in order to determine when monitoring and recording in public places constitute an interference with Article 8 ECHR.<sup>39</sup> The following cases concern surveillance measures undertaken by public authorities. However, the approach of the Court can also be applied to any monitoring activities carried out by any type of actors (individuals, corporates, and journalists).

In the case of *Herbecq v. Belgium*, it was found that mere monitoring does not interfere with Article 8(1):

*The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life.*<sup>40</sup>

The cases of *P.G. and J.H. v. United Kingdom*, *Perry v. the United Kingdom*, and *Amann v. Switzerland*<sup>41</sup> concerned the collection of data and the recording of voices captured in public

---

<sup>35</sup> Ibid., p. 5.

<sup>36</sup> Venice Commission, op. cit., 2007.

<sup>37</sup> Ibid.

<sup>38</sup> ECtHR, *P.G. and J.H. v. the United Kingdom*, application no. 44787/98, Judgment of 6 February 2001, para. 56 (“*P.G. and J.H. v. the UK*”)

<sup>39</sup> Boehm, op. cit., 2012, p. 36.

<sup>40</sup> Venice Commission, *Herbecq and the association “Ligue des droits de l'homme” v. Belgium*, applications nos. 32200/96 and 32201/96, Commission Decision of 14 January 1998, DR 92-B, p. 92

<sup>41</sup> ECtHR, *Amann v. Switzerland*, application no. 27798/95, Judgment of 16 February 2000, para. 65-66 (“*Amann v. Switzerland*”).

places. In the first case, the ECtHR reiterates the same approach as the Commission, that simple monitoring (without recording) does not interfere with Article 8. Specifically, the Court found:

*A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character.*

However, the court goes further than the Commission to distinguish between “monitoring as such” and “recording data in a systematic or permanent way even through the use of overt surveillance methods”.

In the second case, the Court refers to an interference with Article 8(1): “Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain”<sup>42</sup>, and that “the recording of the data and the systematic or permanent nature of the record may give rise to such considerations”<sup>43</sup>. Hence, from these cases, it becomes clear that if monitoring as such in public places does not raise an interference within the meaning of Article 8, the recording of visual images and sound in a systematic and permanent way even through the means of non-covert surveillance methods may create an interference with the right to private life.<sup>44</sup>

In the case of *Peck v the United Kingdom*<sup>45</sup>, the applicant did not submit that the collection of data by a CCTV-camera monitoring his movements or that the creation of a permanent record of himself amounted to an interference with his private life<sup>46</sup>, but the ECtHR considered the question of whether the disclosure or the publication of information recorded in public places by security cameras imply an interference with the right to private life. The European Court of Human Rights considered that the disclosure to the media for broadcast use was found to be a serious interference with the applicant's private life, notwithstanding that he was in a public place at the time.<sup>47</sup>

The reasoning in these cases has not yet been applied to the use of RPAS, although there are many similarities between the issues considered by the courts in the aforementioned cases and the scenarios envisaged by the use of RPAS technology in public places. It can be submitted that an application of the case law to the use of RPAS in public places may not be found to interfere with the right to private life enshrined in Article 8 of the ECHR. This is as long as a

---

<sup>42</sup> *P.G. and J.H. v. United Kingdom*, para. 56.

<sup>43</sup> *Perry v. the United Kingdom*, application no. 63737/00, Judgment of 17 July 2002, para. 38 (“*Perry v. the UK*”); *P.G. and J.H. v. the UK*, para. 56: “where photographs were taken of an applicant at a public demonstration in a public place and retained by the police in a file, the Commission found no interference with private life, giving weight to the fact that the photograph was taken and retained as a record of the demonstration and no action had been taken to identify the persons photographed on that occasion by means of data processing”.

<sup>44</sup> Venice Commission, *Opinion on video surveillance in public places by public authorities and the protection of human rights*, Council of Europe, Strasbourg, March 2007, p. 5.

<sup>45</sup> ECtHR, *Peck v. the United Kingdom*, application no. 44647/98, 28 January 2003, no. 44647/98 (“*Peck v. the UK*”); *Perry v the UK*.

<sup>46</sup> *Ibid.*

<sup>47</sup> *Peck v the UK; Perry v the UK*.

RPAS does not record information, and if the operator does not subsequently disclose the footage captured.<sup>48</sup>

The monitoring in *Peck* concerned simple and static CCTV. The operative expression here is “monitoring as such” without recording in a public place. Thus, it is likely that, depending on the scope and intrusiveness of the surveillance, some forms of monitoring by means of RPAS will, in light of *Peck*, fall outside the protective scope of Article 8 of the ECHR. However, surveillance that goes further than “monitoring *as such*”, such as monitoring carried out with high agility and/or enhanced vision capabilities such as infrared, night vision, thermal imaging or video analytics, will likely fall within the protective scope of Article 8 of the ECHR. Thus, we observe two situations where the use of RPAS in a public space may cause interference in breach of Article 8:

- (i) RPAS that monitor and record data in a systematic and permanent way, regardless of whether the surveillance is covert or overt; and
- (ii) RPAS that do not record images, but monitors a public space through “sophisticated” means.

Once an interference within the meaning of Article 8 is recognised, the Court examines whether conditions of Art. 8(2) ECHR are met and so, determines whether the infringement is justified or not. In this regard, the Court has distinguished in its case law whether the surveillance is operated for “security reasons” or for “unpredictable other reasons”.<sup>49</sup> In this regard, it results that the interference of Article 8(1) caused by the recording of information or the monitoring activities carried out by intrusive means in public places may be justified whether these surveillance activities serve “a legitimate and foreseeable purpose - security reasons” and meet Article 8(2) requirements.<sup>50</sup>

Applied in the context of RPAS technology, this jurisprudence means that when a drone is used for simple monitoring activities (without recording), there will be no interference with Article 8 rights. Conversely, when a RPAS operator either (a) monitors individuals through the means of intrusive payloads; (b) records footages; or (c) discloses information captured in public places then he/ she will be found to have interfered with the right at Article 8(1). Nevertheless, this interference may be justified if the interference is for “a legitimate and foreseeable purpose”, such as public security, and also if it meets the requirements set out at Article 8(2).<sup>51</sup>

### ***Article 8 of the ECHR case law and non-visual surveillance***

#### **a) Interception of communications – Unwanted listening**

As a new technology designed for surveillance, drones are not only able to capture sounds such as private conversations, but they can also intercept electronic communications. The ECtHR has produced a number of relevant judgments in relation to cases involving individuals who have been the subject of communication tapping by law enforcement

---

<sup>48</sup> Williams, Victoria, “Privacy Impact & the Social Aspects of Public Surveillance”, *Covert Policing Review*, London, 2008.

<sup>49</sup> Boehm, op. cit., 2012, p. 38.

<sup>50</sup> *Perry v the UK*, para. 40.

<sup>51</sup> Boehm, op.cit., 2012, p. 39.

authorities. This jurisprudence provides some guidelines on how to determine whether monitoring activities are legitimate, and thus, do not contravene Article 8 of the ECHR. The opinions of the courts in such cases may assist in the regulation of surveillance activities undertaken by drones.

Tapping is often a covert measure. As early as the 1980s, the Court found that an applicant may claim to have been the target of secret surveillance measures without having to prove it.<sup>52</sup> The applicant need only prove that there is “a reasonable likelihood” that the surveillance measures were carried out on them.<sup>53</sup> This is interesting as it implies that a citizen, the subject of drone surveillance, does not have to prove that the surveillance irrefutably occurred in order to pursue the drone operator at trial.

In *Klass v Germany*, the Court found that the existence of legislation permitting the secret monitoring of civilians by a public authority constitutes an interference with Article 8.<sup>54</sup> In addition to secret monitoring legislation, legislation allowing interception or monitoring of paper messages and workplace telephone calls or Internet usage are also considered to be in breach of Article 8(1). Furthermore, a series of surveillance implementation measures may also amount to an interference. These measures include: interception of phone communications<sup>55</sup>; or the installation of wiretapping instruments in an individual’s house or in a workplace<sup>56</sup>. Thus, although monitoring activities may be lawful under domestic legislation, surveillance activities may still be found to interfere with Article 8(1) of the ECHR.

However, the scope of the exception at Article 8(2) extends to include public authorities. In addition, the ECtHR has outlined strict standards that public authorities responsible for the surveillance measure must adhere to should they wish to rely on the exception.<sup>57</sup> For example, to be recognised “in accordance with the law” (the legality principle), public authorities must meet the following conditions:

1. There must be a legal basis for the interception of communications (general condition)
2. This legal basis has to be publicly accessible (general condition)
3. It must specify (specific conditions):
  - ✓ the nature of offences that give rise to an interception order
  - ✓ the category of persons liable to have their phone tapped
  - ✓ a limit on the duration of phone tapping
  - ✓ the procedure to be followed for examining, using and storing the data obtained
  - ✓ precautions to be taken when communicating the data to other parties
  - ✓ the circumstance under which the recordings or tapes may or must be erased
  - ✓ precautions have to be taken to protect privileged communication between attorney and client

---

<sup>52</sup> ECtHR, *Klass v. Germany*, application no. 5029/71, Judgment of 8 September 1978, para. 38 (“*Klass v. Germany*”).

<sup>53</sup> Boehm, op. cit., 2012, p. 39.

<sup>54</sup> *Klass v. Germany*, para. 41; Boehm, op. cit., 2012, p. 35.

<sup>55</sup> ECtHR, *Kopp v. Switzerland*, application no. 23224/94 Judgment of 25 March 1998 (“*Kopp v Switzerland*”).  
<sup>56</sup> *Huvig v. France*; *Valenzuela Contreras v. Spain*, application no. 27671/95, Judgment of 30 July 1998; ECtHR, *Khan v. the United Kingdom*, application no. 35394/97, Judgment of 12 May 2000 (“*Khan v. the UK*”); ECtHR, *Armstrong v. the United Kingdom*, application no. 48521/99, Judgment of 16 July 2002; ECtHR, *Chalkley v. the United Kingdom*, application no. 63831/00, Judgment of 12 June 2003; ECtHR, *Hewitson v. the United Kingdom*, application no. 50015/99, Judgment of 27 August 2003.

<sup>57</sup> The Council of Europe, “Phone Interceptions in Light of Article 8 ECHR, *ECHR Online*. <http://echr-online.com/art-8-echr/phone-interceptions-in-light-of-article-8-echr>

This jurisprudence may be applied to monitoring measures undertaken by drones to capture communications. In conformity with this jurisprudence, operators, using drones to intercept private conversations as well as electronic communications through drones, immediately interfere with Article 8(1). In practical terms, a police officer using a drone to listen the conversation between two persons suspected of belonging to an organised criminal group in a park will, as a primary step, be found to interfere with the Article 8 right. The next step would be for the police body to demonstrate that it satisfies the requirements of Art 8(2) to show that the actions of the police officer were justified.

#### b) Location surveillance

The previous chapter examined the privacy issues related to the use of drones that are fitted with certain sensors, including sensors that can read GPS tags or signals. The ECtHR has determined cases regarding location surveillance, the judgments of which are relevant to drones when they are used to monitor the movements of people and/ or vehicles.

In the case of *Uzun v Germany*, the Court examined the monitoring movement of a suspected terrorist in public places via a global positioning system (GPS) that was installed in a vehicle. The court found that this monitoring might amount to an interference under Article 8(1) of the ECHR.<sup>58</sup> In its judgment, the ECtHR established a graduation in the level of interference depending on the type of surveillance technologies used. The Court held:

*GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings.*<sup>59</sup>

However, the decision in *Uzun*'s case was based on the fact that:

*Investigation authorities have systematically collected and stored data determining the applicant's whereabouts and movements in the public sphere and the recording of personal data and the used it in order to draw up a pattern of the applicant's movements, to make further investigations and to collect additional evidence at the places the applicant had travelled to, which was later used at the criminal trial against the applicant.*<sup>60</sup>

Aside from making this distinction between surveillance technologies, the Court relevantly found that GPS devices are less intrusive than visual payloads and payloads intercepting communications. Hence, the authority responsible for an infringing act of location surveillance must prove that it ensured “a general protection against arbitrary interference” in order to justify that interference under Article 8(2).<sup>61</sup>

The Court also makes a distinction between “hard surveillance” (visual surveillance, tapping communications) and “soft surveillance” (location surveillance). Paul de Hert and Antonella Galetta, observed:

---

<sup>58</sup> ECtHR, *Uzun v. Germany*, application no. 35623/05, judgment of 2 September 2010 (“*Uzun v. Germany*”).

<sup>59</sup> *Ibid.*, pp. 16-17, para. 52.

<sup>60</sup> *Uzun v. Germany*, pp. 16-17, para. 51.

<sup>61</sup> *Uzun v. Germany*, pp.16-17, para. 66; and De Hert, Paul and Antonella Galetta, *op. cit.*, 2013, p. 34.

*the Court makes an interesting statement by making a distinction between ‘soft’ and ‘hard surveillance’. However, it would have been more pragmatic and realistic whether the Court would have established such classification on the basis of the circumstances of the surveillance (monitor, record, track, in public or private places, type of technology, type of data recorded, etc.) rather than on the type of technological device.<sup>62</sup>*

In conformity with this case law, drones fitted with a sensor able to read location data of a person or a vehicle will be found to carry out “a soft surveillance”, in its similarities with GPS technology. It follows that an operator carrying out ‘soft surveillance’ will have a greater chance of justifying that interference under article 8(2) of the ECHR, than if they conducted ‘hard surveillance’ such as visual surveillance.

#### 4.2.3 European Union Law – Article 7 CFREU

In line with the Lisbon Treaty, the provisions of the European Union Charter have “the same legal value as the Treaties” (Article 6 TEU). Article 7 of the Charter recognises the right to private life to all individuals and contains a copy of the rights guaranteed by Article 8 ECHR (Article 52(3)).<sup>63</sup> Article 7 must, therefore, receive “the same meaning and the same scope as Article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human Rights”.<sup>64</sup> We can, nonetheless, remark a difference in the phrasing of the provision: “Everyone has the right to respect for his or her private and family life, home and communications”. Taking in account the technological developments, the European Union has replaced the word “correspondence” by “communications”.

Having the same value as treaties, the Charter has direct effect in national legal systems. In other words, the citizen who’s private life has been interfered with by a private party or another individual can appear before its national courts on the basis of Article 7. Moreover, the European Court of Justice controls the implementation of this Charter and the validity of the European law in the light of the rights of the Charter.

#### 4.2.4 Conclusion

First, this section aims to identify and examine whether the European privacy legislation is applicable to RPAS technology. The ECHR and the EU Charter preserve the right to private life. Both instruments provide for a broad understanding of the right to private life. They provide European citizens the basis to appear before their national courts in defence of that right. As nothing seems prevent the application of both legal basis to RPAS technology, it follows that Article 8 ECHR as well as Article 7 EU Charter may also extend to protect citizens from any interference by commercial, private or governmental drones. However, the study of Article 8 ECHR has shown that that all privacy interferences are not condemned by the law; in some circumstances such interferences may be legally justified. Therefore, although we emphasised in the previous chapter that RPAS may pose some interference with the right of every person to enjoy of its privacy, RPAS operators could justify such interferences. For instance, the RPAS used by a police officer for tracking a criminal which

---

<sup>62</sup> De Hert Paul and Antonella Galetta, op. cit., 2013, p. 34.

<sup>63</sup> Docquir, op. cit., 2008, p. 39.

<sup>64</sup> Aidan O’Neill, “How the CJEU uses the Charter of Fundamental Rights”, *Eutopia Law*, April 2012, <http://eutopialaw.com/2012/04/03/how-the-cjeu-uses-the-charter-of-fundamental-rights/>

has captured some biometric data of citizens could be justified if its operator may prove that he acts under a legal basis, was necessary in a democratic society and be proportionate to the pursue of a legitimate aim.<sup>65</sup> However, the police will likely have more leeway in making such justifications, as the exhaustive character of the list of the legitimate aims would make it difficult for a commercial organisation to justify interfering with private life for purely commercial gains.

Secondly, as the interpretation of Article 8 ECHR and Article 7 CFEU is interpreted by the case law of the ECtHR and the ECJ respectively, we also examine if the ECtHR would have set up some relevant principles that may turn out applicable to RPAS operations. Although we observed that there does not currently exist any case law involving the civil use of drones, the ECtHR's in this comprehensive jurisprudence relating to surveillance and Article 8 encompasses some general principles, which, a priori, apply to surveillance carried out with RPAS technology. As government issued drones are ordinarily capable of carrying out different types of surveillance depending on the drones' payload, we examined cases involving incidents of visual surveillance, communication tapping, and location surveillance. Through an analysis of this jurisprudence, we draw out general principles of law that law enforcement authorities should respect when using drones in surveillance missions. Further, we also highlight that the ECtHR makes a distinction between "soft" and "hard surveillance". With reference to RPAS technology, the intensity of the surveillance will depend on the payload with which the drone is fitted. The distinction between "hard and soft surveillance" will determine whether the surveillance will amount to an interference with the right at Article 8. As to be expected, an operator using drones for hard surveillance is required to comply with more requirements in order to justify its interference than if the interference occurred in a soft surveillance context.

### **4.3 The European law on personal data protection**

#### *4.3.1 General*

The recording of images, videos, sounds, and the geo-localisation data related to an identified or identifiable natural person that has been collected and processed by data processing equipment embedded in RPAS technology is also subject to the application of European data protection law. Unlike privacy laws, personal data protection legislation exists across a breadth of instruments including international conventions, bilateral agreements, and European Union instruments, (treaties, directives, framework decisions). Due to the growing importance of data exchange and the new privacy challenges brought by the new technologies, the Council of Europe and European Union have drafted frameworks that regulate how organisations may deal with the personal data of individuals.

Data protection is a fundamental right in Europe, recognised at Article 8 of the Council of Europe Convention, and at Article 8 of the European Union Charter. In addition to those instruments, the right to data protection is preserved by a number of other subsidiary laws, such as: the Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108); the European Union

---

<sup>65</sup> A legitimate aim may be a "national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive); Directive 2002/58/EC on privacy and electronic communications (the e-Privacy Directive); and the Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (the so-called Data Protection Framework Decision).

#### 4.3.2 Council of Europe Law (Article 8 ECHR and the Convention 108)

Privacy and data protection are closely linked. The interplay between privacy and data protection is explained by Antonela Galetta and Paul De Hert:

*The protection of personal data serves the purpose of the enforcement of the right to private life. So, the infringement of the individual's right to data protection leads to a violation of the right to private life. However, a privacy infringement does not necessarily result in a violation of the right to data protection.*<sup>66</sup>

Schreurs et al. further explain:

*While, the right to private life refers to many activities of the individual's life and is unclear how it may apply to the new technologies, data protection is applicable whenever personal data are processed. Then, it consists in an objective tool to protect individuals and as a result, gives more legal certainty than privacy law.*<sup>67</sup>

Applied to the RPAS technology, this implies that the data protection right will only protect individuals when the RPAS has collected personal data. This differs from the right to privacy which protects people monitored by drones in a systematic way or through the means of intrusive payloads regardless of whether data is collected.

An initial interpretation of Article 8 by the Strasbourg Court did not explicitly recognise that Article 8(1) of the ECHR offers a protection to personal data, but rather found that “only some data protection elements could be found.”<sup>68</sup> An official link between Article 8 of the ECHR and the right of personal data was enunciated in the Court’s judgment in the cases of *M.S. v Sweden* and *S and Marper v the United Kingdom*. In those cases, the court held: “the protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to respect for private and family life as guaranteed by article 8 ECHR”.<sup>69</sup> As we have seen above with the right to private life, the ECtHR has developed jurisprudence regarding data protection rights in relation to surveillance activities carried out by public authorities. It is also accepted that the mere storage of information relating to an individual’s private life by a public authority amounts to an interference within the meaning of Article 8.<sup>70</sup> Over the

---

<sup>66</sup> De Hert and Galetta, op. cit., 2013, p. 34.

<sup>67</sup> Coudert, Fanny, citing Schreurs W, Hildebrandt M, Kindt E, Vanfleteren M. in “When Video Cameras Watch and Screen: Privacy Implications of Pattern Recognition Technology”, *Computer Law and Security Review*, Vol. 26, 2010, p. 381.

<sup>68</sup> ECtHR, *Leander v. Sweden* application no. 9248/81, Judgment of 26 March 1987, para. 48 (“*Leander v Sweden*”); *Kopp v. Switzerland*; *Amann v Switzerland*.

<sup>69</sup> ECtHR, *M.S. v Sweden*, application no. 20837/92, Judgment of 27 August 1997.

<sup>70</sup> *Leander v. Sweden*, para. 48; *Kopp v. Switzerland*; *Amann v Switzerland*.

years, the Court has considered many cases involving data protection issues and consequently, developed general data protection principles for application in such cases.<sup>71</sup>

In the second half of the 1970s, the Council of Europe recognised the wording of Article 8 of the ECHR as insufficiently covering all concerns raised by new technologies (personal data in the private sector, the trans-border data flows at the international stage, the right access to one's own data).<sup>72</sup> Several national privacy laws already existed but differences about the content and procedure were rife.<sup>73</sup> In order to remedy these concerns, the Council of Europe adopted the Convention for the Protection of individuals with regard to Automatic Processing of Personal Data (Convention 108). The Council of Europe included the data protection principles developed by the ECtHR case law in the Convention. It also added new principles which together shape the first binding European data protection instrument.

#### 4.3.3 *The Fundamental Rights Charter (Article 8) and the Lisbon Treaty (Article 16)*

The right to data protection is protected by article 8 of the Charter which also protects right of private life (Article 7 of the CFREU). That Article provides: “*everyone has the right to protection of personal data concerning him or her*”. This Charter is the first legal instrument consecrating the personal data protection as a fundamental right itself<sup>74</sup>. Indeed, contrary to the ECHR, Article 8 of the Charter provides a right of personal data protection as separate to the right of private life stipulated at Article 7. Article 8 encompasses the main data protection principles, although the right to data protection is regulated in more detail in several EU data protection instruments, including a core data protection instrument, the Data Protection Directive (96/46/EC).

The first paragraph of Article 16 of the Lisbon Treaty echoes Article 8 of the Charter, reaffirming that: “Everyone has the right to the protection of personal data concerning them”. Through this simplistic formulation, Article 16 confers explicitly a subjective right on individuals that they may invoke in national court proceedings. This Article 16 replaces and expands on the old Articles 95 and 286 of the European Community Treaty by laying down a single general legal basis for the protection of personal data for all activities undertaken within EU borders.<sup>75</sup>

#### 4.3.4 *The Data Protection Directive 95/46/EC*

##### ***Scope***

Although Viviane Reding, the Vice-President of the European Commission, has expressly confirmed the general application of the Directive 95/46/EC to the RPAS technology in a Parliamentary Question, the scope of a legal text must always be examined in detail to assess if all kinds of data processed by any type of RPAS operator fall under the applicability of such text. The Directive 95/46/EC, commonly referred to as the Data Protection Directive

---

<sup>71</sup> Boehm, op. cit., 2012, p. 81.

<sup>72</sup> Ibid.

<sup>73</sup> European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law*, Council of Europe, Strasbourg, 2013, p. 18.

<sup>74</sup> European Union Network of Independent Experts on Fundamental Rights, “Commentary of the charter of fundamental rights of the European Union”, June 2006. [http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal\\_en.pdf](http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf)

<sup>75</sup> Scirocco, Alfonso, “The Lisbon Treaty and the Protection of Personal Data in the European Union”, *dataprotectionreview.eu*, Issue 5, February 2008, p. 1.

(DPD), ensures the balance between a high level of privacy for individuals and the free movement of personal data within the European Union (Recital 3). Unlike the right to private life, the distinctions between public and private and recorded data and non-recorded monitoring do not play any role with regard to the applicability of data protection. The only real bottleneck for the applicability of data protection is formally stipulated in the Directive that provides:

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

The concept of “automated processing” is *a priori* broad enough to include payloads (CCTV, RFID, microphone, etc.) fitted to RPAS technology. The concept of “personal data” is more complex. It is defined at Article 2 of the Directive as: “any information – including sound and images – concerning an identified or identifiable<sup>76</sup> person natural person (excluding the legal persons’ data)”<sup>77</sup>. However, this definition being too vague and not pragmatic, the Article 29 Working Party issued an Opinion on the concept of personal data to provide a common understanding of what is meant by personal data protection: “Personal data shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly,...”<sup>78</sup> Firstly, the Art. 29WP explains that the DPD applies to image and sound data processed by means of CCTV and other video surveillance systems. Relevantly, biometric data, location data, and traffic data are also generally considered to be personal data.<sup>79</sup> Secondly, it also states “Image and sound data relate to *identified or identifiable* nature person is personal data: a) even if they are not associated with a person’s particulars, b) even if they do not concern individuals whose faces have been filmed, c) irrespective of the media used”<sup>80</sup> Thirdly, the Art.29 WP gives more detail on what it means by “identify someone indirectly”. It explains that every day it is easier to connect different data together to identify someone through the new analytical systems, and the scope of the Directive concerns all personal data which are indirectly identifiable by “all the means likely reasonably to be used”.<sup>81</sup> By saying that it takes into account of the possibilities of future technologies but also it narrows the broad concept of

---

<sup>76</sup> *In cases where prima facie the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be “identifiable” because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others: Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Brussels, 20 June 2007,*

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf) (“A29WP Opinion 4/2007”).

<sup>77</sup> The Article 29 Working Party has issued a more elaborate interpretation of the concept of “personal data”, and has identified a number of criteria that must be met for information to amount to “personal data”.

<sup>78</sup> A29WP Opinion 4/2007.

<sup>79</sup> Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN, WP193, Brussels, 27 April 2012. [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf) (“A29WP Opinion 3/2012”); Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 819/14/EN, WP 215, Brussels, 10 April 2014.

[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf) (“A29WP Opinion 04/2014”).

<sup>80</sup> A29WP Opinion 4/2007.

<sup>81</sup> Kindt, Els J., *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, Springer, 2013, Dordrecht, pp. 112-113.

personal data. Therefore, for instance if the footage taken by a drone only shows the overhead of a person and that you cannot identify it without using sophisticated means, it is not a personal data. However, the same photograph taken in the backyard of a house of which you may easily identify the owner would be considered as a personal data.

Furthermore, whereas the DPD concerns public entities as well as private companies, some type of data collectors are explicitly excluded from the scope of the Directive. First, the Directive does not apply to the processing of data carried out by States authorities in the area of criminal law<sup>82</sup> and/or for purposes of maintaining public order, defence and State security<sup>83</sup>. Therefore, the Directive is not applicable to personal data collected by law enforcement authorities via RPAS technology. In this regard, drones used by governmental agencies that collect images identifying people during a major event for state security and public safety will not be subject to the provisions of the Directive. However, this does not necessarily mean that such agencies should not attempt to comply with the requirements set out in the jurisprudence relating to Article 8 ECHR and 7 CFREU<sup>84</sup>.

Second, data collected by a natural person in the course of purely personal or household activities falls outside the scope of the Directive. The ECJ explains the meaning of this exception in its judgment in the case of *Linqvist*:

*That exception must be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people.*<sup>85</sup>

Therefore, an individual who captures personal information through the means of a civil drone and, subsequently, publishes or transmits that data to an indefinite number of people will be not exempted from the provisions of the Directive.

Further, the Article 29 Working Party has developed some guidelines on how to interpret this exclusion in cases of visual-surveillance. The Article 29 Working Party distinguishes between two situations.<sup>86</sup> The first situation involves video surveillance of the inside of private residences in the prevention of theft, or in connection with management of the so-called e-family. The second situation envisaged by the Court to fall outside of the scope of the

---

<sup>82</sup> De Hert and Gutwirth, "Anthologie de la vie Privée", *ASP*, 2013, p. 14.

<sup>83</sup> Data processing in defense, State security, investigation and prosecution of criminal offences (criminal procedural law) is a national prerogative, and the Member States have sole competence to regulate these areas. However, the processing of data carried out in the context of police and judicial cooperation (area of the former third pillar) is part of the European competence and since the entry into force of the Lisbon Treaty and the abolition of the former pillars structure, these areas may be subject to the Directive. However, President of the EDPS, Peter Hustinx, emphasised that "The entry into force of the Lisbon Treaty leads to the end of the pillar structure, but that does not mean that Directive 95/46 will automatically apply to police and judicial cooperation. The scope of this Directive is limited. It now excludes activities of the State in the area of criminal law. Only a precise amendment of the Directive on that point could change this situation"<sup>83</sup>. Nonetheless, it should be observed that some domestic legislation applies to the principles of the Directive to the police sphere as well<sup>83</sup>.

<sup>84</sup> Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, 11750/02/EN, WP 89, Brussels, February 2004, p. 13.  
[https://www.apda.ad/system/files/wp89\\_en.pdf](https://www.apda.ad/system/files/wp89_en.pdf) ("A29WP Opinion 4/2004").

<sup>85</sup> European Court of Justice, *Bodil Linqvist*, application no. C-101/01, Judgment of 6 November 2013.

<sup>86</sup> A29WP Opinion 4/2004, p. 14.

Directive is when video surveillance equipment is installed either outside or close to private premises with a view to protecting property and/or ensuring security. However, the applicability of the Directive is less clear as it will depend on whether the system is deployed for the sole benefit of an individual family. If so, the Directive will not apply. However, in the case where “the surveillance system is deployed by several owners on the basis of an agreement in order to monitor several entrances and areas in a tenement”, the Directive will be applicable.<sup>87</sup> By analogy, we can, expect that civil RPAS used by an individual to monitor their own property including its home and premises will not fall under the directive contrary to RPAS operated by a Village Committee deciding to monitor several unsecured areas of its village.

Third, Article 9 of the Directive foresees that “Member States shall provide for exemptions or derogations from some of its provisions where processing is carried out solely for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audio-visual field” (see also recital 17). This partial exemption has for aim to balance the right to private life with the right to freedom of expression. Hence, it does not give “an automatic blanket exemption in every case, it is only intended to apply where it is “necessary to reconcile the right to privacy with the rules governing freedom of expression”.<sup>88</sup> Notably, the ECJ, in *Satamedia*, has given a broad interpretation to the phrasing “for purposes of journalism” as intending to cover the disclosure to the public of information, opinions or ideas by any means.<sup>89</sup> Civil drones are often used by journalists or in audio-visual fields and thus, this exemption ought to be applied with precaution. If it is not applied in such a way, we risk living under “a sky of paparazzi-drones”. An Opinion of the Article 29 Working Party on this subject is certainly something to look forward to.

### ***Common Core Principles***

The Data Protection Directive encompasses a number of principles for the processing of personal data. These data protection standards include several general principles commonly recognised as the “data protection principles”. These principles, at Articles 6 and 7 of the Directive, are related to data quality, with the second set of principles relating to the quality of processing. Article 6 (1) of the Directive provides:

Personal data must be:

- (a) processed fairly and lawfully (*lawfulness and fairness principles*);
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (*purpose limitation principle*);
- (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (*proportionality and data minimisation principles*);
- (d) accurate and, where necessary, kept up to data (*data quality principle*);

---

<sup>87</sup> Ibid.

<sup>88</sup> Information Commissioner's Office, *Data protection and Journalism: A Guide for the Media. Draft for Consultation*, Information Commissioner's Office, Cheshire, United Kingdom, 2014, p. 9.

<sup>89</sup> European Court of Justice, *Satamedia*, Judgment of 16 December 2008; Information Commissioner's Office, op. cit., 2014.

- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed (*retention principle*).<sup>90</sup>

### ***Purpose limitation and proportionality principles***

Purpose limitation principle, also called finality principle, imposes two obligations on the collector, namely that collector specify the purpose of the collection and process the data collected only for purposes compatible with that collection.<sup>91</sup> So, prior to collecting the data, the collector must determine which legitimate purposes they will collect data for. The next step is to ensure that the further processing of the data collected be for the purpose they initially specified, or at the very least, be processed for compatible purposes.<sup>92</sup> For example, an energy company may use a commercial RPAS equipped with a GPS sensor and a thermal camera to film the roofs of several residential areas. The information collected from the GPS and the thermal camera enables the energy provider to match this information with customers' addresses and subsequently, offers them discounted roof insulation. When applying the finality principle to this example, one would examine the initial purpose for the collection against the purpose of the further processing of the collected data. If the energy company is found to be processing the collected data for incompatible purposes, such as selling the information to insurance companies, then it will be in breach of the finality principle.

The proportionality and data minimisation principles are related to the finality principle as they require the data controller to hold only personal data that are "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed". Whereas the proportionality principle obliges the data controller to process an amount of data in proportion to the scope pursued; the data minimisation principle goes as far as to require the collector to use the least intrusive technological means of collecting the minimum amount of data necessary for the purposes pursued. For example, a marketing company films in pedestrian shopping streets to observe the impact of advertising posters by filming the correlation between the viewers and the buyers. In accordance with data minimisation principle, the collector could obtain that information through less intrusive means than RPAS technology. A minimalistic approach would see the advertising company conduct a survey amongst buyers to ascertain whether they were influenced by the advertising material. This approach would raise fewer privacy issues than the issues raised when RPAS technology is utilised.

### ***Admissibility or lawfulness principle***

The admissibility principle is also relevant to potential data protection issues arising in relation to the civil use of drones. The processing of personal data must be legitimate, and thus, processed only in the following circumstances:

---

<sup>90</sup> European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995 ("Directive 95/46/EC"), Article 6.

<sup>91</sup> Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN, WP 203, Brussels, 2 April 2013, pp. 4-5. [http://idpc.gov.mt/dbfile.aspx/Opinion3\\_2013.pdf](http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf) ("A29WP Opinion 03/2013").

<sup>92</sup> Ibid.

- (a) the subject concerned has given his consent or whether the processing is necessary;  
or
- (b) the performance of a contract to which the data subject is party; or
- (c) the compliance with a legal obligation to which the controller is subject; or
- (d) in order to protect the vital interests of the data subject; or
- (e) for the performance of a task carried out in the public interest; or
- (f) for the purposes of the legitimate interests pursued by the controller.<sup>93</sup>

The degree of consent required here is that of explicit, and that it is unambiguous and based on clear-cut information.<sup>94</sup> Consent is considered “one of the most important safeguards against data protection threats and the unlawful exercise of surveillance power”.<sup>95</sup> The Article 29 Working Party issued an *Opinion* that touched on the issue of consent: “consent will have to be provided separately and specifically in connection with surveillance activities concerning premises where a person’s private life is led”.<sup>96</sup> It is clear that consent is often essential to ensure that surveillance activities are carried out lawfully. However, there is much debate as to the issue of consent, and the weight given to consent requirement is blurred somewhat by the number of instances outlined at Article 7 of the Directive where consent is not required. This uncertainty is reinforced by the fact that the primary method of surveillance, video-surveillance, can be undertaken without the requirement of explicit consent being obtained, but rather, in those situations, consent is deemed to have been implied by the action of an individual entering a public space.<sup>97</sup>

Nevertheless, in most cases, commercial organisations operating drones will need either the consent of the individual data subject or another valid legal basis for the surveillance, such as a contractual arrangement.

### ***Special categories of data***

Article 8 of the Directive outlines the principle of confidentiality in relation to the “sensitive data”. With its objective of abating discrimination, this provision outlines a non-exhaustive list of the types of data that cannot be processed:

*Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.*<sup>98</sup>

However, data subject’s consent can legitimise the processing of this sensitive data. However, the standard of consent required for the processing of sensitive data is higher than the general

---

<sup>93</sup> Directive 95/46/EC, Article 7; De Hert and Gutwirth, op. cit., 2013, p. 14.

<sup>94</sup> De Hert and Galetta, op. cit., 2013, p. 39; A29WP Opinion 4/2004, p. 18.

<sup>95</sup> De Hert and Galetta, op. cit., 2013, p. 39.

<sup>96</sup> A29WP Opinion 4/2004, p. 18.

<sup>97</sup> Gras, Marianne L., “The Legal Regulation of CCTV in Europe”, *Surveillance and Society Review*, Vol. 2 No. 3, 2004.

<sup>98</sup> Directive 95/46/EC, Article 8.

standard of consent as it must be “explicit” consent.<sup>99</sup> RPAS mounted with biometric sensors collect much sensitive data in the form of biometric data (fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent)<sup>100</sup> would require the data subject’s explicit consent for that collection to be lawful.

### ***Transparency obligation (information, notification and prior-checking)***

The transparency principle requires that the data collector notify the data subject of the personal information collected, as well as notifying the relevant Data Protection Authority (DPA). Article 10 and 11 of the Directive imposes a duty on the data collector whenever data is obtained from the data subject, or from any other means. Furthermore, Article 18 of the Directive requires that all controllers processing data notify the supervisory authority concerned before the data is processed. Once the relevant DPA has been notified, the DPA will assess whether the proposed processing is likely to present specific risks to the rights and freedoms of data subjects.<sup>101</sup> This process may result in “processing operations being prohibited, in an order to change features in the proposed design of the processing operations”<sup>102</sup>, or in a new obligation being imposed on the data controller such as additional safeguards specified by the DPA. A register of processing operations is held in this regard. As some RPAS capabilities and applications may be regarded as privacy intrusive, we wonder whether DPAs should automatically assess the risk related to the data processing resulting from drone collection.

### ***The individual’s rights***

Besides the right to be informed of the processing of one’s personal data, the Directive provides for additional means of safeguarding data protection rights:

- The Directive recognises a right of access to data and a right to rectification for the data subject. Effectively this gives data subjects a right of access to the information collected and stored about them, as well as the opportunity to change incorrect information held about them. The data subject is entitled to know the origin of the data and the purpose for which the data are collected.<sup>103</sup>
- The Directive contains also a right to judicial remedy, a right to erasure and a right to block the data processing in some exceptional cases.<sup>104</sup> Concerning this right to block<sup>105</sup>, the Directive provides that the citizen concerned can oppose on compelling legitimate grounds relating to his particular situation to the processing of data relating to him. It can also rely on this right to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates processing for the purposes of direct marketing.

---

<sup>99</sup> Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 01197/11/EN, WP187, Brussels, July 2011, p. 6.

[http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf)

<sup>100</sup> A29WP Opinion 3/2012, pp. 3, 15.

<sup>101</sup> “National law must determine which processing operations qualify for prior checking”: European Union Agency for Fundamental Rights, *Handbook on European data protection law*, Council of Europe, Strasbourg, 2013, p. 104.

<sup>102</sup> Ibid.

<sup>103</sup> Directive 95/46/EC, Article 12.

<sup>104</sup> Ibid.

<sup>105</sup> Directive 95/46/EC, Article 14.

- The Directive also requires that data subjects be informed before their personal data are disclosed to third parties for the purposes of direct marketing and be expressly offered the right to object.<sup>106</sup>

However, the Directive stipulates exemptions to these rules. The main exemption to the rules proscribed by the Directive relates to data that is used to safeguard matters of national security, defence, public security, the prosecution of criminal offences, is relevant to an important economic or financial interest of a Member State or of the European Union, and/ or is necessary for the protection of the individual concerned.<sup>107</sup> Further, the Directive stipulates the importance of taking secure technological measures to protect the personal data collected. Should the controller be found to be in contravention of the Directive, it may be ordered to pay compensation to the data subject in the event of damage caused by unlawful or unauthorised processing of data.<sup>108</sup>

When we consider the civil use of RPAS technology, the right to access, and the right to block or object form the legal basis for data subjects to retain some control over their personal information collected by the use of those technologies. Citizens may well rely on these rights to prohibit the processing of personal data captured by RPAS, but also control the subsequent use and processing of that data.

### ***Data Transfer to Third Countries***

Under the Chapter IV, the Directive establishes a regime for the transfer of data outside the European Union.<sup>109</sup> Prior to sending personal data to third countries, the controller must ensure that the third country receiving the data provides adequate protection for the data transferred. The data controller must therefore assess the data protection regime of a third country before a transfer is made.<sup>110</sup> The controller can transmit data to third states that ensure “an adequate level of protection”, unless any of the exceptions exhaustively enumerated in the Directive apply.

### ***National and European Data Protection Authorities***

Finally, the Directive establishes European and national supervisory authorities. At the EU level, the Directive provides for an Article 29 Working Party to deal with issues relating to privacy and data protection.<sup>111</sup> Its main role is to examine measures taken by the Member States in accordance with the provisions of the directive in order to achieve the uniform application of these provisions. At the domestic level, each Member State has established one or more supervisory authorities in charge of the application of the Directive.<sup>112</sup>

---

<sup>106</sup> Directive 95/46/EC, Article 14; De Hert and Gutwirth, op. cit., 2013, p. 15.

<sup>107</sup> Directive 95/46/EC, Article 13; De Hert and Gutwirth, op. cit., 2013, p. 15.

<sup>108</sup> Directive 95/46/EC, Article 23.

<sup>109</sup> Directive 95/46/EC, Article 25.

<sup>110</sup> Directive 95/46/EC, Article 25; De Hert and Gutwirth, op. cit., 2013, p. 15.

<sup>111</sup> Directive 95/46/EC, Article 29; De Hert and Gutwirth, op. cit., 2013, p. 15.

<sup>112</sup> Directive 95/46/EC, Article 28.

### 4.3.5 *The Proposed General Data Protection Regulation*

The Directive is currently under review and will likely be replaced by its successor, the Proposed General Data Protection Regulation (GDPR)<sup>113</sup>. The proposed regulation does not provide for RPAS-specific regulations. However, some of the new provisions suggested could be relevant to address the potential data protection concerns related to the use of RPAS as it aims to provide for “a single set of rules technologically neutral - regardless how technology and the digital environment develop in the future”.<sup>114</sup> Notably, other proposals have been drafted by the Working Party on Information Exchange and Data Protection (DAPIX)<sup>115</sup>, and the Committee for Civil Liberties, Justice and Home Affairs of the European Parliament (LIBE)<sup>116</sup>. The analysis of these proposals and other proposed aspects contained within the GDPR fall outside the scope of this deliverable. This report focuses only on the study of the new provisions that are likely applicable to the civil use of drones in the European airspace.

#### ***Privacy (Data Protection) by Design and by Default***

Proposed Article 23 enshrined two principles, Data Protection by Design and Data Protection by Default<sup>117</sup>:

- The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures (Privacy by Design principle)
- The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. (Privacy by Default principle)

The Privacy by Design (PBD) and Privacy by Default principles are concerned specifically with regulating types of information and communication technology (ICT), thereby contributing to an overall more effective data protection framework.<sup>118</sup>

---

<sup>113</sup> 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”), 2012/0011 (COD), 25.01.2012.

<sup>114</sup> European Commission, “How will the EU’s Reform Adapt Data Protection Rules to New Technological Developments?”, *Europa*, 2012.  
[http://ec.europa.eu/justice/dataprotection/document/review2012/factsheets/8\\_en.pdf](http://ec.europa.eu/justice/dataprotection/document/review2012/factsheets/8_en.pdf)

<sup>115</sup> Working Party on Information Exchange and Data Protection, 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, 2012/0011 (COD), 22.06.2012.

<sup>116</sup> Committee for Civil Liberties, Justice and Home Affairs of the European Parliament, Draft European Parliament Legislative Resolution on the 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)0011 – C7-0025/2012 – 2012/0011(COD)), 22.11.2013.

<sup>117</sup> In reality, the Privacy by Design concept is not a new concept as Article 17 and Recital 46 of Directive 95/46/EC alluded to the implementation of this principle. Specifically, Article 17 provides: “[...]data controller must implement appropriate technical and organisational measures[...]”. However, Article 17 and Recital 46 are thought to be vague, broad provisions that are mostly not implemented by companies.

The *Data Protection by Design principle* entails embedding privacy-protective technologies and policies, from design stage and deployment activities, to use and final disposal.<sup>119</sup> In data protection, this principle should “ensure that at the end of the process, all data are securely destroyed, in a timely fashion”.<sup>120</sup> The purpose behind this principle is that manufacture and design companies are made responsible for the potential privacy impacts of their devices and are not only motivated by the profit. Ann Cavoukian, the developer of the PbD approach, explains the *unique preventive and pro-active features* of her theory when she states “Build in privacy from the outset has been my longstanding mantra, to avoid making costly mistakes later on, requiring expensive retrofits”.<sup>121</sup>

In its proposal, the European Commission has also included the Privacy by Default principle. *Data Protection by Default* refers to the “data minimization principle” and imposes to companies to implement this latter through mechanisms inherent to the technology of its product. Hence,:

*when a data collector/user receives a product or service, privacy settings should be as strict as possible, without the user having to change them. This way, everyone is guaranteed a high level of protection, allowing everyone the opportunity to consciously choose the privacy setting that they feel most comfortable with – rather than the service provider making a guess about what they might prefer.*<sup>122</sup>

The Article 29 Working Party recently commented that the application of the PbD principle to the engineering of RPAS technology could contribute to a better respect for privacy and data protection.<sup>123</sup> In that regard, the Article 29 Working Party states:

*In case of use of RPAS equipped with video cameras, video anonymisation or other technical arrangements could be implemented by controllers to automatically process the images by using blurring or other graphical effects so as to prevent images of identifiable persons from being collected whenever they are not necessary. Depending on the purposes of the use of RPAS, the images could be encrypted*

---

<sup>118</sup> Hustinx, Peter, “Le concept de Privacy by Design: Un Remède à L’insuffisance des Moyens Actuels de Protection de la vie Privée”. <http://www.e-juristes.org/le-concept-de-privacy-by-design-un-remede-a-linsuffisance-des-moyens-actuels-de-protection-de-la-vie-privee/>

<sup>119</sup> Cavoukian, Ann, “Privacy by Design in Law, Policy and Practice A White Paper for Regulators, Decision-makers and Policy-makers”, *Information and Privacy Commissioner*, Canada, August 2011, p. 3. <http://www.ipc.on.ca/images/Resources/pbd-law-policy.pdf>. See also European Data Protection Supervisor, Opinion on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, Brussels, 18.03.2010, pp. 4-6.

<sup>120</sup> Security Breaches Administrator, “Implementation of Privacy by Design and Technical and Organisational Security Measures: The Data Masking Solution”, *Information Security Breaches & The Law Blog*, 26 June 2012. [http://blog.security-breaches.com/2012/06/26/implementation\\_of\\_privacy\\_by\\_design\\_and\\_technical\\_and\\_organizational\\_security\\_measures\\_the\\_data\\_masking\\_solution/](http://blog.security-breaches.com/2012/06/26/implementation_of_privacy_by_design_and_technical_and_organizational_security_measures_the_data_masking_solution/)

<sup>121</sup> Cavoukian, op. cit., 2011, p. 3.

<sup>122</sup> EDRI, “An Introduction to Data Protection”, *The EDRI Papers*, Issue 6, Brussels; Danagher, L., “An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data?”, *European Journal of Law and Technology*, Vol. 3, No. 3, 2012; Schwaab, Jean Christophe, “Privacy by Design / by Default – Inverser la logique de Protection des Données en Faveur des Utilisateurs”, *Jean Christophe Schwaab Online*, September 2013. <http://www.schwaab.ch/archives/2013/09/26/privacy-by-design-by-default-inverser-la-logique-de-protection-des-donnees-en-faveur-des-utilisateurs/>

<sup>123</sup> Wong, Rebecca, “The Future of Privacy”, *Computer Law and Security Review*, 2010, p.3.

*immediately they are collected and decrypted only when necessary and made accessible to authorized personnel only.*<sup>124</sup>

Blurred images or data masking are kind of PbD measures that privacy professionals could implement in RPAS companies.<sup>125</sup>

### ***Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA)***

The Privacy Impact Assessment, together with the Privacy by Design and Privacy by Default principles are included in the Draft Regulation alongside a new accountability imposed on the collectors, and the implicit Lifecycle Data Protection Management obligation imposed on industries. In fact, the proposed Regulation makes clear that in practice, these concepts are also targeted at engineers, industry and public authorities to hold them accountable for their role in technological innovations that raise privacy and data protection concerns<sup>126</sup>.

PIA is not defined in the Draft Regulation, however some guidance is offered by Paul De Hert, David Wright and Vagelis Papakonstantinou who define the Data Protection Impact Assessment as: “a systematic process for evaluating the potential effects on privacy and data protection of a project, initiative, proposed system or scheme and finding ways to mitigate or avoid any adverse effects”.<sup>127</sup> Expressly acknowledged in Article 33 of the Draft Regulation, the impact assessment mechanism requires the controller or the processor to carry out an assessment of the impact of the processing operations on the protection of personal data when these operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope of their purpose.<sup>128</sup> In other words, the collectors are responsible for the decision as to whether their processing meets the requirements of the regulation by conducting a DPIA before dealing with personal data. A DPIA must be made “easily accessible to the public”.<sup>129</sup> Furthermore, where results of a DPIA “indicate a high degree of specific risks”, collectors are required to obtain an authorisation through a mandatory consultation with the data protection officer or the supervisory authority concerned. This process builds upon the prior checking requirement at Article 20 of the current Directive 95/46/EC.<sup>130</sup>

Researchers, lawyers, and policy makers working in the field of data protection have welcomed PIA and PbD in the context of drones. As discussed in the previous chapter, the main problem with the drone technology from a privacy and data protection perspective is that the enforcement of data protection and privacy rules is difficult to achieve. Therefore, “if privacy is built in from the beginning, function does not have to be compromised by privacy concerns, and vice versa”.<sup>131</sup> Dr. Ann Cavoukian, the Information and Privacy Commissioner

---

<sup>124</sup> Article 29 Data Protection Working Party, Remotely Piloted Aircraft Systems (RPAS) – Response to the Questionnaire, European Commission, Brussels, December 2013, p. 3.

<sup>125</sup> Security Breaches Administrator, op. cit., 2012.

<sup>126</sup> Cavoukian, op. cit., 2011, p. 26.

<sup>127</sup> De Hert, Paul and Vagelis, Papakonstantinou, “The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals”, *Computer Law and Security Review*, Volume 28, Issue 2, April 2012, p. 140; Wright, David, “Should Privacy Impact Assessments be Mandatory?”, *Communications of ACM*, July 2011; Wright, David and Paul De Hert, “Privacy Impact Assessment”, *Law, Governance and Technology Series*, Vol. 6, Dordrecht, Springer, 2012, p. 523.

<sup>128</sup> General Data Protection Regulation, Article 33.

<sup>129</sup> De Hert and Papakonstantinou, op. cit., 2012, p. 140.

<sup>130</sup> General Data Protection Regulation, Article 34(2).

<sup>131</sup> Canton, David, “Drones Offer Whole New Candid Camera”, *HP Blog*, 2012.

of Ontario and creator of the Privacy by Design concept, has issued a report explaining how PbD and PIA mechanisms are the best solution to prevent the privacy risks associated with RPAS technology<sup>132</sup>. In relation to PIA, she states:

*PIAs provide a number of benefits to organizations considering making use of UAVs: They are a means of enhancing informed policy decision-making and system design; they anticipate the public's possible privacy concerns; they generate confidence that privacy objectives are being considered.*<sup>133</sup>

The Privacy by Design mechanism applied to drones and payload development would see the introduction of privacy features at the engineering stage of civil RPAS. This approach would reduce the risk of personal data breaches and would promote innovation as the responsibility of the manufacturers.

### ***Code of conducts and certification mechanisms***

According to Article 38 of the Draft Regulation, supervisory authorities shall encourage controllers, associations and other related bodies in the drawing up of codes of conduct that embody the data protection principles of the Directive.<sup>134</sup> Article 39 encourages companies to obtain certification for their data processing activities from a supervisory authority. In its clarification of the certification mechanism, the LIBE Committee suggests that certification would be valid for up to 5 years, and that a public register of valid and invalid certificates be maintained.<sup>135</sup> Finally, it encourages certification processors by offering incentives, such as (i) offering a lawful basis for transferring the data if the accredited company is located in a third country (Article 42.2.aa), or (ii) not being subject to fines unless the breach is intentional or negligent<sup>136</sup>.

These “soft regulatory mechanisms” are viewed as reducing the privacy and data protection threats associated with civil drone usage, and they have been recommended by many data protection experts.<sup>137</sup> Finally, many other new provisions of the GDPR will strengthen data protection, particularly the individual right to erasure, the transparency principle, and the data breach principle. In this regard, we can expect that the potential data protection threats that civil RPAS make to the European citizens will be proportionally reduced.

---

<http://harrisonpensa.com/drones-offer-candid-camera>.

<sup>132</sup> Cavoukian, op. cit., 2011.

<sup>133</sup> Ibid., p. 16.

<sup>134</sup> General Data Protection Regulation, Article 38; Mole, Ariane, Ruth Boardman and Gabriel Voisin, “EU Data Protection Regulation: One Step Forward”, *Bird&Bird Online*, 22 October 2013.

<https://www.twobirds.com/en/news/articles/2013/global/libe-committee-of-the-euro-parliament-votes-on-compromise-amendments-to-the-draft>

<sup>135</sup> Ibid.

<sup>136</sup> Committee for Civil Liberties, Justice and Home Affairs of the European Parliament, op. cit., 2013; Mole, et al., op. cit., 2013.

<sup>137</sup> Among others, Roger Clarke, Ann Cavoukian, Catherine Crump and Jay Stanley.

#### 4.3.6 *The Framework-decision 2008/977/JHA*<sup>138</sup>

As discussed above, law enforcement agencies are also using RPAS for capturing information in the context of surveillance programs or for other purposes. Nevertheless, we have observed that the scope of the Directive 95/46/EC explicitly excludes the data processing operated in the framework of law enforcement activities. Instead, the European data protection text that regulates the processing of personal data exercised within the remit of the police and the judiciary in their cooperation on criminal matters is the Framework-Decision 2008/977/JHA. The collection of data relating to this cooperation serves the purpose of crime prevention, carrying out investigations, and in the detection or prosecution of criminal offences, and/or the execution of criminal penalties.<sup>139</sup> Thus, the FDPJ applies to the security-related processing expressly excluded from the DPD. Nevertheless, this data protection text only applies to the European and International cross-border exchanges of personal data and not to the internal processing of the Member States in police and criminal matters.<sup>140</sup>

Regarding to the RPAS technology, the European Commission has confirmed its applicability to data processed via such technology. However, given its restricted scope, situations where government-operated drones fall under its application will be rare. In a nutshell, the FDPJ only applies to data processing that is executed by governmental drones and operated by police and intelligence services in a police or judicial cooperation. Furthermore, to fall within the scope of the FDPJ, the information captured by a law enforcement authority's drone needs to have taken place in one Member State and transmit the collected information to the law enforcement authority of another Member State/third State. Hence, the EU law does not provide data protection to information captured by governmental drones in the context of law enforcement activities when the information does not take place in a European or International cooperation.

#### ***Rights and obligations***

The content of the FDPJ reflects a copy and paste of the data protection principles<sup>141</sup>, and individual rights<sup>142</sup> provided by the Data Protection Directive, with the exception that these principles are mitigated by more derogations and exempted clauses that are particularly due to the pro-security context in which the DPFD has been enacted.<sup>143</sup> For instance, the purpose limitation principle may be easier to set aside given the numerous derogations the FDPJ provided.<sup>144</sup> Regarding the transfer of personal data to third countries, police operators of drones who would transfer information they collect to third-countries or other International Organisations, will have to satisfy the same additional requirement as the DPD, namely an “adequacy of protection of the data protection regime of the third country”.<sup>145</sup> Given the rarity of situations where this text will apply to governmental drones used by the police, and given

---

<sup>138</sup> European Council, Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 27.11.2008 (“Framework Decision 2008/977/JHA”).

<sup>139</sup> Framework Decision 2008/977/JHA, Article 1.

<sup>140</sup> Ibid.

<sup>141</sup> Framework Decision 2008/977/JHA, Article 3.

<sup>142</sup> Framework Decision 2008/977/JHA, Article 4.

<sup>143</sup> Notably, the Framework-Decision 2008/977/JHA was adopted in the aftermath of the 11 September 2001 and has been heavily criticized due to its emphasis on security rather than data protection.

<sup>144</sup> Framework Decision 2008/977/JHA, Article 3(2).

<sup>145</sup> Framework Decision 2008/977/JHA, Article 13.

the similarity of the principles with those stipulated in the DPD, we not undertake any further examination of this data protection text.

#### 4.3.7 *The Proposed Directive regulating data protection in the law enforcement sector*

The proposed Directive, unlike to the current FDPJ, anticipates application to both purely domestic and cross-border data processing<sup>146</sup>, and ultimately aims to strengthen the data protection rules and principles relating to profiling technologies. In the near future, law enforcement authorities using governmental drones for collecting personal information in a police or judicial cooperation context will be subject to this Directive. Therefore, the processing of data operated by a Belgian governmental drone, which takes place in a purely Belgian judicial or police cooperation context, shall be also subject to the future Directive.

#### 4.3.8 *The e-Privacy Directive*

In the previous chapter, we have seen that domestic RPAS will also be used to carry communication systems and provide network services (replacing proxy-satellites).<sup>147</sup> Besides these telecommunication services, they also have the potentiality to intercept communication or communication data, an interesting tool of surveillance for law enforcement agencies. Although these scenarios are expected to be less frequent, it is relevant to touch on the data protection provisions that will regulate this type of processing. In the telecommunications sector, a sector specific harmonisation directive complements the general data protection directive 95/46/EC. This sector-specific Directive is Directive 2002/58/EC on Privacy and Electronic Communications, more commonly referred to as the “e-Privacy Directive”.

##### *Scope*

The e-Privacy Directive is the successor to the Telecommunications Privacy Directive (Directive 1997/66/EC). Hence, this directive applies to the processing of personal data collected by providers of publicly available electronic communications services or of a public communications network in the European Union (Article 3). Similar to the DPD, the e-privacy Directive does not apply to data processed for security and law enforcement purposes.<sup>148</sup> It regulates the processing of “communications”, “traffic” and “location data”<sup>149</sup> (“traffic data” being the data necessary for the provision of communications, and “location data” being the data giving the geographic position of terminal equipment), as well as unsolicited communications (“spam”), spyware and cookies<sup>150</sup>. The scope of the *e-Privacy*

---

<sup>146</sup> European Parliament and European Council, Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10, 25.01.2012, Article 3.

<sup>147</sup> Facebook has recently declared its plans to use drones as proxy satellites to provide Internet access in the regions which still do not have access.

<sup>148</sup> European Parliament and Council, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [2000/0189/COD](#), 12.07.2002, Article 1(3) (“ePrivacy Directive”).

<sup>149</sup> Such location data concerns the localization information about a call. Therefore, the collection of location data by a GPS attached to a RPAS falls outside the ePrivacy Directive as it only applies to the public communications sector.

<sup>150</sup> ePrivacy Directive, Article 2; Privacy International, “Privacy and data protection in the EU-Overview of the legal and institutional framework”, *Privacy International online*, no date. <https://www.privacyinternational.org>

Directive should be extended to telecommunication and network providers using drones to carry communications and provide Internet services.

### ***Confidentiality of the communications and related data***

Articles 5, 6 and 9 of the e-Privacy Directive requires that:

- Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1).<sup>151</sup>
- Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.<sup>152</sup>
- Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.<sup>153</sup>

These articles provide two principles, the confidentiality and anonymisation principles. Whereas the providers have to ensure the confidentiality of the content of the communications and their related data, he also has to anonymised traffic data (after the processing) and location data (prior the processing).

However, Article 15 provides an exception to the confidentiality and annomysation principles. These latter do not apply if the surveillance of communications “constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e., State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system”. This article makes a direct reference to the retention of data for national security and criminal investigation purposes (Data Retention Directive).

Under these considerations, it makes clear that the interception of electronic communications and related data (traffic and location data) by an operator of civil RPAS shall be strictly prohibited, unless the consent is obtained from the user of the communication. Nonetheless, it seems that surveillance of communications and related data exercised by governmental drones in a law enforcement mission may be recognised lawful if that activity satisfies the grounds for lawfulness proscribed by Article 15.

---

<sup>151</sup> ePrivacy Directive, Article 5.

<sup>152</sup> Ibid., Article 6.

<sup>153</sup> ePrivacy Directive, Article 9.

### ***Security requirements - Appropriate technical and organisational measures***

Article 4 (1) provides that

The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

By requiring that “the provider of a publicly available electronic communications service must take appropriate technical and organisational measures”, the e-Privacy Directive enshrined “the Privacy by Design principle” (PbD). As a matter of fact, the service providers have therefore to ensure that privacy and particularly protection of communication data is directly integrated in the conception and the functioning of the telecommunication and Internet systems.

Under these considerations, it seems clear that although nothing in the scope of the e-Privacy prohibits telecommunication and broadband providers to use the RPAS technology to carry communication and network services, providers shall demonstrate how they respect the privacy by design principle by using RPAS and, thus do not compromise the confidentiality of the information and communications of their subscribers.

As observed in the previous chapter of this deliverable, today, drones can easily be hacked. The ability to hack drones with software has been confirmed by several researchers.<sup>154</sup> Therefore, we can wonder how providers will ensure that RPAS is a reliable technology to carry communications and enable Internet connections. In the hypothesis the e-Privacy Directive applied to drones, these latter seems to be non-compliant by nature with Article 4, unless technological innovation stakeholders develop RPAS technology that is not capable of being easily hacked.

### ***Security Data Breach Notification***

Since 2009, in addition to the security principle already described, the e-Privacy Directive encompasses a mandatory security breach notification obligation for the holder of data.<sup>155</sup>

---

<sup>154</sup> RT.com staff writer, “Drone Hack Explained: Professor Details UAV Hijacking”, *RT Online*, 3 July 2012. <http://rt.com/usa/texas-professor-drone-hacking-249/>; Bryant, Jordan, “Hacker Releases Software to Hijack Commercial Drones”, *DefenseTech Online*, 9 December 2013. <http://defensetech.org/2013/12/09/hacker-releases-software-to-hijack-commercial-drones/>; Fink, Erika, “This drone can steal what's on your phone”, <http://money.cnn.com/2014/03/20/technology/security/drone-phone/>

<sup>155</sup> Article 4 (3) of the ePrivacy Directive provides: *In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or*

This requires that the service provider must inform the persons concerned and the relevant authorities in case of a breach relating to the use of one's personal data. Data breaches arise following theft of data accessed by unauthorised person, unauthorised disclosure of data and unlawful destruction, loss or alteration.<sup>156</sup> This notification data breach duty has a preventive and a "curative" purposes, as on one hand, it "makes individuals aware of the risks they face when their personal data are compromised and helps them to take the necessary measures to mitigate such risks"<sup>157</sup> and, on the other hand, it allows individuals victims of data breaches to "take action against the effects of a breach"<sup>158</sup> like changing passwords, delete their account. Applied to the context of the RPAS technology, this provision brings another protection to subscribers whose communications or Internet connection services could be provided by RPAS.

#### 4.3.9 *The Directive 2006/24/EC on the retention of data*

The Data Retention Directive is applicable to matters of surveillance and communications, although this Directive does not specifically address privacy or data protection. The Data Retention Directive obliges providers of electronic communications services and networks to conserve traffic and location data related to phone calls and emails for a period between six month and two years.<sup>159</sup> Traffic and location data may be made available to law enforcement authorities, upon their request, for the purposes of investigating, detecting and prosecuting serious crime and terrorism.<sup>160</sup> This Directive enables governments and intelligence agencies to track and store information pertaining to emails, mobile calls, and other phone and Internet use of EU citizens. It follows that law enforcement authorities can request access to location data and traffic data of communications that a drone belonging to a telecommunication provider has (lawfully or unlawfully) collected.

Notably, the Retention Directive has been the subject of much criticism for its intrusive character, and has not been implemented in all Member States.<sup>161</sup> Additionally, the European Court of Justice recently made a finding that the Retention Directive is invalid as it is inconsistent with Article 7, 8, 52 and 11 of the European Charter.<sup>162</sup> Therefore, we can expect a reconsideration of the surveillance laws in the Member States, and a reiteration of the weight of the data protection right.

---

*individual of the breach without undue delay. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.* For more information about "Security Data Breach Notification" see Barcelo, Rosa and Peter Traung, "The Emerging European Union Security Breach Legal framework: The 2002/58 ePrivacy Directive and Beyond", in Serge, Gutwirth, Yves, Poulet and Paul, De Hert (Eds.), *Data Protection in a Profiled World*, Springer, Brussels, 2010, pp. 77-104.

<sup>156</sup> ePrivacy Directive, Article 4(2).

<sup>157</sup> Barcelo, Rosa and Peter Traung, op. cit., 2010, pp. 77-104.

<sup>158</sup> Ibid.

<sup>159</sup> European Parliament and Council, Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 13.04.2006, Articles 3 and 6.

<sup>160</sup> Ibid., Articles 1-5; Bignami, Francesca, "Privacy and Law Enforcement in the European Union: The Data Retention Directive", *Chicago Journal of International Law*, Vol. 8 No. 1, 2007, p. 238.

<sup>161</sup> Germany, Norway, Poland, Slovenia.

<sup>162</sup> European Court of Justice, *Digital Rights Ireland Ltd v. The Minister for Communications, Marine and Natural Resources, The Minister for Justice, Equality and Law Reform The Commissioner of the Garda Síochána Ireland and The Attorney General*, Case C-293/12, 08.04.2014.

#### 4.3.10 Conclusion

This third section had two main objectives. On one hand, this study had to identify the existing European data protection laws and, on the other hand, it had to assess the applicability of the identified laws to the RPAS technology. In this last regard, we have particularly examined the scope of each data protection texts. From this analysis, it follows that each data protection laws apply to different sector depending on the purposes of the processing (commercial, law enforcement, journalistic, household, telecommunication and Internet services purposes). Hence, applied to the context of drones, four insights can be drawn.

The *first insight* we can present is that the RPAS' operator processing data through the means of drones for commercial purposes shall a priori respect the main data protection text, the Data Protection Directive 95/46. Regarding journalists and film-makers, these latter could be exempted of several provisions when it is necessary to strike a fair balance between the data protection right and the freedom of expression. The DPD encompasses a range of data protection principles, as well as proscribing an individual's rights, together with obligations on the data collector and processor. In a close future, the General Data Protection Regulation will be adopted. As we observed, nothing prevents its application to the processing of data executed by commercial operators. Although this latter will apply to the same type of processing (commercial operators and journalists with exemption or several articles), the proposal encompasses more protective rules and particularly relevant pro-active principles for the RPAS technology (PbD, PIA, etc.).

The *second insight* is that drones used by telecommunication or Internet providers to carry communications or offer broadband services fall under the application of the e-Privacy Directive, in complement to the Data Protection Directive. When analysing its articles, we remarked that the e-Privacy Directive prohibits the interception of communications and data, as well as requiring telecommunication and Internet providers to adhere to strict security measures in order to avoid any breach with the confidentiality of data principle.

The *third insight* is that after having analysed the scope of the Decision Framework 977/2008, (the FDPJ regulates data processing by law enforcement authorities when that processing takes place in the context of a European judicial or police cooperation between Member States), we can say that governmental drones collecting data in surveillance operations or for other purposes are mainly not regulated at the European level. This comes from the national security exemption included in the Lisbon Treaty and the data protection legislation. Nevertheless, this lack of rules at the European level should be partially remedied with the future Directive which is devoted to apply to processing executed by law enforcement bodies in European as well as national police and judicial cooperation.

Finally, the *fourth insight* is that private users of RPAS who may collect personal data in the context of household or personal uses are not covered by the existing European data protection framework.

#### 4.4 General Conclusion

The principal conclusion arising from this comprehensive analysis of the European privacy and data protection legal frameworks is that both types of regulations apply to RPAS

technology. However, they do not apply to the same drones activities and some differences may be highlighted in term of the nature of protection.

Firstly, we remarked that the right to privacy is much broader than the right to data protection as it not only protects the processing of information but also the monitoring in certain specific circumstances. However, the right to privacy is legally recognised but only regulated by the general principles set up by the Courts (mainly, the ECtHR). Furthermore, such regulation does not produces obligations and rights in the parties at stake but intervenes when the threat to privacy has been posed and consists to determine if this threat interferes and violates a citizens' fundamental right. On contrary, the data protection regulation does not determine explicitly what is a violation of the data protection right but provides rights and obligations to each actor (processor, collector, data subject, data protection authority) during all the process of processing personal data (from prior to the execution to the use). Therefore, we can say that the regulation of the right to privacy is passive, "curative" while the legislation of data protection is proactive and preventive.

Secondly, we emphasised that, by contrast to the right to privacy, that data protection legislation establishes various obligations, restrictions and rights depending on the entity recording the data. Applied to the context of RPAS technology, we observed that two types of operators are exempted of the European data protection regulations, law enforcement authorities processing data which does not take place in a European or International cooperation and private individuals processing data via a the equipment of a drone for recreational and household purposes. However, we have seen in the previous chapter that both types of actors, law enforcement bodies and private individuals, are and will use RPAS and their equipment for civilian applications. Nevertheless, although the main data protection directive excludes its application to private individuals and law enforcement bodies using RPAS, these groups must respect Article 8 of the EU Charter of Fundamental Rights, which recognises the right to data protection including the main data protection principles and individuals' rights. Furthermore, these activities are often regulated at the Member State level, rather than the European level. As such, the next chapter examines Member State regulations relevant to RPAS.

## **5 RPAS TECHNOLOGY AND DOMESTIC PRIVACY AND DATA PROTECTION LAW**

### **5.1 Introduction**

As explained in Annex B, some aspects of RPAS technology, such as safety, are already the subject of national regulation. However, Member States do not currently provide RPAS-specific privacy or data protection regulations. Yet, certain countries, generally those having safety regulations in place, have permitted some RPAS to fly in their domestic airspace. Nevertheless, each Member State includes in its legislation two types of laws which may be applied to RPAS applications and have an impact on the privacy of citizens. On one hand, there is the general privacy legislation. As a matter of fact, each Member States' legislation encompasses at least the minimum privacy and data protection laws that reflect the European privacy and data protection legislation framework previously examined. On the other hand, some Member States have also drafted surveillance-oriented regulations, which include some privacy elements, such as regulations for CCTV systems and police surveillance. Such legislative instruments could regulate some RPAS applications such as aerial photography or visual surveillance. Furthermore, in addition to these national legal regimes, some national data protection authorities have also adopted an official position or certain initiatives in relation to the RPAS technology and the data protection. Hence, this chapter will assess the applicability of each of these instruments (by examining their scope) in order to determine which RPAS applications these could effectively regulate.

Besides European Member States, some lawmakers in third countries, such as the United States and Switzerland, have also reacted to the existing and potential privacy and data protection concerns raised by the use of RPAS technology. It is relevant to examine whether these third countries have enacted some specific privacy laws to regulate the RPAS technology and, otherwise, analyse what is their general privacy legislation applicable to RPAS as it could encompass some relevant principles.

Finally, some international organisations associated with the RPAS industry have released codes of conduct. As these codes set out the ethical and safety recommendations relevant to the use of RPAS technology, the codes may assist with developing a framework to tackle privacy concerns arising from RPAS use.

Against this background, we have divided this chapter into five main sections:

1. Member States already using civil RPAS;
2. Member States currently preparing regulations;
3. Overview of the position and activities adopted by the DPAs;
4. Third Countries; and
5. International soft-law.

To meet the objective of this contribution, we examine six Member States that have implemented safety regulations for RPAS use, the United Kingdom, France, Germany, Italy, Sweden and Denmark and one Member State that is currently preparing a RPAS-specific regulation, Belgium. In addition, we look at relevant privacy regulations of two countries outside of the EU (third countries), namely the United States, and Switzerland. As mentioned above, for each country we will discuss both privacy legislation, and surveillance oriented

regulations. With respect to privacy, we examine the legislative approach to preserving the right to privacy, the right to data protection, and any relevant telecommunication regulations. With respect to surveillance issue, we focus our study on CCTV regulations, and regulations governing the law enforcement sector in their surveillance missions.

## 5.2 Member States already using civil RPAS

In this first chapter, we examine the legal privacy framework of three Member States that have already implemented RPAS aviation regulations, including the regulatory instruments of the United Kingdom, France and Germany.

### 5.2.1 The United Kingdom

The regulatory structure of privacy, data protection and surveillance in the UK is multi-faceted. First, we examine the right to privacy as it is preserved by the Human Rights Act. Second, we study how the UK regulates rights to data protection by examining the Data Protection Act, the ICO Guidance and the Freedom of Information Act. Third, we analyse how the telecommunications and Internet service sectors are regulated under the Privacy and Electronic Communications regulation. Then, we examine the regulation of surveillance activities by looking at CCTV systems regulations and the legislation governing the use of surveillance, investigation and the interception of communications by UK public bodies/authorities.

#### *Privacy and data protection regulations*

##### a) The right to privacy: Article 8 of the Human Rights Act 1998<sup>163</sup>

Relevantly, “there is no one privacy law in the UK, it comes from a variety of Acts of Parliament, procedural rules and key cases”.<sup>164</sup> The first legislative instrument mentioning the right to privacy is Article 8 of the Human Right Act. That Act refers explicitly to Article 8 European Convention of Human Rights (ECHR) and its accompanying jurisprudence when it stipulates:

*All legislation, past and present, wherever possible should be read and given effect in a way compatible with Convention rights and where relevant to proceedings before them, the courts must take into account jurisprudence from the European Court.*<sup>165</sup>

This reference is interesting because it means that the jurisprudence of the ECtHR surrounding Article 8 is directly applicable to UK citizens. Therefore, the principles of the ECtHR that we pointed out in the previous chapter and the jurisprudence of Article 8 Human Rights Act together apply to RPAS technology used in United Kingdom airspace.

---

<sup>163</sup> United Kingdom Parliament, The Human Rights Act 1998, 09.11.1998 (“the Human Rights Act 1998”).

<sup>164</sup> Duke, “Privacy: The Development of a Law and the Legal Theory”, *Legal Piracy Blog*, 18 May 2011. <https://legalpiracy.wordpress.com/2011/05/18/privacy-law-1/>

<sup>165</sup> Taylor, Nick, “State Surveillance and the Right to Privacy”, *Surveillance & Society*, Vol. 1(1), p. 72. <http://www.surveillance-and-society.org/articles1/statesurv.pdf>

b) The data protection legislation: The Data Protection Act 1998<sup>166</sup>, the ICO Guidance and the Freedom of Information Act 2000

Firstly, the processing of personal data is governed by the Data Protection Act 1998. The Data Protection Act implements the Data Protection Directive 95/46/EC. Although the UK has not yet implemented any specific privacy rules for the use of RPAS, the UK Civil Aviation Authority states:

*Aircraft operators and pilots should be aware that the collection of images of identifiable individuals (even inadvertently) when using surveillance cameras mounted on a Small Unmanned Surveillance Aircraft may be subject to the Data Protection Act. As this Act contains requirements concerning the collection, storage and use of such images, Small Unmanned Aircraft operators should ensure that they are complying with any such applicable requirements or exemptions.<sup>167</sup>*

This statement makes it clear that operators recording personal data through the means of civil RPAS should apply the Data Protection Act. However, the scope of the Data Protection Act must be examined as well to determine exactly to which type of processing and collectors it applies.

The Data Protection Act covers all personal data collected by private sector actors as well as public entities. However, the Data Protection Act does not apply to the domestic processing of collected data. With regard to the media and the police sectors, they may be exempt from several of the Data Protection Act's principles in certain cases.<sup>168</sup> So, all RPAS operators processing personal data fall within the scope of the Data Protection Act, unless it is a private processing for purely domestic purposes.<sup>169</sup> Although journalists and law enforcement authorities may, in certain circumstances, be exempt from this law, the Data Protection Act otherwise applies to them as well.

The Data Protection Act enshrines the same principles and individual rights as the ones provided in the Data Protection Directive which we examined previously.<sup>170</sup> Nevertheless, it is important to note that the UK Data Protection Authority does not execute "prior checking". Hence, whereas we have seen in the previous chapter that the "prior checking" could be an interesting way to exercise a "preventive" control on the collector of data by RPAS, this mechanism does not exist in UK.

---

<sup>166</sup> United Kingdom Parliament, Data Protection Act 1998, 16.07.1998 ("UK DPA 1998").

<sup>167</sup> UK Civil Aviation Authority (CAA), "Unmanned Aircraft and Aircraft Systems", *Operations and Safety*, no date. <http://www.caa.co.uk/default.aspx?CATID=1995>

<sup>168</sup> Section 32 of the UK DPA 1998 sets out the exemption for journalism. Its purpose is to safeguard the right to freedom of expression as set out in Article 10 of the European Convention on Human Rights. It covers the 'special purposes' of journalism, art and literature. The scope of the exemption is very broad, and may override a number of other provisions of the UK DPA 1998, and gives the media a fair amount of leeway to decide for themselves what is in the public interest. However, in accordance with Directive 95/46/EC, it does not give an automatic blanket exemption in every case: UK Information Commissioner's Office ("UK ICO"), *Data Protection and Journalism. A Guide for the Media – Draft for Consultation*, Information Commissioner's Office, Cheshire, 23 January 2014. [http://ico.org.uk/~media/documents/library/Data\\_Protection/Research\\_and\\_reports/data-protection-and-journalism-a-guide-for-the-media-draft.pdf](http://ico.org.uk/~/media/documents/library/Data_Protection/Research_and_reports/data-protection-and-journalism-a-guide-for-the-media-draft.pdf)

<sup>169</sup> UK DPA 1998, Article 5.

<sup>170</sup> UK DPA 1998, Parts I and Part II.

Secondly, in addition to the Data Protection Act, the UK Data Protection Authority (the Information Commissioner's Office - ICO) issued some interesting Guidance, such as the *Privacy by Design Code of Practice*, *Privacy Impact Assessment Code of Practice* and *Anonymisation Code of Practice*.<sup>171</sup> Although these rules are not legally binding, they influence private sector and public bodies that collect personal data by encouraging them to adopt more privacy protective approaches.

Thirdly, The Freedom of Information Act (FOIA)<sup>172</sup> gives UK citizens the right to access any recorded information held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. It is not limited to official documents, and the right also covers information held on computers, in emails and in printed or handwritten documents as well as images, video and audio recordings.<sup>173</sup> “[T]he Freedom of Information Act is about getting rid of unnecessary secrecy”.<sup>174</sup> Applied to the context of RPAS, it would allow, for instance, to citizens having participated to a gathering filmed by a governmental drones to access to such videos. Under the FOIA, citizens spotting a drone above their backyard could request that authorities provide information related to this specific RPAS operation launched by public bodies (purpose of the flight, eventual data captured by the drones, etc.). However, this Act comprises specific formal and substantive requirements for access to such public data. Moreover, the data could only be given to its applicant if the disclosure of such data does not contravene the provisions of the Data Protection Act.

c) Privacy regulation in the telecommunication sector: The Privacy and Electronic Communications Regulations 2011 (PECR)<sup>175</sup>

The PECR transcribes the e-Privacy Directive into UK national law. In conformity with the e-Privacy Directive, the PECR “restrict[s] the processing and sharing of personal traffic data and location data and provide for access to users’ personal data in the interest of national security”.<sup>176</sup> The PECR also promotes public security, and the prevention, detection and prosecution of criminal offences. Additionally, it includes the principle of confidentiality of electronic communications. Hence, under these legal bases, operators that attempt to intercept electronic communications by the use of drones could be punished in UK.

In addition to the confidentiality principle, the same “security measures article” as the one studied in the analysis of the Data Protection Directive<sup>177</sup> is included in the PECR:

*A provider of a public electronic communications service must take appropriate technological and organisational measures to safeguard the security of its services. An*

---

<sup>171</sup> For more information about these principles, see Part III of this deliverable; UK ICO, “Topic Guides for Organisations: Data Protection”, *UK ICO online*, no date.  
[http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides](http://ico.org.uk/for_organisations/data_protection/topic_guides)

<sup>172</sup> United Kingdom Parliament, Freedom of Information Act, 30.11.2000 (“UK FOI Act 2000”).

<sup>173</sup> UK ICO, “What is the Freedom of Information Act?”, *UK ICO online*, no date.  
[http://ico.org.uk/for\\_organisations/freedom\\_of\\_information/guide/act#what-is-the-freedom-of-information-act-8](http://ico.org.uk/for_organisations/freedom_of_information/guide/act#what-is-the-freedom-of-information-act-8)

<sup>174</sup> *Ibid.*

<sup>175</sup> United Kingdom Parliament, Privacy and Electronic Communications Regulations, 26.05.2011 (“UK PECR 2011”).

<sup>176</sup> Rouse Margaret, “Privacy and Electronic Communications Regulations (PECR)”, *SearchSecurity online*, April 2012. <http://searchsecurity.techtarget.co.uk/definition/Privacy-and-Electronic-Communications-Regulations-PECR>

<sup>177</sup> See Part III, Chapter 1, Section 2 of this deliverable.

*appropriate measure is one that is proportionate to the risks it would safeguard against, taking account of the state of technological development and the cost of implementing the measure.*<sup>178</sup>

In the context of RPAS, this security measure obligation implies that UK Internet and telecommunication providers shall adopt all security measures required by the PECR if they use RPAS to carry electronic communications and network services. As mentioned earlier, given the ease with which it is possible to hack drones<sup>179</sup>, it seems that the confidentiality and security principles are not easy to comply with for providers using drones to carry telecommunications or broadband services.

In addition, the Data Retention Regulation 2009, stipulates that data related to communications must be retained by the telecommunication providers when these latter are necessary to:

- trace and identify the source of a communication;
- identify the destination of a communication;
- identify the date, time and duration of a communication; and
- identify the type of communication.<sup>180</sup>

Such data may only be accessed by law enforcement authorities “in specific cases and in circumstances in which disclosure of the data is permitted or required by law”.<sup>181</sup> Concerning the period of retention, Article 5 provides that “data must be retained by the public communications provider for 12 months from the date of the communication in question”.<sup>182</sup> Applied to the RPAS technology, it means that telecommunications providers have to retain data related to the communications carry by drones during a period of 12 months.

### ***Surveillance regulations applicable to civil RPAS***

#### **a) Visual surveillance (CCTV systems) regulation: The Data Protection Act 1998<sup>183</sup> and the CCTV Code of Practice<sup>184</sup>**

In the United Kingdom, there is no specific legal CCTV regime. However, it is noteworthy that the Data Protection Act applies to general overt video surveillance operated in public places when these latter record data.<sup>185</sup> Camera surveillance is considered overt as soon as the CCTV cameras are visible and people are aware that these CCTV systems are filming them, for example by pictograms.

---

<sup>178</sup> UK ICO “Security of Services”, *UK ICO online*, no date.

[http://ico.org.uk/for\\_organisations/privacy\\_and\\_electronic\\_communications/the\\_guide/security\\_of\\_services](http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/security_of_services)

<sup>179</sup> Fink, Erica, “This drone can steal what's on your phone”, *CNNMoney online*, 20 March 2014.

<http://money.cnn.com/2014/03/20/technology/security/drone-phone/>

<sup>180</sup> UK PECR 2011, Article 5.

<sup>181</sup> Pinsent Masons, “Data Retention Laws: What they Mean for Communication Service Providers”, *Out-Law online*, no date. <http://www.out-law.com/en/topics/tmt--sourcing/data-protection/data-retention-laws-what-they-mean-for-communication-service-providers/>

<sup>182</sup> UK PECR 2011, Article 5.

<sup>183</sup> UK DPA 1998.

<sup>184</sup> UK ICO, “Code of Practice. Draft for Consultation 20 May 2014 - 1 July 2014”, (UK ICO Code of Practice 2014”) p. 5.

[http://ico.org.uk/about\\_us/consultations/~media/documents/library/Data\\_Protection/Research\\_and\\_reports/draft-cctv-cop.pdf](http://ico.org.uk/about_us/consultations/~media/documents/library/Data_Protection/Research_and_reports/draft-cctv-cop.pdf)

<sup>185</sup> UK ICO, Code of Practice, 2014, p. 5.

In addition to the Data Protection Act, it should be noted that the Information Commissioner's Office issued Code of Practice for CCTV systems that includes relevant recommendations. The ICO has just enacted a draft for Consultation. This new version of the Code of Practice should be adopted in July of 2014. The ICO specifically connects this document to the use of RPAS, and states that it explicitly applies "to the use of camera related surveillance equipment such as remotely operated vehicles (drones)".<sup>186</sup> Like the Data Protection Act, this Code applies to the use of CCTV and other systems by public bodies, commercial organisations and professionals that capture images of identifiable individuals or information relating to individual.<sup>187</sup> The CCTV Code of Practice does not apply to processing of data for journalistic purposes and to collection of personal data by CCTV systems implemented by a private user for limited household purposes.<sup>188</sup> For example, it does not apply when "an individual [who] uses CCTV to protect their home from burglary, even if the camera overlooks the street or other areas near their home".<sup>189</sup> Hence, the use of cameras for private and recreational uses is not regulated in the UK.

Although the Code of Practice is not mandatory, it provides relevant recommendations that are supplemented by the incorporation of practical examples for commercial users of CCTV systems. For instance, in relation to the disclosure of information, it provides:

*Disclosure of images from the CCTV system must also be controlled and consistent with the purpose for which the system was established. For example, it can be appropriate to disclose surveillance information to a law enforcement agency when the purpose of the system is to prevent and detect crime, but it would not be appropriate to place them on the internet.*<sup>190</sup>

Regarding to drones, the Code of Practice provides specifically some questions that private actors who collect personal information via the aid of RPAS should check (prior and after the processing) to assess if they comply with the guidance:

- Has a PIA been undertaken which justifies the drone's use, rather than a less privacy intrusive method?
- Has a method of informing individuals that recording is taking place been identified?
- Has a method of providing fair processing information been identified?
- Is the recording continuous or triggered by something? If recording is continuous, is it proportionate and justifiable?
- Is there a method by which recording can be restricted to the focus of the drones attention, rather than recording a wide field of vision?
- Have appropriate security measures, such as encryption and access controls been put in place?
- Have appropriate retention and deletion schedules been incorporated?

---

<sup>186</sup> Ibid., pp. 5, 22.

<sup>187</sup> UK ICO, Code of Practice, 2014, p.5.

<sup>188</sup> UK, ICO Code of Practice, 2014, p. 5.

<sup>189</sup> UK ICO Code of Practice 2014., pp. 5, 22.

<sup>190</sup> Ibid., p. 12.

b) Surveillance regulation in the law enforcement sector: The Regulation of Investigatory Powers Act (RIPA) 2000<sup>191</sup>

The Regulation of Investigatory Powers Act (hereinafter, RIPA) has been enacted to ensure the balance between the public interest and the fundamental individual rights protected under the Human Rights Act 1998. The legislator has published a RIPA Codes of practice that assists public authorities to assess and understand whether, and in what circumstances, it is appropriate to use covert techniques.<sup>192</sup> The RIPA covers any surveillance that is directed at an individual, or covert<sup>193</sup>, intrusive surveillance, directed surveillance, property interferences and the interception of communications. Law enforcement authorities remain sole bodies authorised to use such surveillance techniques.

Intrusive surveillance refers to “surveillance carried out in relation to residential premises or private vehicle” while directed surveillance encompasses “surveillance that is likely to discover personal information about a target”.<sup>194</sup> According to section 28(3) of RIPA 2000, the operators of directed surveillance need to obtain an authorisation, which must be granted by an authorising officer. RIPA 2000 also requires that police forces carrying out intrusive surveillance obtain authorisation either from the Secretary of State or from a senior authorising officer.<sup>195</sup> It is noteworthy that the RIPA does not provide any information concerning the period of retention of the data stored. Regarding *property interferences* often related to intrusive surveillance, the RIPA also requires law enforcement authorities to obtain an authorisation from the authorising officer<sup>196</sup>. However, this authorisation is not needed when the individual of the property concerned has provided their consent.<sup>197</sup>

The interceptions of private communications are conditional upon the issuing of a warrant by the Secretary of State.<sup>198</sup> In addition to the provisions of the RIPA, the Code of Practice related to the interceptions of communications refers to Article 8 of the ECHR and the related wiretapping ECHR case law. In that regard, the RIPA stipulates “obtaining a warrant under the Act will only ensure that the interception authorized is a justifiable interference with an individual’s rights under Article 8 of the European Convention of Human Rights (the right to privacy) if it is necessary and proportionate for the interception to take place”.<sup>199</sup>

Given that RPAS can be mounted with various different payloads, including cameras, GPS, and sensors, and that they capable of wiretapping and recognising human targets, they will undoubtedly be used for all types of intrusive and directed surveillance activities, property interferences, and interceptions of communications carried out by police and intelligence services. As the RIPA does not exclude from its scope surveillance operated by aerial

---

<sup>191</sup> The United Kingdom, Regulation of Investigatory Powers Act 2000, 20.07.2000 (“UK RIPA 2000”).

<sup>192</sup> “RIPA Codes”, *Gov.uk online*, no date. <https://www.gov.uk/government/collections/ripa-codes>

<sup>193</sup> “Unmanned Aerial Vehicles and Unmanned Aerial Systems Briefing”, *Big Brother Watch*, 2013. <http://appgondrones.files.wordpress.com/2013/06/unmanned-aerial-vehicles-briefing-big-brother-watch.pdf>

<sup>194</sup> Finn, Rachel L. and David Wright, “Unmanned Aircraft Systems: Surveillance, Ethics and Privacy in Civil Applications”, *Computer Law & Security Review*, Vol. 28, Issue 2, April 2012, pp. 184-194; The Government of the United Kingdom - Home Office, *Covert Surveillance and Property Interference Revised Code of Practice*, TOS, London, 2010 (“UK Home Office Code of Practice 2010”).

<sup>195</sup> UK RIPA 2000, Section 32.

<sup>196</sup> UK Home Office, Code of Practice, 2010, p. 61.

<sup>197</sup> *Ibid.*, p. 62.

<sup>198</sup> UK RIPA 2000, Section 5.

<sup>199</sup> UK Home Office, Code of Practice, 2010, p. 7.

equipment, we can assume that law enforcement using drones for blanket surveillance shall be required to obtain authorisations, as well as be subject to the all other RIPA obligations.

### *Summary*

This study of the UK legal system illuminates several points for RPAS operators. First, the use of commercial, governmental and journalistic drones for collecting personal data should be covered by the Data Protection Act, even if in some circumstances law enforcement and journalistic RPAS' operators are exempted from several provisions. Secondly, the provider of telecommunications or Internet services which use RPAS technology to carry its services shall a priori respect the Data Protection Act and the Privacy and Electronic Communications Regulations when personal data are processed. The latter particularly protects the secrecy of communications and set up for the providers an obligation to safeguard the security of that service. Thirdly, the study of UK regulations related to surveillance have pointed out that two types of laws may be distinguished: those regulating overt surveillance operated in public places and those covering the covert surveillance operated by public bodies. Commercial, governmental and journalistic operators using drones mounted with a surveillance camera to record images in public places should adhere to the relevant provisions of the Data Protection Act, as well as the CCTV Code of Practice 2014. Regarding to the future CCTV Code of Practice 2014, it is important to note that visual surveillance operated by drones is explicitly covered and their collectors receive some specific Guidance under the form of "check questions". For the public bodies using governmental drones for overt and covert surveillance missions, the provisions of the RIPA applies. Finally, these findings allow us to conclude that private individuals using drones to record data or simply monitoring by visual surveillance is neither covered by the DPA, nor by the CCTV Code of Practice 2014. However, we should mention that the law of torts could be extended to prohibit some applications, we think for instance to the tort of nuisance which could prevent a private user from flying a drone above a neighbour's property. Furthermore, citizens can pursue claims of violation of the right to privacy in front of British or European the courts.

#### *5.2.2 France*

We firstly discuss the right to privacy as it is preserved by the French Constitution and the Declaration of the Rights of Man and the Citizen. We then examine the Computer, Files and Liberties Act as it relates to the collection of personal data. Further, we examine the applicability of the French Ordinance on electronic communications to use of RPAS as proxy-satellite by Telecommunication and Internet providers

Finally, we examine how users of surveillance cameras fitted on RPAS, in particular public bodies carrying out surveillance missions, could be regulated by the Computer, Files and Liberties Act, and the Security Act.

#### *5.2.3 Privacy and data protection regulations*

- a) The right to privacy: Article 2 of the Declaration of the Rights of Man and the Citizen 1789 and Article 9 of the Civil Code

The right of privacy is not explicitly enshrined in the French Constitution of 1958, but the Constitutional Council hold that the right of privacy is implicitly included in the Constitution.

Besides the Constitution, the right to privacy is expressly enshrined in Article 2 of the 1789 Declaration of the Rights of Man and the Citizen and Article 9 of the Civil Code.<sup>200</sup>

b) The data protection legislation: The Computer, Files and Liberties Act 1998<sup>201</sup>

In France, the processing of personal data is regulated by the Computer, Files and Liberties Act (hereinafter, the CFLA). This Act has been amended several times to implement the Data Protection Directive and to adapt to the recent technologic developments. Recently, the French Data Protection Authority (the CNIL) has explicitly declared that any processing of personal data by any equipment fitted on a drone shall respect the CFLA: “Si la prise de vue aérienne est réglémentée par l'article D. 133-10 du code de l'aviation civile, il n'en demeure pas moins que la captation et l'enregistrement d'images relatives aux personnes relèvent également de la loi Informatique et Libertés”.<sup>202</sup> Thanks to this statement, it is clear that the CLFA applies to the RPAS technology. However, we should have a look to its scope to determine the outlines of its application.

The scope of the CFLA provides that it applies to personal data processed by both public and private sectors, excluding solely the processing of data carried out by individuals for private and household activities.<sup>203</sup> It also applies partially to the processing of data for journalistic and artistic purposes.<sup>204</sup> Unlike the European Data Protection Directive, nothing in the CFLA seems to prevent its application to the processing of data by law enforcement authorities.<sup>205</sup> However, some obligations are reinforced when these latter process data for public security, defence, State security or purposes related to criminal matters. For instance, prior to processing collected data, law enforcement authorities have to obtain authorisation by a Ministerial Decree, issued on the basis of an Opinion of the CNIL, and they are required to publish processing activities.

In terms of content, the CFLA incorporates the same principles as those laid down by the Data Protection Directive: quality of the data (accurate, complete and updated), quality of the processing: legitimacy, finality, proportionality, minimisation, transparency and retention principles, sensitive data, individual rights, adequate level of protection in case of transfer to third countries, and the notification to the Data Protection Agency before the processing.<sup>206</sup>

c) Privacy regulation in the telecommunication sector: The French Ordinance on electronic communications 2011<sup>207</sup>

In France, the European “Telecommunication Package” including the e-Privacy Directive has been implemented by The French Ordinance no. 2011-2012 of 24 August 2011 on electronic

---

<sup>200</sup> Privacy International, the Electronic Privacy Information Center (“EPIC”) and the Center for Media and Communications Studies (“CMCS”), *European Privacy and Human Rights (“EPHR”)*, European Commission, Brussels, 2010, p. 278.

<sup>201</sup> French Parliament, Computer, Files and Liberties Act, 13.10.1978 (“French CFLA 1978”).

<sup>202</sup> La Commission Nationale de l'Informatique et des Libertés (“CNIL”), “Usages des Drones et Protection des Données Personnelles”, 2012. <http://m.cnil.fr/linstitution/actualite/actualite/article/usages-des-drones-et-protection-des-donnees-personnelles/>

<sup>203</sup> French CFLA 1978, Article 2.

<sup>204</sup> French CFLA 1978, Article 67.

<sup>205</sup> French CFLA 1978, Articles 26 and 41.

<sup>206</sup> French CFLA 1978, Chapters II, V and VI.

<sup>207</sup> France, Ordinance on Electronic Communications, 24.08.2011 (“Electronic Communications Ordinance 2011”).

communications. This amends the French Consumer Protection Code, the French Penal Code, the French Postal and Electronic Communications Code and the French Data Protection Act. In accordance with the e-Privacy Directive, this Ordinance regulates the telecommunication and network sector. Its scope is “to ensure better regulation of the electronic communication sector, ensure more efficient spectrum management and to facilitate spectrum access and reinforce consumers’ protection and data protection”.<sup>208</sup>

The Ordinance requires the telecommunication and network services providers to ensure the confidentiality of the communications and the deletion or the anonymisation of the traffic data related to these communications.<sup>209</sup> The location data related to the communications cannot be processed or stored by the providers following the transmission of the communication without the consent of the subscriber. Furthermore, the Ordinance also enshrines security and data breach principles:

*Public network services providers should notify the French Data Protection Authority (“CNIL”) without delay as soon as a personal data breach occurs in connection with the provision of electronic communication services. A personal data breach is defined as any security breach resulting accidentally or unlawfully in the destruction, loss, alteration, disclosure or unauthorised access to personal data. Where such a personal data breach might impact a user or an individual’s personal data or privacy, the service provider must also notify that person without delay, unless the CNIL determines that adequate protective measures have been implemented to render the data inaccessible by unauthorized persons (for example, as a result of encryption). In cases where an operator fails to notify such breach, sanctions may be imposed of up to five years’ imprisonment and fines up to €300,000. Operators must also maintain an inventory of data breaches, which must be provided to the CNIL on request.*<sup>210</sup>

Furthermore, the Decree of the 25<sup>th</sup> February 2011 implementing the Data Retention Directive provides that:

*Electronic communication operators are subject to the legal obligation to retain traffic data of clients for one year for the purposes of research and prosecution of criminal offenses or breaches of authors’ intellectual property rights, but it also allows for access to such data by judicial authorities.*<sup>211</sup>

Further, it provides: “Internet service providers have to retain all information on Internet users and telephone subscribers and to deliver it to the police or the State at a simple request”.<sup>212</sup> Additionally, competent authorities might apply at any time to obtain data necessary for the investigation of criminal offenses from the operators.<sup>213</sup>

---

<sup>208</sup> Rousseau Sylvie and Ambre Fortune, “France - European Telecom Package Finally Implemented”, *Linklaters Newsletter online*, 2011. <http://www.linklaters.com/Publications/Publication1403Newsletter/TMT-newsletter-September-2011/Pages/France-ePrivacy-cookies.aspx#sthash.4uzeP4FF.dpuf>

<sup>209</sup> Electronic Communications Ordinance 2011.

<sup>210</sup> Rousseau and Fortune, op. cit., 2011.

<sup>211</sup> Privacy International, EPIC and CMCS, op. cit., 2010, p. 285.

<sup>212</sup> *Ibid.*, p. 286.

<sup>213</sup> Garance, Mathias, “Données de Connexion : à la Suite du Décret du 25 février 2011, une tentative d’état des lieux du ‘patchwork ‘juridique’”, 2013. <http://www.unixgarden.com/index.php/misc/donnees-de-connexion-a-la-suite-du-decret-du-25-fevrier-2011-une-tentative-detat-des-lieux-du-patchwork-juridique>

Under this analysis, it seems that providers of Internet and telecommunication services using drones to carry their services shall apply the CFLA 1978, the Ordinance 2011 and the Decree 2011.

### *Surveillance regulations applicable to civil RPAS*

- a) Visual surveillance (CCTV systems) regulations: The Computer, Files and Liberties Act 1998<sup>214</sup>, The Act orienting and programming the Security 2011 (The Security Act)<sup>215</sup> and Article 9 of the Civil Code and Article 226-1 of the Criminal code

In France, the legal regime for CCTV systems, called “video-protection” depends on where the visual-surveillance takes place (in public places, at home, in shops, in schools, etc.). In public places, sole public bodies may capture images.<sup>216</sup> Public authorities are subject not only to the CFLA if they record but also to some Articles of the Security Act 2011 (Articles L223-1 and foll. and Articles L251-1 and foll.). The Security Code provides that a video camera can be installed in public places only to prevent acts of terrorism, public security breaches of people and goods where there is particularly a risk of assault, theft or trafficking narcotics.<sup>217</sup> Persons filmed must be informed of the existence of the device, of who is responsible for the device, and of the practical arrangements for exercising their right to access to visual records concerning them.<sup>218</sup> The images captured can only be conserved for a period of one month and watched by specific persons.<sup>219</sup> These cameras should not be allowed to see inside residential buildings. Hence, the CNIL recommends that software masking these areas visible should be implemented<sup>220</sup>. Furthermore, all CCTV system installations in a public place, regardless if the images will be recorded or not, are subject to an authorisation from the police headquarters issued on the opinion of a departmental committee chaired by a judge. This authorisation is valid for a period of 5 years and needs to

---

<sup>214</sup> French CFLA 1978.

<sup>215</sup> French Parliament, The Act Orienting and Programming the Security, 14.03.2011 (“French Programming and Security Act 2011”).

<sup>216</sup> CNIL, “La Vidéosurveillance sur la Voie Publique. Fiche Pratique”, 2012.  
[http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Videosurveillance/CNIL\\_Video\\_voie\\_publique.pdf](http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Videosurveillance/CNIL_Video_voie_publique.pdf)

<sup>217</sup> « La transmission et l'enregistrement d'images prises sur la voie publique par le moyen de la vidéoprotection peuvent être mis en œuvre par les autorités publiques compétentes aux fins d'assurer :

- « 1° La protection des bâtiments et installations publics et de leurs abords ;
- « 2° La sauvegarde des installations utiles à la défense nationale ;
- « 3° La régulation des flux de transport ;
- « 4° La constatation des infractions aux règles de la circulation ;
- « 5° La prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières prévues par le second alinéa de l'article 414 du code des douanes et des délits prévus à l'article 415 du même code portant sur des fonds provenant de ces mêmes infractions ;
- « 6° La prévention d'actes de terrorisme ;
- « 7° La prévention des risques naturels ou technologiques ;
- « 8° Le secours aux personnes et la défense contre l'incendie; French Programming and Security Act 2011, Article 18.

<sup>218</sup> CNIL, “La Vidéosurveillance Sur la Voie Publique. Fiche Pratique”, 2012.  
[http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Videosurveillance/CNIL\\_Video\\_voie\\_publique.pdf](http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Videosurveillance/CNIL_Video_voie_publique.pdf)

<sup>219</sup> Ibid.

<sup>220</sup> CNIL, op. cit., 2012.

be renewed before expiration.<sup>221</sup> Finally, it is noteworthy that some private places accessible to the public or a specific public place are regulated by specific sector legislation. Applied to the context of the RPAS technology, it results that governmental drones used for visual surveillance could be regulated by the CFLA and the Security Code. However, it is noteworthy that these regulations do not say anything about mobile cameras. So, whereas this legislation should a priori apply, the CNIL could consider that the CFLA and the Security Code do not cover mobile cameras.

At home, the use of surveillance cameras by individuals is not subject to specific CCTV regulations. Therefore, on the basis of the CCTV regulation, the private and family sphere represent the limits of CCTV law beyond which the rules find no application.

b) Surveillance in the law enforcement sector: The Act orienting and programming the Security 2011 (The Security Act)<sup>222</sup>

All types of surveillance, including the wiretapping of electronic and private communications, by law enforcement authorities are allowed in France by the Law 2011-267 orienting and programming the Security (Security Act).

Besides overt video-surveillance, this same law provides that the Criminal Investigation Police can intercept electronic communications by “physically or remotely install spying software on a suspect's computer to listen to electronic communications, gain access to all the data in a computer in real time, and introduces Internet filtering by administrative decision”<sup>223</sup>.

This interception of telecommunications is also authorised in France. In this regard, the French legal regime distinguishes between administrative wiretapping and judicial wiretapping. In the first case, the interception must be authorised by the First Minister and must concern: (i) national security, (ii) safe-guard of the essential elements of the scientific and economic of France, (iii) the Prevention of Terrorism, (iv) the prevention of crime and organized crime, (v) the prevention of the recovery or the maintenance of combat groups and private militias dissolved. Regarding the judicial listening, it is the investigating judge who authorises them when they are needed in the administration of justice.<sup>224</sup>

Given that civil drones are able to hack mobile phones, computers and, then, intercept electronic and telecommunications, we can imagine that law enforcement authorities will use them in their surveillance operations. As nothing restricts the application of the Security Act to the surveillance operated by drones, governmental authorities shall respect the Security Act when they use drones in a surveillance context.

---

<sup>221</sup> Service-Public.fr, “Vidéoprotection Dans les Lieux Publics”, 2013. <http://vosdroits.service-public.fr/particuliers/F2517.xhtml>

<sup>222</sup> France LOI, “D'orientation et de Programmation Pour La Performance de la Sécurité Intérieure”, No. 2011-267, 14 March 2011.

<sup>223</sup> Privacy International, EPIC and CMCS, op. cit., 2010, p. 283.

<sup>224</sup> Service Public, “Ecoutes Téléphoniques”, 2013. <http://vosdroits.servicepublic.fr/particuliers/f2515.xhtml>

c) Surveillance by the use of geo-localisation systems (location data) in the law enforcement sector<sup>225</sup>: The Geo-localisation Act 2014<sup>226</sup>

Whereas the location data processed by the commercial sector is regulated by the CFLA, the French Government enacted a specific act concerning the geo-localisation technologies used for surveillance purposes by law enforcement agencies and judicial authorities. Geo-localisation includes all techniques allowing the permanent localisation of a mobile phone or an object such as a vehicle or even a home.<sup>227</sup> GPS devices and ANPR have been recognised amongst geo-localisation technologies. Although this Act does not provide explicitly its application to such systems when they are mounted on RPAS, we can easily imagine that it can apply to them by analogy.

This act allows that geo-localization systems are used in real time to track an individual or a vehicle or any other objects covertly. Nevertheless, it also provides some boundaries to the use of the geo-localisation systems, with the exception of law enforcement authorities, which can capture such location data in a surveillance context, and only for legally restricted purposes.<sup>228</sup> In addition, it adds several provisions in the Criminal Code in order to subject the measure to an authorisation of the Public Prosecutor.<sup>229</sup> It must be remembered that the law enforcement authorities using geo-localisation systems will not only be subject to this Act but also to the CFLA, as location data have been recognised by the CNIL as personal data.

Under these considerations, commercial actors processing location data for marketing purposes through the means of RPAS would be regulated by the CFLA, and police officers using drones mounted with ANPR or GPS devices aiming to collect the location data of someone or track a target shall respect the CFLA and the Geo-localisation Act.

### *Summary*

Although the relevant French legislative instruments do not provide any specific provisions related to RPAS, we have seen in this analysis that different rules may apply to the different circles of the society. Public bodies (including law enforcement authorities), commercial organisations and other corporate operators (including journalists but with partial exemptions) using RPAS to collect data fall under the application of the data protection legislation, the CFLA. Second, the present analysis has also demonstrated that providers of telecommunication or Internet services that would like to use RPAS in the provision of services should also apply the rules of the Ordinance on electronic communications, more particularly the provisions related to the confidentiality, the security and data breach. This examination has shown that CCTV systems in public places are reserved to public bodies according to the Security Act while private users may only use CCTV systems to monitor their own property. If we take this approach by analogy to RPAS technology used for visual surveillance, this implies that *governmental drones* operated by law enforcement bodies are subject to the Security Act, as for any other type of surveillance. In addition, police officers using geo-localisation systems, such as ANPR shall apply the Geo-localization Act 2014. Finally, we observed through this detailed analysis that private users of drones when they use

---

<sup>225</sup> CNIL, Délibération No. 2013-404 Portant Avis ur un Projet de Loi Relatif à la Géolocalisation, 19.12.2013 (“CNIL Deliberation No. 2013 – 404”).

<sup>226</sup> French Parliament, The Geo-Localisation Act, 28.03.2014 (“French Geo-Localisation Act 2014”).

<sup>227</sup> Ibid.

<sup>228</sup> French Geo-Localisation Act.

<sup>229</sup> CNIL Deliberation No. 2013 – 404.

drones to capture personal information for household purposes are not regulated by the data protection legislation neither by CCTV laws. However, the French Civil law, the Criminal law and the Property law could be invoked to mitigate such issues. For instance, Article 9 of the Civil Code and Article 226-1 of the Criminal Code could be seen as answers to prevent private individuals equipped of surveillance camera to monitor outside of their own property.

#### 5.2.4 Germany

Under this present section, we will, firstly, discuss three privacy laws; Article 10 of the German Constitution encompassing implicitly the right to privacy, the Federal Data Protection Act covering the processing of personal data, and the Telecommunication Act regulating the telecommunication and internet services sector.

Regarding the surveillance legislation, we will examine particularly the Criminal Procedural Code and the G10 Act regulating the visual surveillance and the interception of communications by law enforcement authorities.

##### ***The privacy and data protection legislative framework***

###### a) The right to privacy: Article 10 of the German Constitution<sup>230</sup>

Whereas the Basic Law (the German Constitution) does not recognise explicitly a general right to privacy, Article 10 provides for the privacy of communications as it stipulates:

1. Privacy of letters, posts, and telecommunications shall be inviolable.
2. Restrictions may only be ordered pursuant to a statute. Where a restriction serves to protect the free democratic basic order or the existence or security of the Federation, the statute may stipulate that the person affected shall not be informed of such restriction and that recourse to the courts shall be replaced by a review of the case by bodies and auxiliary bodies appointed by Parliament.<sup>231</sup>

###### b) The personal data protection legislation: The Federal Data Protection Act 1977<sup>232</sup>

In Germany, data protection is regulated “by several laws and regulations which can be classified into the following categories:

Federal legislation:

- The Federal Data Protection Act
- Federal data protection regulations governing specific areas

State legislation:

- The data protection acts of the states
- State data protection regulations governing specific areas”<sup>233</sup>

---

<sup>230</sup> German Parliament, Basic Law for the Federal Republic of Germany, “Grundgesetz”, 23.05.1949 (“German Basic Law”), Article 10.

<sup>231</sup> German Basic Law, Article 10; Privacy International, EPIC and CMCS, 2010, p. 313.

<sup>232</sup> German Parliament, Federal Data Protection Act, “Bundesdatenschutzgesetz”, 20.12.1990 (“German DPA 1990”).

For the scope of this contribution, we will only analyse the Federal Data Protection Act. This Federal Data Protection Act (hereinafter, the FDP) has been amended many times, *inter alia*, in 2001 in order to implement the EU DPD 95/46. This Act covers the collection, processing, use of personal data executed by private bodies for commercial, corporate and professional purposes as well as by Federal public authorities and bodies, including judicial authorities. Regarding processing of data for journalistic purposes, Section 41 provides that only section 5 (confidentiality principle)<sup>234</sup> and section 9 (technical and organisational measures)<sup>235</sup> of the FDP applies. It should also be noted that when the security of the Federation is at stake, the law enforcement authorities processing data do not have to ensure individuals' rights.<sup>236</sup> Although the German Federal Data Protection Act does not explicitly cover civil RPAS technology, the rights and obligations described above shall a priori be respected. This means that the operator has to be granted with an authorisation by the German DPA and shall render the data anonymous or aliased as far the effort is not disproportionate to the desired purpose. As in UK and France, the German DPA does not cover the personal sphere and then, the German data protection law do not address the concerns that a private drone flight could pose by taking photographs or films.

In addition to the basic data protection principles<sup>237</sup>, the text provides for the anonymisation<sup>238</sup> and pseudonymisation<sup>239</sup> principles. The subject's rights are also reinforced compared to the DPD, for example, consent needs to be informed and written. The derogations are rare and very restricted. Furthermore, Section 5 provides a confidentiality maximal as it requires that each person employed for processing data has an authorisation.<sup>240</sup> It also stipulates that:

*apart from public bodies, private companies are now also required to appoint a data protection officer if they collect, process, or use personal information. Without this responsible person, each introduction of automated data processing must be registered with the Federal Commissioner for Data Protection and Freedom of Information (BfDI).*<sup>241</sup>

---

<sup>233</sup> The North Rhine-Westphalia Commissioner for Data Protection and Freedom of Information (LDI NRW), "Regulation of Data Protection", *Data Protection*, no date.

<sup>234</sup> The confidentiality principle provides that "Persons employed in data processing shall not process or use personal data without authorization": German DPA 1990, Section 5.

<sup>235</sup> Section 9 of the German DPA 1990 provides that technical and organisational measures shall be adopted by data collectors: "Public and private bodies processing personal data either on their own behalf or on behalf of others shall take the technical and organisational measures necessary to ensure the implementation of the provisions of this Act, in particular the requirements set out in the annex to this Act. Measures shall be required only if the effort involved is reasonable in relation to the desired level of protection".

<sup>236</sup> German DPA 1990, Section 19.

<sup>237</sup> See Part II of this deliverable.

<sup>238</sup> "Rendering anonymous" shall mean the alteration of personal data so that information concerning personal or material circumstances cannot be attributed to an identified or identifiable natural person, unless such attribution would require a disproportionate amount of time, expense and effort: German DPA 1990, section 3(6).

<sup>239</sup> "Aliasing" shall mean replacing the data subject's name and other identifying features with another identifier in order to make it impossible or extremely difficult to identify the data subject: German DPA 1990, Section 3.6(a).

<sup>240</sup> German DPA 1990, Section 5.

<sup>241</sup> Privacy International, EPIC and CMCS, op. cit., 2010, p. 314.

Under these last observations, it is easy to confirm that Germany holds one of the strictest data protection legislative regimes.<sup>242</sup>

c) Privacy in the telecommunication and Internet sectors: The Telecommunications Act 2004

In Germany, the Telecommunications Act covers the privacy of telecommunication. This Act regulates the telecommunication and network services and imposes some obligation on service providers. “Privacy of telecommunications” is expressly guaranteed by this Act under Section 88. According to this:

- (1) *The content and detailed circumstances of telecommunications, in particular the fact of whether or not a person is or was engaged in a telecommunications activity, shall be subject to telecommunications privacy. Privacy shall also cover the detailed circumstances surrounding unsuccessful call attempts*
- (2) *Every service provider shall be obliged to maintain telecommunications privacy. The obligation to maintain privacy also applies after the end of the activity through which such commitment arose.*
- (3) *Any person subject to the obligation according to (2) above shall be prohibited from procuring for himself or other parties any information regarding the content or detailed circumstances of telecommunications beyond that necessary for the commercial provision of telecommunications services.*<sup>243</sup>

Paragraph 4 of the same section seems to offer an interesting provision for the RPAS as it states, “Where the telecommunications system is located on board a ship or an aircraft, the obligation to maintain privacy does not apply in relation to the captain or his second in command.” Applied to the context of the civil RPAS technology, this Act seems to be suggesting that any service provider (regardless the operator) using RPAS to offer broadband or telecommunication services must meet the privacy principles.

Besides the secrecy contained within the Telecommunication Act, another section of the Act refers to the e-Privacy Directive. Section 87 requires:

*Whosoever operates telecommunications systems serving the commercial provision of telecommunications services shall take appropriate technical precautions or other measures with regard to telecommunications and data processing systems operated for such purpose in order to protect: 1. telecommunications secrecy and personal data; 2. programme-controlled telecommunications and data processing systems against unauthorised access; 3. systems against functional disruption resulting in considerable harm to telecommunications networks; and 4. telecommunications and data processing systems against external attack and the effects of natural disasters. Due regard shall be paid to state of the art technology.*<sup>244</sup>

Regarding the retention of data, before 2010, “telecommunications operators providing publicly available services were mandated to provide – at their own expense – the technical facilities required to implement telecommunications interception for law enforcement

---

<sup>242</sup> Ibid., p. 313.

<sup>243</sup> German Parliament, Telecommunication Act, 22.06.2004 (“German Telecommunication Act”), Section 88.

<sup>244</sup> Ibid., section 87.

purposes”.<sup>245</sup> Moreover, they had to keep all location and traffic data (data related to telecommunications and electronic communications) for a period of 6 months and made them available at the request of the law enforcement authorities. However, since 2010 Germany does not encompass regulation about the conservation of telecommunications data anymore, the law transposing the EU Data Retention directive having been annulled by the German Federal Constitutional Court. It resulted from this decision that “all retained telecommunications traffic data has to be deleted without undue delay and cannot anymore be transferred to law enforcement agencies”.<sup>246</sup>

### ***Surveillance regulations applicable to civil RPAS***

#### **a) Visual surveillance (CCTV systems) regulations: The Federal Data Protection Act 1977 and the Criminal Procedure Code (§201a)**

In Germany, there is no specific legal text governing video-surveillance, only numerous sectorial laws. Furthermore, the installation of cameras is regulated by each Länder. Against this background, this section will only point to the most relevant provisions.

First, regarding video surveillance operated by commercial entity and Federal public bodies, it is important to recall that the FDA, especially Section 6b, applies to recorded personal data. Section 6b covers “the monitoring in publicly accessible areas by optic-electronic devices”. In this context, this section should be applicable to govern the monitoring activities operated by civil RPAS as the cameras they carry for such activities should be recognised as “an optic-electronic device”. In the hypothesis, it applies to RPAS, the operator of this type of drone shall ensure their activities are necessary for one of the following purposes: *i)* for public bodies to perform their duties, *ii)* to exercise the right to determine who shall be allowed or denied access, or *iii)* to pursue legitimate interests for specifically defined purposes. The transparency obligation is also required as paragraph 2 and 4 stipulate that the public has to be aware they are monitored and, in case of collection of personal data, the identifiable or identified person shall be informed as well. Consequently, RPAS operators using drones equipped with visual photography equipment like a camera should respect these additional provisions.

Second, there are no CCTV regulations specific to the law enforcement sector. However, the Criminal Procedure Code (StPO) governs the use of covert visual surveillance technologies by the law enforcement sector in some circumstances. Section 100(c)(1)(b) explicitly allows investigators to use “technological means” to conduct visual surveillance of persons suspected of serious crimes.<sup>247</sup> The effect of this provision is that RPAS could probably fall inside the broad concept of “technological means”. Hence, according to this legal basis, the use of drones by public bodies for visual surveillance purposes is lawful in Germany.

Third, the use of automatic number plate recognition camera by law enforcement authorities to match the findings with a database of searched vehicles has been declared unconstitutional by the Court for violation of the finality and proportionality principles.<sup>248</sup> Nevertheless, it does not mean that drones mounted with ANPR cameras are totally prohibited in Germany.

---

<sup>245</sup> Privacy International, EPIC and CMCS, op. cit., 2010, p. 323.

<sup>246</sup> Privacy International, EPIC and CMCS, op. cit., 2010, p. 323.

<sup>247</sup> Ross, Jacqueline E., “Germany’s Supreme Court and the Regulation of GPS Surveillance”, *German Law Journal*, Vol. 06, No. 12, 2005, p. 1806.

<sup>248</sup> Privacy International, EPIC and CMCS, op. cit., 2010, p. 327.

They could “still make possible under narrowly described circumstances” and if these drones are used for determined purposes.<sup>249</sup>

b) Surveillance, tracking and access to communications regulations in the law enforcement sector: the Criminal Procedural Code, the G10 Act and the Surveillance Case Law of the German Federal Court

As already mentioned in the context of visual surveillance, the Criminal Procedural Code allows the law enforcement sector to execute surveillance missions (visual, tracking someone, interception of communications) in certain circumstances strictly defined. Therefore, although the secrecy of electronic communications, private conversations is a constitutional right and its violation is punished by the Criminal Code<sup>250</sup>, intercept electronic communications and listen to conversations in the case of crime investigation.<sup>251</sup> Besides the police, German Intelligence Services are also empowered of surveillance powers thanks to the G-10 Act. This latter allows “warrantless automated wiretaps of domestic and international communications by the national and states' Intelligence Services for purposes of protecting the freedom and the democratic order, preventing terrorism and illegal trade in drugs and weapons”.<sup>252</sup> Under these considerations and in the hypothesis these laws apply to the RPAS technology, this means that German police and intelligence services could be authorised to use civil drones to intercept communications when this is necessary for the investigation of crimes or to protect the national security.

Regarding tracking through geo-localisation systems, a German specialist in German data protection has recently issued an article where he explains:

*German Federal Court of Justice's case law on surveillance using GPS tracking systems can be applied to the scenario of civilian drones (see BGH, judgment from 04.06.2013 – 1 StR 32/13). The same restrictions that apply to the use of GPS tracking devices to conduct surveillance, apply to civilian drones. This is because there is a risk that civilian drones that make use of photography or filming technology could severely breach the personality rights of those being watched.*<sup>253</sup>

### **Summary**

Under this third section, we found that although there are no specific privacy provisions related to RPAS in Germany for now, some rules could apply to different operators of RPAS, such as public bodies, journalists, commercial and private users. This analysis pointed out that operators of commercial drones are a priori subject to the provisions of the Federal Data Protection Act when they process personal data. The Section 6b of this law may also regulate the use of drone for filming and recording individuals in public places. Telecommunication and network service providers using drones to carry their services are required to respect the Telecommunication Act.

---

<sup>249</sup> Ibid.

<sup>250</sup> German Parliament, the Criminal Code, “Strafgesetzbuch”, 13.11.1998, Sections 201-206 (“German Criminal Code 1998”).

<sup>251</sup> Privacy International, EPIC and CMCS, op. cit., 2010, p. 318-20.

<sup>252</sup> Ibid.

<sup>253</sup> Solmecke, Christian, “Civilian Drones and the Legal Issues Surrounding their Use”, *wbs-law blog online*, 18 February 2014. <http://www.wbs-law.de/internetrecht/civilian-drones-legal-issues-surrounding-use-50459/>

Second, we discussed that a public body using RPAS to process data must adhere to the principles and obligations of the FDPA. Moreover, when law enforcement authorities use drones for overt visual surveillance they have to respect Section 6b of the FDPA. In surveillance missions, law enforcement using RPAS to capture data and conversations have to ensure that they respect the Criminal Code and the Gt10. Furthermore, the German Federal Court encompassing a comprehensive jurisprudence on surveillance operated by GPS devices, civil drones mounted by such equipment for tracking shall also respect principles drawn out by such case laws.

Finally, we observed that the German legal framework does not contain any privacy legislation regulating the private use of domestic drones. Nevertheless, the German Private Property law and other rules figuring in the German Criminal Code could be invoked to prevent several applications including hacking and monitoring activities in public places.

### 5.2.5 Italy

In Italy, ENAC, the Italian CAA, has adopted an aviation regulation which is studied described in detail in Annex B. Besides these new rules, the present section examines whether the following privacy Italian acts apply to RPAS applications: Article 14 and 15 of the Italian Constitution, the Data Protection Code and the Electronic Communications Code, the Criminal Procedure Code and the Acts on International Terrorism.

#### ***The Privacy and data protection legislative framework***

##### a) The right to privacy: Article 14 and 15 of the Italian Constitution<sup>254</sup>

The Italian Constitution, adopted in 1948, protects the secrecy of communication (Article 15) and the inviolability of the personal home (Article 14) but there is no explicit recognition of “a stand-alone right of privacy”.<sup>255</sup>

##### b) The personal data protection legislation and the privacy in the telecommunication sector: The Data Protection Code 2003<sup>256</sup> and the Electronic Communications Code<sup>257</sup>

The Italian Data Protection Code (hereinafter, the DPC) implements not only the Data Protection Directive 95/46 but also the e-Privacy Directive 2002/58 and the Data Retention Directive 2006/24. Additionally, it includes relevant Codes of Conduct enacted by the Italian Data Protection Authority. Therefore, DPC regulates (i) personal data processing operations, (ii) the electronic communications network and service providers and (iii) the conservation of the location data and traffic data for law enforcement purposes.<sup>258</sup> Regarding the personal data protection rules, we emphasise that these rules apply to the data processing operations of both the private and public sectors.

Otherwise, the main principles are similar to those we found in the EU DPD 95/46. Whereas the DPC applies to the personal data related to the electronic communications (some traffic and location data), it is noteworthy that the Italian Electronic Communications Code

---

<sup>254</sup> Italian Parliament, Italian Constitution, 27.12.1947 (“Italian Constitution 1947”), Articles 14 and 15.

<sup>255</sup> Privacy International, EPIC and CMCS, op. cit., 2010, p.413.

<sup>256</sup> Italian Parliament, the Data Protection Code, 30.06.2003 (“Italian Data Protection Code 2003”).

<sup>257</sup> Italian Parliament, the Electronic Communications Code, 01.08.2003 (“Italian ECC 2003”).

<sup>258</sup> Italian Data Protection Code 2003.

(hereinafter, the ECC) provides some complementary rules regulating the electronic communications and telecommunications sector.<sup>259</sup> The EEC provides for the confidentiality principle as well as a requirement that service providers set up security measures for the prevention of any data breach. Regarding the retention of data related to telecommunications (traffic and location data), Article 132 of the DPC provides that such telecommunication data must be retained for a period of two years and the internet data for a duration of one year for the purpose of detecting and preventing crime. These data are transmitted upon the request of the competent authorities without undue delay. The application of these laws to RPAS technology means that when an RPAS captures personal data or carries a communication system in Italy, operators of such RPAS shall respect the principles, rights and obligations set out in the DPC and the ECC. For other activities operated by RPAS that may prove to be privacy intrusive, Article 14 and 15 of the Italian Constitution grant individuals a general protection against any intrusion in their personal domicile or private communications.

### ***The surveillance regulations applicable to civil RPAS***

#### **a) Visual surveillance (CCTV systems) regulations: many sectorial laws**

There is no CCTV law in Italy relating to video-surveillance. Nevertheless, there are many sectorial regulations regulating the use of the “videovergianza”.<sup>260</sup> These govern the installation and use of video cameras by individuals and within public and private sectors. Operators of RPAS shall respect all the rights and obligations enshrined in these regulations, although the prohibition of some uses and the extent to which the law applies depend on the drones operator, namely whether the operator is a journalist, private person using the RPAS for personal uses, or the police. Irrespective of this, we can already observe that visual surveillance in Italy may only be exercised for the following purposes:

*(1) protection and integrity of individuals – including urban security; public order; public bodies' prevention, detection and/or suppression of offences; streamlining and improving publicly available services also in order to enhance user safety; (2) protection of property; (3) detecting, preventing and controlling breaches of the law; (4) gathering of evidence.*<sup>261</sup>

Individuals monitored by drones in public places, such as banks, and shops, shall be informed by operators who are also required to obtain authorisations. However, the public sector can derogate from this transparency principle when drones are used for monitoring individuals for security or public order purposes.<sup>262</sup>

Where drones capture footage for security or public order purposes, these images may not be retained for more than seven days, and should be destroyed after this time unless they concern terrorist activities. By contrast, images captured by RPAS operated by public authorities, companies or individuals for other purposes may be kept for only 24 hours. In conformity

---

<sup>259</sup> Ibid.

<sup>260</sup> Italian Parliament, Decree on the Visual Surveillance, 08.04.2010 (“Italian Decree on Video Surveillance 2010”); Italian Parliament, General Decree on the Visual Surveillance, 29.04.2004; Italian Parliament, Decree on the Visual Surveillance Respecting the Privacy, 29.12.2000.

<sup>261</sup> Italy, Decision Garante per la Protezione dei dati personali, Video Surveillance, 08.04.2010; Cocq, Céline and Francesca Galli, *Surveillance: Deliverable 4.1: The use of Surveillance Technologies for the Prevention and Investigation of Serious Crimes*, European Commission, Brussels, 2012.

<sup>262</sup> Ibid.

with the personal data protection laws, RPAS fitted with video cameras that have recorded images or films showing the identity of an individual are governed by the DPC, in particular Article 134, as well as by the 2010 regulation on video-surveillance and personal data.<sup>263</sup>

b) Surveillance, wiretapping and access to communications regulations: Criminal Procedure Code<sup>264</sup> and the Acts on the International Terrorism 2001 - 2005<sup>265</sup>

As discussed above, confidentiality of communications is a constitutional right. However, this right is subject to several derogations afforded to the law enforcement sector. The Italian wiretapping regime distinguishes post-delictum and ante-delictum interceptions. *Post-delictum wiretapping* is only authorised in the context of a “legal proceeding” and in relation to most serious offences under Articles 266-271 of the Criminal Procedure Code (Codice di Procedura Penale or CPP)<sup>266</sup>. *Ante-delictum wiretapping* is referred to in the Law 431/2001<sup>267</sup> and Law 155/2005<sup>268</sup> on International Terrorism, which provides that such interceptions are only permitted in the case of terrorism or organised crimes investigations. However, the requirements here are less stringent. For example, blanket surveillance of communications can be conducted by law enforcement bodies even if no Public Prosecutor investigation is on-going.<sup>269</sup> Moreover, unlike to post-delictum telephone tapping, ante-delictum interceptions are not subject to authorisation and do not need to be exercised under the supervision of judicial authorities. Additionally, there exist some sectorial texts that provide “common provisions as well as special regimes for wiretapping and surveillance law”.<sup>270</sup>

Law enforcement bodies must adhere to regulations governing both visual and non-visual surveillance in their operations. Whereas the operators of overt visual surveillance have some subject’s rights to respect (transparency), covert surveillance (visual and non-visual such as the wiretapping) is generally subject to authorisations.

### **Summary**

Some Italian privacy laws may apply to the RPAS technology even if they do not encompass any specific rules governing this latter. First, this section has shown that nothing prevents the application of the Data Protection Code to a commercial operator of drones. Regarding the potential providers of Internet and Telecommunication service using drones as proxy-satellites, the Data protection Code could even be complemented by the Electronic Communication Code. Second, it appears that Italian journalists who intend to use drones for journalistic purposes should refer to the Data Protection Code even if this Code affords some exemptions to such operators. Third, we have seen that public authorities are also subject to the Data Protection Code when they use drones for processing data. In surveillance, we have seen two texts regulate their surveillance missions. Hence, we can expect that Criminal Procedure Code and the Acts on the International Terrorism will apply to the blanket surveillance operated by drones as well. Finally, like in other Members States, private users

---

<sup>263</sup> Italian Decree on Visual Surveillance 2010.

<sup>264</sup> Italian Parliament, Criminal Procedure Code, 21.04.2014 (“Italian Criminal Procedure Code 2014”).

<sup>265</sup> Italian Parliament, Acts on the International Terrorism, 14.12.2001 (“Italian Terrorism Act 2001”).

<sup>266</sup> Italian Criminal Procedure Code 2014, Articles 266-271.

<sup>267</sup> Italian Terrorism Act 2001.

<sup>268</sup> Ibid.

<sup>269</sup> Privacy International, EPIC and CMCS, op. cit., 2010 p.422.

<sup>270</sup> Ibid.

using drones to process data for domestic purposes are not subject to the Data Protection Code and remain unregulated in this context.

## 5.2.6 Sweden

### **General**

The Swedish Transport Agency has issued an Act governing civilian RPAS in 2013<sup>271</sup>. It requires that operators hold a permission for commercial and research and development using drones.<sup>272</sup> Regarding law enforcement, it requires that they have “the right authorization, and that it is used when a preliminary investigation has been opened”<sup>273</sup> while hobbyist do not need permission. Although this Act provides that civilian RPAS are limited to flying within sight of the pilot, and at a height lower than that at which most manned vehicles fly, there are no specific privacy measures included in the Act.<sup>274</sup>

Therefore, this is section devoted to the study of the Swedish privacy and surveillance regimes. We will firstly study the right to privacy, the Personal Data Act 1998 and the Electronic Communications Act 2011. Furthermore, we will examine the Camera Surveillance Act 2013 and the Swedish Code of Judicial Procedure,.

### ***The privacy and data protection legislative framework***

#### a) The right to privacy: Article 3 and 6 (Chapter 2) of the Instrument of Government

In Sweden, the Constitution consists of four fundamental legal texts: the Instrument of Government, the Act of Succession, the Freedom of the Press Act, and the Fundamental Law of Freedom of Expression.<sup>275</sup> The right to privacy is explicitly enshrined at Article 6, Chapter 2 of the Instrument of Government Act of 1974: “*Every citizen shall be protected in his relations with the public institutions against any physical violation also in cases other than cases under Articles 4 and 5. He shall likewise be protected against body searches, house searches and other such invasions of privacy, against examination of mail or other confidential correspondence, and against eavesdropping and the recording of telephone conversations or other confidential communications.*”<sup>276</sup> At the same chapter, Article 3 we can also find a right to protection of personal integrity (privacy) in relation to automatic data processing.<sup>277</sup> The European Convention on Human Rights (ECHR) is part of the Swedish law since 1994. Although the “ECHR is not formally part of the Swedish Constitution, it has, in effect, similar status”.<sup>278</sup>

#### b) The personal data protection legislation: the Personal Data Act 1998 (Personuppgiftslag)

---

<sup>271</sup> Sweden, Föreskrifter om ändring i Transportstyrelsens föreskrifter om verksamhet med obemannade luftfartyg (UAS), 15.03.2013.

<sup>272</sup> Ibid.

<sup>273</sup> The Local, “Swedish police want investigation drones”, <http://www.thelocal.se/20140123/swedish-law-lags-drone-trend>

<sup>274</sup> Ibid.

<sup>275</sup> Privacy International, EPIC and CMCS, op. cit., 2010, p. 736.

<sup>276</sup> Sweden, The Instrument of Government, “Svensk författningssamling”, 1974.

<sup>277</sup> Privacy International, EPIC and CMCS, op. cit., 2010, p. 736.

<sup>278</sup> Ibid..

Being a member of the European Union, Sweden implemented the EU Data Protection Directive 95/46/EC in 1998 with the Swedish Personal Data Act (*personuppgiftslagen*), which regulates activities processing personal data. This is also supplemented by the Data Protection Ordinance and the Statute Book of the Data Inspection Board (Swedish DPA).

The PDA, in conformity with the European Directive, applies to all processing of personal data as is wholly or partly automated and, “in certain cases, manual processing of personal data on traditional paper-based files”<sup>279</sup> by public authorities as well private entities. The concept of *personal data* comprises all types of “personal data, that is, data that are directly or indirectly (that is, used in conjunction with other data) referable to an existing natural person”.<sup>280</sup>

Regarding to the scope, we found the *standard exemptions* in the DPA. One concerns the processing of personal data by private persons for household purposes for which the DPA does not apply at all. The second exemption regards processing activities for journalistic (artistic and literary expression) purposes for which the majority of the articles do not apply.

Structured as the DPD 95/46/EC, Section 9 of the PDA enshrines the *core data protection principles* and section 10 clarifies the lawfulness principle (for certain processing, the consent is required. It must be a voluntary, specific and unambiguous expression of will<sup>281</sup>). Section 13 prohibits the processing of several categories of data (*standard sensitive data and legal offences*<sup>282</sup>) unless the standard conditions for processing sensitive data are met.

There also exists a *duty to notify* the Swedish Data Protection Authority (Data Protection Board). “The notification must occur prior to the first processing of personal data. There is no charge for notification”.<sup>283</sup> However, “the notification duty only includes processing of data that is completely or partially automated”<sup>284</sup> and it encompasses several broad exemptions. For example, the duty to notify does not apply if the data subject has given its consent to the processing. Nevertheless, the notification is mandatory when data processing regards the integrity of the person.<sup>285</sup>

Amongst the *individual rights* of the data subject we found: the right to fair processing information, the right to access, the right to prevent further processing, the right to object to direct marketing and the rights to delete, rectify and block data unlawfully processed.

Finally, the data controller must comply with the *general data security principle* (and “undertake technical and organisational measures” to ensure data security). “This also applies when processing personal data in accordance with the Unstructured Material Rule”<sup>286</sup> (images

---

<sup>279</sup> Wiking Häger, Erica and Anna, Mirsch, “Data Protection Multi-jurisdictional Guide - Data protection in Sweden: overview”, <http://us.practicallaw.com/8-502-0348#a571787>

<sup>280</sup> Ibid.

<sup>281</sup> Sweden, Section 10 of the Data Protection Act, “Datainspektionen “, 29.04.1998 and Linklaters, “Data Protection – Sweden”, <https://clientsites.linklaters.com/Clients/dataprotected/Pages/Sweden.aspx>

<sup>282</sup> “Data concerning legal offences may, subject to a few exemptions, only be processed by public authorities unless permission is granted by the Data Inspection Board”, Linklaters, “Data Protection – Sweden”, 2014. <https://clientsites.linklaters.com/Clients/dataprotected/Pages/Sweden.aspx>

<sup>283</sup> Linklaters, “Data Protection – Sweden”, 2014.

<sup>284</sup> Ibid.

<sup>285</sup> Sweden, Section 41 of the Data Protection Act, “Datainspektionen “, 29.04.1998

<sup>286</sup> Linklaters, “Data Protection – Sweden”, 2014.

and sounds). Nevertheless, there is no mandatory requirement in the Act to report data security breaches or losses to the data protection authority. “Data security breaches are handled on a case-by-case basis and addressed by the DIB only if they for instance relate to a large number of data subjects or indicate a general non-compliance issue. There is no DIB guidance on the subject matter”<sup>287</sup>.

c) Privacy in the telecommunication and Internet sectors: The Electronic Communications Act (Sw. lagen om elektronisk kommunikation) 2011

The Electronic Communications Act (*Sw. lagen om elektronisk kommunikation*) was amended on 1 July 2011 to implement the amendments to the Privacy and Electronic Communications Directive (e-Privacy Directive).<sup>288</sup>

The principle of *confidentiality* of communications is enshrined in Article 20 and the prohibition of wire-tapping at Section 17 and the use of secret wire-tapping at Section 19.<sup>289</sup> Therefore the confidentiality principle encompasses some derogations including the exemption related to wiretapping by law enforcement authorities for security and criminal investigation purposes<sup>290</sup>.

Regarding the security principle, there is a standard duty to undertake security measures. Furthermore, a specific notice of breach requirements applies to the electronic communications sector in accordance with the amendments to the Privacy and Electronic Communications Directive.<sup>291</sup>

Finally, there are additional requirements that apply when traffic data and location data are processed. For example, traffic data shall be eradicated or prevented from being identifiable (*anonymous principle*) when it is no longer necessary to transfer an electronic message<sup>292</sup> and location data may only be processed after it has been prevented from being identifiable or the user or subscriber has given his or her consent to the processing (*consent requirement*).<sup>293</sup>

---

<sup>287</sup> Henrik Nilsson, “Data Protection and Privacy in 26 jurisdictions worldwide”, in Getting the Deal Through, Rosemary P Jay (Eds.), 2014.

<sup>288</sup> Linklaters, “Data Protection – Sweden”, 2014.

<sup>289</sup> Sweden, Section 20 of the The Electronic Communications Act “Sw. lagen om elektronisk kommunikation”, 25.07.2003.

<sup>290</sup> Ibid.

<sup>291</sup> “Section 3. A party that provides a public electronic communications service shall implement appropriate measures to ensure that the data processed is protected. A party that provides a public communications network shall implement those measures that are necessary to maintain the protection within the network. These measures shall be intended to ensure a level of security that, taking into account the available technology and costs for implementation of the measures, is adapted to the risk to infringement of privacy. Section 4 If, upon the provision of a public electronic communications service, there is a particular risk for inadequate protection of data processed, the party providing the service shall inform the subscriber about the risk. If the party that provides the service is not liable under Section 3 to remedy the risk, the subscriber shall be informed about how and at what approximate cost the risk can be remedied”. Sweden, Section 3 and 4 of the The Electronic Communications Act “Sw. lagen om elektronisk kommunikation”, 25.07.2003.

<sup>292</sup> Sweden, Section 5 of the The Electronic Communications Act “Sw. lagen om elektronisk kommunikation”, 25.07.2003.

<sup>293</sup> Sweden, Section 9 of the The Electronic Communications Act “Sw. lagen om elektronisk kommunikation”, 25.07.2003.

### ***Surveillance regulations applicable to civil RPAS***

**a) Overt visual surveillance (CCTV systems) regulations: The Camera Surveillance Act 2013**

The Camera Surveillance Act regulates the use of equipment for audio-visual monitoring and surveillance. Different rules apply according to whether the surveillance is operated in public or private spaces.

In areas where the public has access, monitoring requires a *license* from the County Administrative Board in the current county. This latter specifies that “If it is a shop, bank, post office, multi-storey car park or underground station which is to be monitored, you need to submit an application to us. This application must contain detailed information about the planned system and surveillance area”.<sup>294</sup> It is noteworthy that this requirement applies even for the police; they need a license for CCTV installations. “When applying for a permission the interest for monitoring is weighed against the interest for integrity. An application can be granted in part or as a whole or only for a limited period of time” states the Lansstyrelsen.<sup>295</sup>

We found also in this Camera Act a *purpose limitation* principle; installation may only be for crime prevention and detection reasons. Furthermore, there is a requirement to inform the public of the presence of surveillance systems by signposting outside of the surveillance area.<sup>296</sup> In addition, the Act also requires the cameras must be fixed and may not have a zoom function. To monitor on private places, you do “not need a license to monitor enclosed areas within companies, industrial processes, rooms in the home or similar. The crucial factor is that the public does not have access to the area”.<sup>297</sup> Finally, the CCTV Act is enforced by the County Administrative Board that “monitors that the regulations are being followed, including by visiting those areas to which the public has access”.<sup>298</sup>

**b) Covert visual surveillance (CCTV systems) regulations: Chapter 27 of the Swedish Code of Judicial Procedure.**

In case of use of secret camera surveillance, the Swedish Code of Judicial Procedure applies. According to this code, covert camera surveillance means that remote-controlled TV cameras or other comparable electronic equipment are used for visual surveillance of persons in preliminary investigations without providing notification of the surveillance.<sup>299</sup> Law enforcement bodies are the sole entity legally permitted to perform covert surveillance. They need a warrant and “the surveillance may only apply to a place where it can be assumed that the person reasonably suspected of an offence will be present. If there is no one who is

---

<sup>294</sup> Lansstyrelsen, Camera surveillance (CCTV), <http://www.lansstyrelsen.se/stockholm/En/manniska-och-samhalle/kameraovervakning/Pages/default.aspx>

<sup>295</sup> Ibid. and Marianne L. Gras, The Legal Regulation of CCTV in Europe”, in CCTV Special, Norris, McCahill and Wood (Eds.), *Surveillance & Society*, 2(2/3), 2004, pp. 216-229.

<sup>296</sup> Gras, op. cit., 2004.

<sup>297</sup> Lansstyrelsen, Camera surveillance (CCTV), <http://www.lansstyrelsen.se/stockholm/En/manniska-och-samhalle/kameraovervakning/Pages/default.aspx>

<sup>298</sup> Ibid.

<sup>299</sup> Chapter 27 Section 20a of the Swedish Code of Judicial Procedure and CoE committee of experts on terrorism (codexter), “Profiles on counter-terrorism capacity – Sweden”, [http://www.coe.int/t/dlapil/codexter/Country%20Profiles/Profiles-2014-Sweden\\_EN.pdf](http://www.coe.int/t/dlapil/codexter/Country%20Profiles/Profiles-2014-Sweden_EN.pdf)

reasonably suspected of the offence, covert camera surveillance may be used to monitor the place where the offence has been committed or an area close to this place in order to establish who may be reasonably suspected of the offence”.<sup>300</sup>

c) Surveillance, tracking and access to communications regulations in the law enforcement sector: Chapter 27 of the Swedish Code of Judicial Procedure.

The covert interception of telecommunications and the covert telecommunications surveillance are also regulated by Chapter 27 of the Swedish Code of Judicial Procedure. The covert interception of telecommunications “*concern messages that are transmitted, or have been transmitted to or from a telephone number or other address within an electronic communication network are secretly listened to or recorded by means of technical devices in order to relate the content of the message*”.<sup>301</sup> Covert telecommunications surveillance “*means that information is secretly obtained about a) messages within an electronic communication network that are transferred or have been transferred to or from a telephone number or other address, b) what electronic communication equipment that have been present within a certain geographical area) in what geographical area a certain electronic communication equipment is or has been present. Covert telecommunications surveillance can also be used in order to prevent messages mentioned under a) from reaching their destination. Information on the contents of messages is not included in this form of coercive measure*”.<sup>302</sup> For both, a court order is needed by the law enforcement agencies before the surveillance operation commences. Such surveillance measures may be only used “if a person is reasonably suspected of an offence and the measure is of exceptional importance to the investigation of the offence”.<sup>303</sup> Furthermore, the Code requires that they are undertaken under some specific and legally limited grounds.<sup>304</sup>

Finally, it is noteworthy that Sweden has passed a new internet law (FRA law) in 2009. This authorized the National Defence Radio Establishment (Swedish government agency) “to monitor all cable-bound communications traffic into and out of Sweden, including emails, text messages and telephone calls. FRA is now alleged to engage in intercepting and storing communications data from fibre-optic cables crossing Swedish borders from the Baltic Sea. The metadata are retained in bulk and stored in a database for a period of 18 months”.<sup>305</sup>

### **Summary**

The analysis of the Swedish national regimes found that drones’ operators have to respect the right to privacy of individuals enshrined at Article 3 and 6 (Chapter 2) of the Instrument of Government. Furthermore, like any other Member States, the ECHR is incorporated in the

---

<sup>300</sup> Ibid., Chapter 27 Section 20a

<sup>301</sup> Ibid., Chapter 27 Section 18

<sup>302</sup> Ibid., Chapter 27 Section 19

<sup>303</sup> Chapter 27 of the Swedish Code of Judicial Procedure and CoE committee of experts on terrorism (codexter), “Profiles on counter-terrorism capacity – Sweden”,

<sup>304</sup> Chapter 27 of the Swedish Code of Judicial Procedure and CoE committee of experts on terrorism (codexter), “Profiles on counter-terrorism capacity – Sweden”,

<sup>305</sup> European Commission, Directorate General For Internal Policies Policy Department C: Citizens' Rights And Constitutional Affairs, Civil Liberties, Justice And Home Affairs, “National Programmes For Mass Surveillance Of Personal Data In Eu Member States And Their Compatibility With Eu Law”, [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE\\_ET\(2013\)493032\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf)

Swedish privacy regime, so RPAS operators have to respect it as well as its related case-law. We also demonstrated that RPAS operators who collect personal information during commercial operations have to respect the **Swedish Personal Data Act**. In addition, if they want to use a drone equipped with a video camera, they have also to respect the Camera Surveillance Act, which requires commercial operators to respect tailored specific standards, such as requiring a license from the County Administrative Board. State agencies also have to respect the **Swedish Personal Data Act** when they use a RPAS to collect personal information even if they are exempted from several provisions. Furthermore, they also have to respect the Camera Surveillance Act if they use a drone equipped with a surveillance camera in public places. In case of use of RPAS equipped with a visual or non-visual payload in a secret surveillance context, state agencies are subject to the specific surveillance legislation applying to the law enforcement sector, the Chapter 27 of the Swedish Code of Judicial Procedure in addition to the **Personal Data Act**. Swedish telecommunication and Internet providers fall under the provisions of the Electronic Communications Act whether they use a drone as a proxy-satellite. Regarding to private individuals using RPAS for personal activities and hobbyists, they are exempted from the **Swedish Personal Data Act**. **Instead, only the right to privacy and some patchy privacy-oriented rules in other civil law, like property law, will apply.**

### 5.2.7 Denmark

#### *General*

In Denmark, RPAS operations operating in the visual line of sight (VLOS) “are generally legal under the model aircraft regulation, also for commercial purposes. However, exemptions are issued to an increasing number of professional operators that need further operational possibilities – flying closer to roads, inhabited areas etc.”, explains the managing director of Hans Christian Andersen Airport in Denmark.<sup>306</sup> In the present section we will examine the privacy and surveillance regimes currently working in Denmark. We will study the right to privacy enshrined in the Danish Constitution 1953, the Act on Processing of Personal Data 2000 and Act on Electronic Communications and Network Services 2011. Furthermore, we will analyse the Act on TV surveillance of 2007 and the Administration of Justice Act 2008.

#### *The privacy and data protection legislative framework*

##### a) The right to privacy: Danish Constitution 1953

Although the right to privacy is not expressly mentioned in the Danish Constitution of 1953, it contains two provisions relating to privacy and, indirectly, to data protection. Section 71 requires the inviolability of personal liberty while Section 72 states *“The dwelling shall be inviolable. House searching, seizure, and examination of letters and other papers as well as any breach of the secrecy to be observed in postal, telegraph, and telephone matters shall take place only under a judicial order unless particular exception is warranted by Statute.”*<sup>307</sup> It is noteworthy that Section 72 also applies to all kinds of telecommunication

---

<sup>306</sup> UAS Vision, “The European Approach to Civil RPAS at the RPAS 2014 Conference”, <http://www.uasvision.com/2014/05/27/the-european-approach-to-civil-rpas-at-the-rpas-2014-conference/> and Civil Aviation Administration, Regulations on unmanned aircraft not weighing more than 25 kg, 09.01.2004.

<sup>307</sup> Denmark, Section 72 of the Danish Constitution, 05.06.1953.

and electronic data.<sup>308</sup> Finally, the Danish law has incorporated the European Convention on Human Rights (ECHR) in 1992.

**b) The personal data protection legislation: Act on Processing of Personal Data 2000**

The Act on Processing of Personal Data (DPA, hereafter) of 31 May 2000 implements the [Data Protection Directive](#). It applies to all electronic processing and manual files and in the private sector, it also applies to systematic manual processing<sup>309</sup> (i.e. data that is viewed as private in the penal code section 264d). Furthermore, it covers CCTV surveillance systems.<sup>310</sup>

Regarding to its scope, the Act encompasses the two standard exemptions related to domestic processing (wholly exempted) and journalistic processing (partially exempted)<sup>311</sup>. Besides these exemptions, the Act does also not cover the following: processing in accordance with article 10 of the human rights convention, parliament and institutions under parliament, the secret services.<sup>312</sup> Furthermore, “certain of the data subject rights do not apply to the police and the courts in criminal proceedings. These rights are regulated in the Administration of Justice act”<sup>313</sup>.

Recalling that the DPA has implemented the European Directive, we found the [standard conditions for processing personal data](#).<sup>314</sup> Among the legitimate grounds under which data may be processed, we found, that consent was required. Therefore, drones operators do not absolutely need the consent of the data subject, for example the presence of a contract would be sufficient. Like in the European Directive, categories of data (*sensitive data*) require additional protective safeguards for being processed. Among these latter, we found biometric information and information that concerns the health of an individual.<sup>315</sup> The Danish DPA recognises also *semi-sensitive data* which includes the criminal offences, serious social problems and purely private matters.<sup>316</sup>

Although the duty to notify is mandatory<sup>317</sup>, the DPA does not contain any specific obligation to inform the Agency or [data subjects](#) of a security breach. “However, in practice, the Agency has interpreted the obligation to comply with good practices of processing data as requiring

---

<sup>308</sup> Privacy International, the Electronic Privacy Information Center (EPIC) and the Center for Media and Communications Studies (CMCS), European Privacy and Human Rights (EPHR) 2010.

<sup>309</sup> Denmark, Section 1(2) concerning personal data of a private nature, The Act on Processing of Personal Data, 31.05.2000.

<sup>310</sup> Denmark, Section 1(8) concerning personal data of a private nature, The Act on Processing of Personal Data, 31.05.2000.

<sup>311</sup> Denmark, Section 2 of the Act on Processing of Personal Data, 31.05.2000.

<sup>312</sup> Denmark, Section 2 of the Act on Processing of Personal Data, 31.05.2000.

<sup>313</sup> European Commission, Directorate General For Internal Policies Policy Department C: Citizens' Rights And Constitutional Affairs, Civil Liberties, Justice And Home Affairs, “National Programmes For Mass Surveillance Of Personal Data In EU Member States And Their Compatibility With Eu Law”, [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE\\_ET\(2013\)493032\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf) and Denmark, Section 2 of the Act on Processing of Personal Data, 31.05.2000.

<sup>314</sup> Denmark, Section 5 and 6 of the Act on Processing of Personal Data, 31.05.2000.

<sup>315</sup> Denmark, Section 7 of the Act on Processing of Personal Data, 31.05.2000.

<sup>316</sup> Linklaters, “Data Protection – Denmark”, 2014.

<https://clientsites.linklaters.com/Clients/dataprotected/Pages/Denmark.aspx> and Denmark, Section 7 of the Act on Processing of Personal Data, 31.05.2000.

<sup>317</sup> Denmark, Chapters 12 and 13 of the Act on Processing of Personal Data, 31.05.2000.

a [data controller](#) to notify [data subjects](#) of any unintended publication of personal data”.<sup>318</sup> Moreover, the Act provides that for some specific processing activities including the combination of data, an Opinion from the Danish DPA is needed prior the execution of processing (prior-checking).<sup>319</sup>

In terms of security measures, “the DPA requires that [data controllers](#) apply the [general data security obligations](#). Furthermore, the Agency has issued guidance on its website which deal with the security in connection with transmission of personal data via the internet in the private sector. The Agency requires that confidential information and information which is deemed confidential is encrypted when the information is sent via webpages. Further, the Agency recommends that a strong encryption is used if sensitive or confidential data is being sent via e-mail”.<sup>320</sup>

Finally, regarding to the individuals rights, the Danish rules are similar to those of the Directive (fair information, right to be informed, right to access, right to object to direct marketing processing, right to rectify, erasure, etc.).

c) Privacy in the telecommunication and Internet sectors: Act on Electronic Communications and Network Services 2011

The ePrivacy Directive, as amended, has been implemented in the Danish law through the adoption of the Act on Electronic Communications and Network Services of 3 March 2011. This Act provides the obligation for Internet and telecommunication providers to respect the *secrecy of communications*<sup>321</sup> with a standard derogation for the law enforcement sector.<sup>322</sup> Furthermore, they have also to “*appropriate technical and organisational measures for the purpose of managing the risks posed to the information security of networks and services*”<sup>323</sup> (security principle) and to notify eventual data breaches to the Danish DPA<sup>324</sup>. However, we cannot find any article related to specific requirements for processing location and traffic data (no obligation to render anonymous, encrypted).

***Surveillance regulations applicable to civil RPAS***

a) Overt visual surveillance (CCTV systems) regulations: the Act on Processing of Personal Data 2000 and the Act on TV surveillance 2007

The Data Protection Act expressly states that it applies to any processing of personal data in connection with video surveillance. Therefore only RPAS recording personal data are subject to this Act. There is a whole Chapter 6a devoted to the video surveillance which specifies certain principles when data are processed in this context. For example, it affords a stricter purpose limitation principle as it requires that “*Disclosure of image and sound recordings containing personal data, which are recorded in connection with video surveillance for*

---

<sup>318</sup> Linklaters, “Data Protection – Denmark”, 2014.

<sup>319</sup> Denmark, Sections 45 and 50 of the Act on Processing of Personal Data, 31.05.2000.

<sup>320</sup> Linklaters, “Data Protection – Denmark”, 2014. and Denmark, Section 41 of the Act on Processing of Personal Data, 31.05.2000

<sup>321</sup> Denmark, Article 7 of the Act on Electronic Communications and Network Services, 03.03.2011.

<sup>322</sup> Denmark, Article 10 of the Act on Electronic Communications and Network Services, 03.03.2011.

<sup>323</sup> Denmark, Article 8(2) of the Act on Electronic Communications and Network Services, 03.03.2011.

<sup>324</sup> Denmark, Article 8(2) of the Act on Electronic Communications and Network Services, 03.03.2011.

*criminal prevention purposes may only take place if the data subject has given his explicit consent, or the disclosure follows from law, or the data are disclosed to the police for crime-solving purposes*".<sup>325</sup> Contrary to other processing activities, it also stipulates that data can only be retained for a maximum of 30 days after what they must be erased.<sup>326</sup> However, there is no longer a duty to notify the Data Protection Agency prior to installing surveillance equipment.

Besides the Danish DPA, the visual surveillance is also regulated by the Act on TV surveillance of 2007. This latter replaced the previous Act Prohibiting Video Surveillance. Unlike the DPA, this Act applies whether or not the pictures are stored or recorded. Therefore, drones mounted with a camera are subject to such law. "TV surveillance is defined as systematic and continuous surveillance of persons via remote-controlled or automatic cameras. General surveillance of *public areas* such as public streets and squares are not allowed for private parties, however the police may perform surveillance in any public area if it is found necessary to prevent or investigate crime. The police may set quality standards for the recordings".<sup>327</sup> Regarding to *private places*, the Act only "gives private enterprises such as banks, gas stations, hotels, and shops extended powers to perform surveillance on areas related to their property"<sup>328</sup>. Furthermore, there is a duty to inform people via signs that there is TV surveillance in the area.

Briefly, we can summarize such considerations by saying that Danish operators capturing personal information through a drone equipped with a camera must ensure the DPA, particularly the specific strict rules of Chapter 6a, and the Act on TV surveillance are respected. However, it is noteworthy that no provision in either act contains information on mobile cameras specifically, so we can only presuppose that they will apply to drones equipped with a visual payload.

b) Covert visual surveillance: Section 791a of the Administration of Justice Act 2008

Covert visual surveillance performed by law enforcement bodies is regulated by the Section 791a of the Administration of Justice Act. This later provides that the police may operate *surveillance* on persons who are in a not freely accessible place by means of a *remotely controlled* or automatic camera, TV camera or similar equipment if the investigation concerns an offence punishable under the law with imprisonment for one year and six months or longer.<sup>329</sup> Regarding the surveillance of individuals operated in a home or other premises by means of a *remotely controlled* or automatic camera, TV camera or similar equipment or by means of a device used in the home or the premises, the rules are stricter and imposes very strict *purposes limitations*.<sup>330</sup>

---

<sup>325</sup> Denmark, Section 26a (1) of the Act on Processing of Personal Data, 31.05.2000.

<sup>326</sup> Denmark, Section 26a (3) of the Act on Processing of Personal Data, 31.05.2000.

<sup>327</sup> Denmark, Act on TV surveillance, 11.10.2007 and Privacy International, the Electronic Privacy Information Center (EPIC) and the Center for Media and Communications Studies (CMCS), European Privacy and Human Rights (EPHR) 2010.

<sup>328</sup> Denmark, Act on TV surveillance, 11.10.2007 and Privacy International, the Electronic Privacy Information Center (EPIC) and the Center for Media and Communications Studies (CMCS), European Privacy and Human Rights (EPHR) 2010.

<sup>329</sup> Denmark, Section 791a (2) of the Administration of Justice Act, 06.11.2008.

<sup>330</sup> Denmark, section 791a (3) of the Administration of Justice Act, 06.11.2008.

**d) Surveillance, tracking and access to communications regulations in the law enforcement sector: Section 780 and foll. of the Administration of Justice Act 2008**

As we have seen that drones are also able to capture information electronic communications and sounds, it is relevant to examine the Danish wiretapping law. Of course although such surveillance operations are prohibited for commercial and private drones' operators, law enforcement bodies are exempted in certain circumstances.

In Denmark, the interception of communications by the police, including the Security Intelligence Service is also governed by the Administration of Justice Act (Section 780 and foll.). This Act covers different types of interception of communications - telephone tapping, other interception (bugging), traffic data, extended telecommunications records (such as transmission mast data) and the opening and stopping of letters- and set up specific requirements. Among these requirements, we found the obligation to have a warrant (accountability principle)<sup>331</sup>, a strict purpose limitations principle<sup>332</sup>, a kind of necessary principle<sup>333</sup>, a requirement as to the nature of the crime<sup>334</sup> and a proportionality principle<sup>335</sup>.

In practice, the amendment of the Act on Administration of Justice increased the police surveillance mandate by allowing them to access to a list of all active mobile phones near the scene of a crime at the time the crime was committed.<sup>336</sup>

***Summary***

The analysis of the Danish national privacy legislation has shown that any operators using RPAS have to respect the right to privacy of the individuals enshrined at Section 72 of the Danish Constitution. Commercial operators have to ensure they comply with the Danish Act on Processing of Personal Data in circumstances where they collect personal information with their RPAS. Furthermore, we have seen that those which use a drone equipped with a video camera have to respect on one hand, the Act on Processing of Personal Data, particularly the Chapter 6a, and on the other hand, the Act on TV surveillance. This latter prohibits the use of surveillance by private entities in public spaces, and commercial operators can only use such combination of technologies in private places. State agencies have also to respect the Act on Processing of Personal Data when they use a RPAS to collect personal information but certain of the provisions do not apply to the police and the courts in criminal proceedings. For instance, the data subject rights are regulated in the Administration of Justice act if they are exempted from several provisions. Like commercial operators, State agencies have also to

---

<sup>331</sup> Any interception of communications must take place on the basis of a warrant, and the warrant must indicate, for example, the telephone number that is the target of interception, Section 783(1) of the Administration of Justice Act, 06.11.2008.

<sup>332</sup> There must be certain grounds for assuming that messages to or from a suspect are conveyed by the communication in question, Section 781(1)(i) of the Administration of Justice Act, 06.11.2008.

<sup>333</sup> The second condition for the interception of communications is that the interference is assumed to be of decisive importance to the investigation, Section 781(1)(ii) of the Administration of Justice Act, 06.11.2008.

<sup>334</sup> A requirement as to the nature of the crime, particularly that the investigation concerns an offence with a maximum penalty exceeding six years or contravention of Parts 12 and 13 of the Criminal Code, Section 781(1)(iii) of the Administration of Justice Act, 06.11.2008.

<sup>335</sup> If in view of the purpose of the interference, the importance of the case and the outrage and inconvenience that the measure is assumed to cause to the person(s) affected by it, it will constitute a disproportionate intrusion, Section 782 of the Administration of Justice Act, 06.11.2008.

<sup>336</sup> Privacy International, the Electronic Privacy Information Center (EPIC) and the Center for Media and Communications Studies (CMCS), European Privacy and Human Rights (EPHR) 2010, p. 218.

respect the Act on Processing of Personal Data, the specific Chapter 6a and the Act on TV surveillance since they use overtly a drone equipped with a video camera in public places. In case of use of RPAS equipped with a visual or non-visual payload in a secret surveillance context, State agencies are subject to the specific surveillance legislation applying to the law enforcement sector, Section 791a of the Administration of Justice Act 2008 and Section 780 and foll. of the Administration of Justice Act 2008. Danish telecommunication and Internet providers fall under the provisions of the Act on Electronic Communications and Network Services whether they use a drone for offering their services. Regarding to private individuals and hobbyists, they are exempted from the Act on Processing of Personal Data. So sole the right to privacy and some privacy oriented rules figuring in other civil legislation apply.

### 5.3 Member State preparing RPAS regulations

Today, Belgium, is included within a set of countries that are adopting a proposal regulating the safety aspect of civil RPAS. This section analyses the general privacy legislation and the surveillance regulations of Belgium, which will likely apply to the RPAS technology as well.

#### 5.3.1 Belgium

In this section, we will discuss three privacy acts, Article 22 of the Belgian Constitution, the Privacy Act and the Telecom Act, and three acts related to surveillance, the Camera Act, and the Criminal Code and the Procedural Criminal Code.

#### *The privacy and data protection legislative framework*

a) The right to privacy: Article 22 of the Belgian Constitution<sup>337</sup>

Article 22 of the Constitution recognises explicitly the right to the private life since 1994. Additionally, the same text provides respectively at Articles 29 and 15, the confidentiality of private communications and the inviolability of home principles. It is noteworthy that the Constitution allows derogations to the right to private life. However, these latter must be enshrined in a formal law and must respect at least the “minimal guarantees” figuring in the Privacy Act.<sup>338</sup>

b) The data protection law: The Privacy Act 1992<sup>339</sup>

The *Act related to the protection of the private life regarding the processing of personal data* (hereinafter the Privacy Act) has been amended by the Act of the 11 November 1998 in order to enforce the European Data Protection Directive 95/46/EC. Shaped on the basis of the Data Protection Directive, the Privacy Act encompasses the same scope, core principles and individual rights. According to Article 3, the Privacy Act applies to all processing of personal data automated in whole or in part<sup>340</sup>. Like the Article 29 WP, the Belgian Data Protection Authority has recognised biometric data and data collected by the means of Automatic Number Plate Recognition (ANPR) as personal data falling inside the scope the Privacy

---

<sup>337</sup> Belgium Parliament, the Belgian Constitution, 17.02.1994 (“the Belgian Constitution 1994”), Article 22.

<sup>338</sup> Privacy International, EPIC and CMCS, op. cit., 2010, p. 98.

<sup>339</sup> Belgium Parliament, The Privacy Act, 08.12.1992 (“Belgian Privacy Act 1992”).

<sup>340</sup> Belgian Privacy Act 1992, Article 3.

Act.<sup>341</sup> The cameras attached to an RPAS, as well as any other kind of payloads that allow RPAS to process personal data shall undoubtedly exercise such automated data processing. If the drone equipment collects data recognised as being personal data<sup>342</sup>, then, this Privacy Act will apply.

Like the Data Protection Directive, the scope of the Privacy Act is limited to the general and commercial processing of personal data. According to Article 3(2) the Privacy Act does not apply to the processing of personal data carried out by a natural person in the course of a purely personal or household activity.<sup>343</sup> Hence, the Privacy Act will not apply when a drone, fitted with a GPS for instance, processes personal data for purely recreational purposes. Secondly, the Privacy Act stipulates that it only applies “partially” to the processing of personal data carried out solely for purposes of journalism, literary or artistic expression and to the collection of data collected by the police and intelligence services.<sup>344</sup> Some of the Privacy Act provisions do not apply to the journalism and police sector in certain situations restricted by the law itself.<sup>345</sup> Therefore, for example, journalists but also the police can use drones to process images identifying people without requiring the consent of the individuals concerned as well as without notifying the Belgian Data Protection Agency.

The hypothesis that the Privacy Act applies to the use of a drone processing personal data, this use will be subject to the same principles of the Data Protection Directive. In fact, Chapter II and more particularly, Article 4 and 5 provide that all personal data processing shall respect the lawfulness and fairness, purposes limitation, proportionality, data minimisation and retention principles. However, the Privacy Act does not provide a list of what are to be considered ‘legitimate aims’. Nevertheless, it is obvious that acts of voyeurism and/ or of spying on a third person would not be considered legitimate aims. It is unclear whether the use of a thermal camera fitted on an RPAS by a home insulation company to film the roofs of several residential areas in order to develop a marketing strategy on houses with sub-standard roof insulation can be considered a legitimate aim.

Besides the requirements around the processing of data, the Privacy Act requires the collector to act in accordance with the transparency principle. This obligation requires the collector to inform the data subject of its name, the finality of the processing and other categories of information (Article 9). Under this obligation, the collector is also required to notify the DPA (Article 17), and respect the following individual rights: a right to oppose to the processing, a right to rectification, and a right to deletion or to prohibit the use of data.<sup>346</sup>

---

<sup>341</sup> Privacy Commission, “Avis D’initiative Relatif aux Traitements de Données Biométriques Dans le cadre de L’authentification de Personnes, (A/2008/017), 2008, p. 7.

<sup>342</sup> Regarding images, the Belgian Data Protection Authority (the Privacy Commission) has issued several advices stating that the Belgian Privacy Act 1992 applies to the processing of images that concern identified or identifiable persons or their goods. Thus, the Privacy Commission has declared that since cameras equipped on a drone are susceptible to collect images of individuals or goods of individuals, such as the image of a license plate, this collection of information shall be considered as the processing of personal data. Other types of information collected and processed by drones such as thermal data, biometric data, location data, sounds, etc., may also be considered as personal data and subject to the Belgian Privacy Act 1992 if that data concerns an identified or identifiable person.

<sup>343</sup> For a description of this exception, see Part II, Directive 95/46/EC concerning the exception on processing data for purely personal or household activity.

<sup>344</sup> Belgian Privacy Act 1992, Article 3(3).

<sup>345</sup> Belgian Privacy Act 1992, Article 3 (3-5).

<sup>346</sup> Belgian Privacy Act 1992, Chapter 3.

c) Privacy in the telecommunication sector: The Telecom Act 2005<sup>347</sup>

The Telecom Act 2005 which implements the e-Privacy and the Data Retention Directives provides for the confidentiality of public communications and traffic data collected by providers of public communications and providers of electronic communications made available to the public.<sup>348</sup> Hence, like the e-Privacy Directive, it is forbidden for all, save for the user, to listen, intercept and store communications and traffic data or to subject these communications to any other means of surveillance without the consent of the users concerned. In addition, according to Article 122, the traffic data have to be deleted or anonymised once they are no longer necessary to the transmission of the communications.<sup>349</sup> This Telecom Act makes clear that the interception of communication is legally prohibited in Belgium. Hence, using an RPAS to intercept electronic communications and telecommunications would contravene the Telecom Act.

Article 126 of the Telecom Act provides that, after the implementation of the Retention Directive on 30 July 2013, Internet providers and telecommunication providers have to retain certain identification, locations and traffic data related to public communications for a period of 12 months.<sup>350</sup> These data can subsequently be made available to the police forces for the purposes of investigations, instructions and prosecution of an exhaustive list of criminal offences.

***Surveillance regulations applicable to civil RPAS***

a) The visual surveillance (CCTV systems) regulation: The Camera Surveillance Act 2007<sup>351</sup>

In addition to the Privacy Act which applies to the processing of personal data, a Belgian collector of personal information processed by the means of video-surveillance cameras is also subject to the Camera Surveillance Act. The aim of this legislation is to regulate the use of surveillance CCTV systems. Therefore, this Camera Surveillance Act applies to the installation and the use of fixed and mobile video-surveillance cameras used for the following purposes (a) to prevent, detect or observe offenses, e.g., co-owners attempting to fight against vandalism in the entrance hall of an apartment building or (b) to prevent, detect or identify annoyances, e.g., the Municipality which wants to prevent vandalism on its territory or (c) to maintain public order, e.g., during the Annual yard sale.<sup>352</sup> In the other areas, The Privacy Act remains in application. However, it does not apply to the video cameras of surveillance installed at workplaces and to the areas specifically regulated, for instance the surveillance cameras for security purposes during the soccer matches.<sup>353</sup> It has to be emphasised that the Camera Surveillance Act applies regardless whether the information collected are personal or

---

<sup>347</sup> Belgium Parliament, Telecom Act, 10.07.2012 (“Belgian Telecom Act 2012”).

<sup>348</sup> Belgian Telecom Act 2012, Article 12.

<sup>349</sup> Belgian Telecom Act 2012, Article 122.

<sup>350</sup> Belgian Telecom Act, 2012, Article 126.

<sup>351</sup> Belgium Parliament, Camera Surveillance Act, 21.03.2007.

<sup>352</sup> Belgian Privacy Commission, “Les caméras de Surveillance et Notre vie Privée”, *CPVP online*, no date.  
<http://www.privacycommission.be/fr/cameras-de-surveillance>

<sup>353</sup> CCTV systems installed for security reasons during soccer matches are specifically regulated by the Act 21/12/1998 concerning the security during soccer matches and the Royal Decree 12/09/1999 concerning the installation and the functioning of CCTV systems in soccer matches: Belgian Privacy Commission, “Les Caméras de Surveillance et Notre vie Privée”, *CPP online*, 2014.  
<http://www.privacycommission.be/fr/cameras-de-surveillance>

not. Therefore, any RPAS operator using a drone equipped with a camera for surveillance purposes must adhere to the provisions of this Act.

Article 2 clarifies that cameras fitted on a drone have to be considered as mobile cameras. According to Articles 7/1 and 7/2, the use of such mobile cameras for surveillance purposes is only authorised in the accumulation of the following strict conditions: (a) the use is restricted to the enforcement authorities (b) the use has to take place in the framework of great gatherings, (c) only non-permanent monitoring missions are authorised (c) the period of the surveillance has to be limited, the use has to take place in a public place or in a close place accessible by the public.

Moreover, recorded images cannot be stored for more than one month. Given this restriction on the use of mobile cameras, the use of Automatic Number Plate Reader (ANPR) by the police through the means of fixed cameras is prohibited by the CCTV regulation. Furthermore, the Privacy Commission has recently issued two *Opinions* confirming the legal prohibition of the use of such new technology by the law enforcement authorities.<sup>354</sup> Therefore, the use of drones mounted with cameras is greatly restricted in Belgium today both in terms of actors (by law enforcement authority) and finality (in great gatherings) for which they can be used.

According to Article 8, all use of hidden video-surveillance cameras is prohibited.<sup>355</sup> The second paragraph of the article defines the concept of “hidden video-surveillance” by stipulating that “all use of video surveillance which has not been authorised by the individual concerned” shall be considered hidden use. In other words, the collector of images must obtain the explicit consent of the individual concerned to use a video surveillance camera. However, paragraph 3 of the same Article (8) provides two exceptions when it states that posting a pictogram signalling the presence of the cameras or the presence of the person in a public place where video-camera are visible may be considered prior authorisation.<sup>356</sup> Finally, concerning the aerial and visual surveillance carried out by the police sector, the legislator has been more flexible as it states that “the cameras fitted on a marked-police aircraft are deemed to be visible” and, then, does not need to obtain consent before exercising the surveillance mission.<sup>357</sup> It is clear from the analysis of these last provisions that this Act applies to the use of RPAS fitted with a video surveillance camera as covert/blanket surveillance operations are prohibited. Hence, drones will have to be identifiable and visible during their use by bearing specific colours.

Relevantly, the Camera Surveillance Act is currently under review. This review was commenced following criticism that its provisions are ambiguous, and that it is silent on its application to (a) other data than photos and videos, such as the sound, the thermal images and (b) the new technologies such as the drones, e.g., facial recognition, etc. According to a recent Proposal of the Privacy Commission, the scope of the next camera regulation will

---

<sup>354</sup> Belgian Privacy Commission, Recommendation No. 04/2012 - Recommendation D'initiative sur les Diverses Possibilités D'application de la Surveillance par Caméras (CO-AR-2011-011) (“Belgian Recommendation No.04/2012”), Articles 49-53.

<sup>355</sup> Belgium Parliament, the Camera Surveillance Act, 21.03.2007 (“Belgian Camera Surveillance Act 2007”), Article 8.

<sup>356</sup> Ibid.

<sup>357</sup> Belgian Camera Surveillance Act 2007, Article 8.

extend the use of new technologies such as drones and ANPR and the use of these technologies together by law enforcement authorities for different purposes.<sup>358</sup>

b) Systematic covert surveillance regulation: Article 47sexies and Article 47septies of the Procedural Criminal Code

After having analysed the mobile overt visual surveillance in public places which is restricted to the police sector, we shall have a look to the regulation which shapes covert surveillance. Blanket surveillance, also called the systematic observation, of an individual is obviously only permitted by police forces and under very strict requirements.<sup>359</sup> This systematic observation encompasses surveillance operations exercised from public places during long period (weeks, months) or operated through technical means allowing the detection, the transmission or the recording of information such as CCTV systems, GPS devices, sensors, etc.<sup>360</sup> Article 47sexies and 47septies of the Criminal Code strictly regulates when these surveillance missions may be exercised.<sup>361</sup> The adoption of a broad definition of “Systematic observation” appears to encompass drones equipped with GPS, cameras and any other surveillance equipment used for covert surveillance purpose by law enforcement authorities.

c) Regulations of the surveillance, wiretapping and access to communications: The Criminal Code and The Procedural Criminal Code

Secrecy of communications is a fundamental principle in the Belgian Constitution and Criminal Code. Indeed, Article 314bis§1 of the Criminal Code prohibits deliberately acquiring the content of a private communication or telecommunication to which the acquirer was not a party.<sup>362</sup> Nevertheless, this secrecy of communications (public and private) principle is limited by some exceptions. The Procedural Criminal Code<sup>363</sup> regulates in which circumstances the surveillance and the interception of private communications and electronic communications may be carried by police services.<sup>364</sup> In this Code, the legislator gives the police sector the power to observe telecommunications, to identify the subscribers and users of a telecommunication network and to access and to record the content of communications.<sup>365</sup> Obviously, these exceptions are conditional.

We can already assume that Belgian RPAS operators would be prohibited from intercepting any private or public communications. However, this prohibition will not apply to RPAS operated by the police authorities when they are used in the certain circumstances and for the legitimate purposes set out in the law.

### **Summary**

This study shows that in Belgium, commercial operators of drones are subject to the Belgian Privacy Act 1992 when they process personal data. Under the basis of the Camera Surveillance Act 2007, the use of visual payloads mounted on drones for monitoring activities

---

<sup>358</sup> Belgian Recommendation No.04/2012, Articles 49-53.

<sup>359</sup> Docquir, Benjamin, *Droit de la vie Privée*, Larcier, Brussels, 2008, p. 295.

<sup>360</sup> Ibid.

<sup>361</sup> Belgium Parliament, Criminal Code, 08.06.1967, (“Belgian Criminal Code 1967”), Section 47.

<sup>362</sup> Ibid.

<sup>363</sup> Belgium Parliament, the Procedural Criminal Code, 17.11.1808, Articles 46bis, 88bis, 90ter to 90decies.

<sup>364</sup> The reference to communication includes not only phone calls but also all oral and written communications, such as email and sms; Belgian Cass, 26 March 2003, *J.T.*, 2003, p. 626; Docquir, op. cit., 2008, p. 296.

<sup>365</sup> Docquir, op. cit., 2008, p. 296.

is strictly prohibited in commercial use. Moreover, telecommunication and broadband service providers seem to fall under the Telecom Act whether they intend to use RPAS to carry out their services. Regarding journalists using RPAS to record information, they fall under the Privacy Act but are exempted of almost all relevant provisions. Governmental drones operated by public bodies are partially regulated in Belgium by the Privacy Act when they process personal data. However, the present section demonstrates that the use of civil RPAS for overt monitoring activities is subject to the Camera Surveillance Act 2007 and is restricted to the police sector. Therefore, the State agencies using a drone equipped with a surveillance camera will be subject to some provisions of the Privacy Law and the tailored standards enshrined in the Camera Surveillance Act. Regarding covert surveillance (systematic surveillance, the interception of communications and wiretapping), the operator of governmental drones should respect Procedural Code and the Criminal Code. Finally, the analysis of the Camera Surveillance Act 2007 implicitly shows that private users of drones are prohibited to use drones for visual surveillance in public places. However, in case of processing personal data through the means of drones for domestic purposes, these private individuals are not regulated.

### 5.3.2 Conclusion

In Sections 6.2 and 6.3, we examine the legislation of six Member States - three Member States already implementing RPAS-related laws (the United Kingdom, France, Germany) and three Member States preparing privacy regulations related to RPAS use (Belgium, Luxembourg and Italy). For each Member State two types of legislation has been examined. First, were the privacy laws encompassing the right to privacy, the data protection law and the privacy law governing the telecommunication and network services sectors. Second, were laws related to surveillance, including CCTV systems regulations and surveillance regulations in the law enforcement sector. The analysis has shown that all Member States studied encompass some privacy and surveillance oriented legislation that may be applicable to different applications of the RPAS technology.

We have also found that the data protection laws and the legislation concerning the telecommunication and Internet services sector of the Member States are all very similar as they transcribe the EU Data Protection Directive and e-Privacy Directive. In this regard, we observed that *commercial drones' operators* (corporates, professionals, journalists) from all Member States, are subject to the national data protection law if they use drones for collecting data and even though some operators, such as journalists, are exempt from several provisions. Furthermore, all Member States contain a law governing privacy and the telecommunication sector in their implementation of the e-Privacy Directive. Hence, *telecommunication and Internet service providers* willing to use drones to provide services should also ensure that they respect relevant requirements set out in those pieces of legislation.

Thirdly, we remarked that few Member States include specific CCTV regulations in their privacy regime. Most of the states apply their data protection law to the recording of images identifying individuals through the means of CCTV systems and do not regulate the “simple monitoring without recording”.

Fourthly, we have also examined that generally public bodies are also subject to the data protection law but that law enforcement entities may be exempt in certain circumstances. We could, therefore, say that *law enforcement operators and other public bodies* using drones to collect data in their general activities are in principle subject to the application of States' data protection law. However, law enforcement authorities using drones to process data for

investigations of crimes or when national order is at stake (in their surveillance activities), may be exempt. Additionally, each Member State holds legislation allowing law enforcement authorities to intercept communications. Hence, this analysis seems to have shown that under the basis of surveillance-oriented laws, law enforcement authorities could use drones to intercept communications and listen to conversations taking place within European Union borders. However, in many cases, this requires some authorisation or oversight.

Finally, *private* collectors are always out of the scope of the national data protection laws examined. Therefore, private users of drones remain unregulated when they process personal data. Furthermore, we observed that no privacy law(s) seem(s) to apply to the use of RPAS for private purposes. However, the right to private life is generally recognised in Constitutions. Moreover, some provisions in criminal law, civil law and property law could be extended to prohibit some domestic drone applications and to compensate citizens infringed in the enjoying of their rights.

## 5.4 An overview of the current DPA positions and activities

In this last section, we will discuss the positions and initiatives that some national data protection authorities have already undertaken. To our knowledge, four data protection authorities have adopted an official position or initiatives in relation to the potential implications of the civil use of RPAS for privacy and data protection, the Czech DPA, the Belgian DPA, the UK DPA and the French DPA. Their positions and the links to their articles are summarised here.

### 5.4.1 The Czech Republic

The Czech DPA (Úřad pro ochranu osobních údajů) has delivered “*Position No. 1/2013 - Processing of personal data via recordings from cameras on unmanned aircraft*”<sup>366</sup> on its own website (<http://www.uouu.cz>) in January 2013. In this document, the Czech DPA explains in which applications and to which type of operator of drones the Czech Personal Data Protection Act applies. The Position explains that the use of RPAS with visual imaging capabilities provide an opportunity to “acquire personal data in a relatively easy manner from an environment that would otherwise be very difficult to access”.<sup>367</sup> RPAS operators who use visual cameras to record information must respect all of the articles of the Data Protection Act, and they must endeavor to protect privacy. However, it explains that the Czech Data Protection Act does not apply to RPAS operations that do not collect personal data and that it does not apply to RPAS operators who monitor images but do not record them. Specifically, RPAS operators that capture images of persons must obtain prior consent of those persons or must destroy the data “without undue delay”.<sup>368</sup> Finally, the Position also states that the use of an RPAS to record audio data must also respect the principles of the Data Protection Act, and that it should be recognised that such recordings would be a significant encroachment on privacy. While this particular document represents a useful clarification of the applicability of the Czech Data Protection Act to specific RPAS operations, it unduly focuses on visual image

---

<sup>366</sup> The Office for Personal Data Protection, *Position No. 1/2013 - Processing of personal data via recordings from cameras on unmanned aircraft*, January 2013.

[http://www.uouu.cz/en/vismo/zobraz\\_dok.asp?id\\_org=200156&id\\_ktg=1342&archiv=2](http://www.uouu.cz/en/vismo/zobraz_dok.asp?id_org=200156&id_ktg=1342&archiv=2)

<sup>367</sup> Ibid.

<sup>368</sup> Ibid.

recording and audio image recording, and does not encourage RPAS operators to consider how other payloads might also infringe on privacy, data protection and ethics.

#### 5.4.2 *Belgium*

In Belgium, the Belgian DPA (Commission Vie Privée- Commissie voor de bescherming van de persoonlijke levenssfeer) has recently published an article entitled “Questions fréquemment posées concernant les drones” on its website.<sup>369</sup> This article encompasses twenty FAQs relevant to RPAS that are answered by the Privacy Commission.

The first five FAQ examine the concept of drone, payload and the different usages of the RPAS technology. In relation to its features, the Privacy Commission particularly points out the remotely character of drones and the fact that they can be remotely piloted by high technological equipment as well as by simpler technology like Smartphone. It also highlights the wide variety of models, sizes and weights they can have. Regarding to the equipment they can carry, the Privacy Commission mentions the five categories of payload: cameras, night vision devices, radar technologies, infra-red technologies, specific sensors like chemical and sounds sensors. Afterwards, the DPA has identified five main drone applications: military use, commercial use, scientific use, public sector use in pursuit of the public interest and use for police missions and criminal investigation.

Second, the FAQ identifies the atypical features of the drone technology that pose privacy concerns. The following characteristics are mentioned: the invisibility of the technology, the transparent use, the particular privacy intrusive character compared to other data collection technologies, the ability to process data on very wide territories, the ability to process a massive amount of information, the ability to perform continuous surveillance, the ability to store data indiscriminately and the evolving character of the technology.

Thirdly, the next fourteen FAQs concern the Belgian legal privacy framework applying to drones. In these, the Privacy Commission recalls that Article 8 of the ECHR, its case law and Article 22 of the Belgian Constitution, which protects the right to private life, apply also to drones. It also clarifies to what extent the Belgian Camera Act applies to the use of a drone equipped with a surveillance camera. In this regard, it evokes that a drone should be considered as a mobile camera and thus falls under the restrictions applying to such type of camera. Consequently, it makes clear that drones equipped with a camera can currently only be used in public places by the police services in the context of large gatherings for a short mission. Afterwards, the Commission clarifies to journalists and private individuals the extent to which they are partially (journalists) or wholly (private individuals) exempted from certain provisions of the data protection law. Furthermore, it explains how certain data protection principles should be understood in the context of drones. It includes clear and comprehensive explanations about the following data protection principles: proportionality, purposes limitation, transparency, legitimacy, necessary, data minimisation, data processing security and privacy by design. Finally, besides clarifying how RPAS collectors should apply such and such principles, the Privacy Commission also attempts to provide some recommendations to manufacturers, designers, commercial operators. For instance, it suggests that commercial operator to privacy-by-design features such as blurring software to avoid the processing of unnecessary data.

---

<sup>369</sup> Commission Vie Privée- Commissie voor de bescherming van de persoonlijke levenssfeer, “Questions fréquemment posées concernant les drones”, 2014. <http://www.privacycommission.be/fr/faq-themas/drones>

Thus, the Privacy Commission also links the privacy, data protection and ethical risks associated with RPAS to legislation and guidance on CCTV. However, it specifically distinguishes the use of RPAS from ordinary CCTV, by describing them as mobile cameras, which have specific obligations and prohibitions. Furthermore, the Belgian DPA stands alone in emphasising that RPAS may carry additional payloads that have impacts on privacy, data protection and ethics that are entirely separate from visual photography issues. As such, the Belgian DPA explicitly recognises the unique characteristics posed by RPAS technology.

### 5.4.3 The UK

The UK's Information Commissioner's Office (ICO) has delivered *CCTV code of practice: Draft for consultation 20 May 2014- 1 July 2014*<sup>370</sup>, which provides good practice advice for operators of CCTV and other surveillance camera technologies, that view or record individual's information or information related to individuals (e.g. license plate numbers). As such, in addition to CCTV, the code also covers the use of Automatic Number Plate Recognition, body worn cameras and remotely operated vehicles (drones). The ICO code reflects wider regulatory context e.g., Freedom of Information Act 2000 (FOIA), the Protection of Freedoms Act 2012 (PFA), and the Human Rights Act 1998 (HRA) and sets out how legal requirements of the DPA can be met. The code does not cover the use of surveillance systems for limited household or information captured by recreational purposes.

The document classifies drones as “emergent technology” and recognises that as they are becoming more affordable to businesses and members of the public, specific questions regarding privacy, personal data and security are raised. The overall stance of the ICO is that the use of drones should be appropriate, proportionate and that operators should take necessary steps to protect individuals' data. As with other surveillance, the code stipulates that audio recordings of conversations should not be performed, but image data only.

In the first instance a user should decide on the basis of a Privacy Impact Assessment (PIA)<sup>371</sup> whether the use of drones is justified, or whether a “less privacy intrusive method” is available. This undertaking will also allow for consultation and gives insight into public views on privacy and privacy intrusion. Privacy by design should also be incorporated into the process, e.g., to make sure that continuous recording is not undertaken, but only as needed. The code stipulates that drone users must think of identifying methods for informing individuals of recording. ICO recognises that this may prove difficult but suggests that innovative ways, e.g. the use of social media, may be developed and used for this purpose. In addition the user must provide fair processing information.

The code restricting the focus of the drones' attention to only a necessary field of vision and if, for example, a drone is bought for monitoring purposes, its use should be restricted to those specific functions but not blanket recording e.g., whilst flying between monitoring or surveillance tasks, or to record a broad area of view, to avoid capturing unnecessary images of individuals.

---

<sup>370</sup> Information Commissioner's Office, *CCTV code of practice: Draft for consultation 20 May 2014-1 July 2014*, 2014.  
[http://ico.org.uk/about\\_us/consultations/~media/documents/library/Data\\_Protection/Research\\_and\\_reports/draft-cctv-cop.pdf](http://ico.org.uk/about_us/consultations/~media/documents/library/Data_Protection/Research_and_reports/draft-cctv-cop.pdf)

<sup>371</sup> Information Commissioner's Office, *Conducting privacy impact assessments: code of practice*, 2014.  
[http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/~media/documents/library/data\\_protection/practical\\_application/pia-code-of-practice-final-draft.pdf](http://ico.org.uk/for_organisations/data_protection/topic_guides/~media/documents/library/data_protection/practical_application/pia-code-of-practice-final-draft.pdf)

With regard to data protection, encryption and access controls should be incorporated into use processes, when it comes to processing image data captured by drones, as well as appropriate retention and deletion schedules. With regard to more detailed information regarding these practices ICO refers to the document *Privacy and Drones: Unmanned Aerial Vehicles* published by the Information & Privacy Commissioner Ontario, Canada, which states that “Applied security standards must assure the confidentiality, integrity, and availability of personal data throughout its lifecycle including, inter alia, methods of secure destruction, appropriate encryption, and strong access control and logging methods.”<sup>372</sup>

Thus, like the Czech DPA, the advice from the Information Commissioner’s Office seems to focus on the use of RPAS that collect visual information. However, the ICO does recognise that audio recording and/or smart visual surveillance may also be possible. Furthermore, this is somewhat expected as the advice is contextualised by the CCTV Code of Practice, which specifically focuses on visual information collection.

#### 5.4.4 France

In France, the French DPA (La Commission Nationale de l'Informatique et des Libertés - CNIL) has firstly issued its position through the publication of a Press Release entitled “Usages des drones et protection des données personnelles” the 30<sup>th</sup> October 2012. Second, the CNIL published in December 2013 another Press Release which links to an Article entitled “La lettre innovation et prospective de la Cnil - Drones, innovations, vie privée et libertés individuelles” that Édouard Geffray, the Secretary-General of the CNIL, has issued. This section examines both publications.

In the 30<sup>th</sup> October 2012 press release, the CNIL firstly clarifies what a drone is and for which usages they can be used. In that respect, it states that a drone is a small cheap aerial engine which can be equipped with multiple payloads and be easily remotely operated via a Smartphone.<sup>373</sup> In addition, it explains that drones can be used for governmental projects in the framework of the protection of the national security, control of borders and detection of forest fires and for recreational purposes by the general public (drones used for recreational or for professional purposes). Furthermore, it emphasised that mounted with a mobile video camera, a sound sensor or a geo-localisation system, they can easily capture personal data. In this regard, it recalls that although the aerial photography is regulated by article D. 133-10 of the civilian aviation code, the French Data Protection Act (la loi Informatique et Libertés) applies also when the processing and collection of images is related to identified or identifiable persons. Finally, it concludes that as part of its advisory role, the CNIL has taken up the issue and is engaged in a retrospection reflection with stakeholders. It also mentions that it follows research projects in this area and participates in works and reflections related to ethical issues of the robotics in the civil sector.

In the second press release “Drones: quelle vision prospective, quels enjeux pour les libertés ?”<sup>374</sup>, the CNIL presents the article “La lettre innovation et prospective de la CNIL -

---

<sup>372</sup> Cavoukian, A. Information & Privacy Commissioner Ontario, Canada, *Privacy and Drones: Unmanned Aerial Vehicles*, August 2012, p. 23.. <http://www.ipc.on.ca/images/Resourcess/pbd-drones.pdf>

<sup>373</sup> CNIL, “Usages des drones et protection des données personnelles”, 30 October 2012.

[www.cnil.fr/linstitution/actualite/article/article/usages-des-drones-et-protection-des-donnees-personnelles](http://www.cnil.fr/linstitution/actualite/article/article/usages-des-drones-et-protection-des-donnees-personnelles)

<sup>374</sup> CNIL, “Drones : quelle vision prospective, quels enjeux pour les libertés ?”, 06 December 2013.

<http://www.cnil.fr/linstitution/actualite/article/article/drones-quelle-vision-prospective-quels-enjeux-pour-les-libertes/>

Drones, innovations, vie privée et libertés individuelles”.<sup>375</sup> It also mentions that such article is part of the prospective research made by the CNIL about drones, which will allow them to create an adequate legal framework accompanying the innovation and development of new usages and placing limits that must not be crossed in terms of surveillance.

We can find in the heading of the article “La lettre innovation et prospective de la CNIL” that it is divided into two main sections, a section “Study and Investigations” followed by “3 questions posed to Ryan Calo” and a section entitled “Focus” on hacking by drones. Under the first section “Study and Investigations”, the Secretary-General of the CNIL firstly speaks about drones used for surveillance purposes. In that respect, it explains that drones can be mounted with a wide range of equipment like cameras, microphones, thermal sensor, infra-red sensors, chemical sensors, which makes drones the perfect tool for observation and for collection and transmission of geo-localisation data regardless if they are used for military or civil purposes. Second, it explains that, in the future, drones will be used for a wide range of applications. It states that as they have been initially a military device, they will firstly be used in contexts of overall security by public authorities for public order and civil protection. Second, it mentions the use of drones by scientists for ecological research and humanitarian purposes. Thirdly, he pointed out that besides surveillance, drones will also be used as loading vehicles for professional purposes like agriculture and construction. It also makes reference to recreational drones bought by private individuals and hobbyists. Secondly, it includes an interview with Ryan Calo, Professor of Law at the University of Washington and associate researcher with the “Center for Internet and Society” at Stanford. This latter mainly refers to statements written by Ryan Calo itself in the article “Open robotics” published in the Law journal *Maryland Law Review*.<sup>376</sup> Furthermore, there is a short sub-section devoted to the identification of the characteristics of drones, which makes it an atypical surveillance device. Among others, we can find the discretion characteristic, its intrusive feature and its ability to capture a massive amount of data in a non-discriminatory way. In a more legal reflection, he reports that there is a need to set up a legal framework tailored to the technology by revising the existing texts to make them adapted to the features of the device. In this regard, he suggests setting up blurring technology and pre-determined locations for drone uses. Finally, under the second section “Focus”, he concludes that more and more people are interested in making their drones and payloads themselves, which may pose security processing concerns as equipped with specific software they could be used for hacking the content of other drones or smartphone.

Consequently, although the CNIL has inserted themselves within the larger debate on RPAS and indirectly recommended changes in legislation, the information provides little advice for RPAS operators in terms of responsible practice. Furthermore, like other DPAs, the CNIL intervention is largely focused on visual photography (especially by police), rather than other payloads, capabilities and applications. Nevertheless, this intervention is useful in that it warns RPAS operators of the potential risks to privacy and data protection engendered by these technologies.

---

<sup>375</sup> Geffrey, Edouard, “La lettre innovation et prospective de la CNIL - Drones, innovations, vie privée et libertés individuelles”, December 2013.

[http://www.cnil.fr/fileadmin/documents/La\\_CNIL/publications/DEIP/LettreIP6.pdf](http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/LettreIP6.pdf)

<sup>376</sup> Calo, Ryan, “Open robotics”, *Maryland Law Review*, Vol. 70, N°3, 2011,  
[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1706293](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1706293)

These four Data Protection Authorities are the only ones who have specifically, at this point, addressed RPAS technology. While most of them are undertaking this work by linking their advice on RPAS with their advice on CCTV, all DPAs must be encouraged to consider and provide information about how additional RPAS capabilities and applications might also pose specific risks to privacy, data protection and ethics. They need to be technology neutral, not focused on an existing and narrow set of payloads and applications. Otherwise, the DPAs are risking that their advice might become quickly out-dated, and the fundamental rights of members of the public might be negatively impacted by these other capabilities and applications.

## 5.5 Third Countries

After having studied the privacy and data protection legal framework of the aforementioned European Member States that may apply to RPAS technology, we now consider that the analogous situation in the third countries of Switzerland and the United States. While both countries have not yet adopted federal privacy regulation specific to RPAS, the study of their privacy and data protection regimes highlights some privacy protection rules relevant to the regulation of the civil use of RPAS technology.

### 5.5.1 Switzerland

Before examining its legislation, it is essential to point out that as of 2010, law enforcement authorities have used RPAS for surveillance purposes. Since this time, the increase of RPAS in the Swiss airspace has continued. Furthermore, Switzerland is home to a large number of civil RPAS manufacturers.

*The right to privacy and protection of personal data: Article 13 of the Swiss Constitution*<sup>377</sup>  
Since 2000, the right to privacy and protection of personal data has been constitutionally recognised. Article 13 expressly provides: "All persons have the right to the respect of their private and family life, home, mail and telecommunications. All persons have the right to be protected against abuse of their personal data".<sup>378</sup> It refers to Article 8 of the ECHR and, thus, encompasses several privacy rights.

*The personal data protection legislation: The Federal Data Protection Act 1992*<sup>379</sup>  
In Switzerland, there are two levels of personal data protection legislation. At the federal level, there is the Federal Data Protection Act 1992 (hereinafter, FDP) while at the cantonal level, 16 cantons have their own data protection law.<sup>380</sup> As with the analysis of the EU Data Protection Directive and its implementation in national laws, the scope of the Swiss Federal Data Protection Act will be examined in order to determine the applicability of this Act to RPAS technology and use. The Federal Data Protection Act regulates the processing of personal data pertaining to natural persons and legal persons by private persons and federal bodies (Article 2).<sup>381</sup> This regime is technology neutral. As in the DPD, personal data concerns all information relating to an identified or identifiable person. This includes all types of data - images, sound, biometric, location data, traffic data, etc. – that could allow someone

---

<sup>377</sup> Swiss Parliament, the Swiss Federal Constitution, 18.04.1999 ("Swiss Constitution 1999"), Article 13.

<sup>378</sup> Swiss Constitution 1999; Privacy International, EPIC and CMCS, op. cit., 2010, p. 764.

<sup>379</sup> Swiss Parliament, The Federal Data Protection Act, 19.06.1992 ("Swiss DPA 1992").

<sup>380</sup> Privacy International, EPIC and CMCS, 2010, p. 764.

<sup>381</sup> Swiss DPA 1992, Article 2.

to be identified directly or indirectly.<sup>382</sup> Given the technological neutrality of the texts, it is applicable to the civil RPAS technology regardless with which equipment it is mounted and the types of data it captures, as long as these data contain personal information. For instance, a commercial company that decides to launch drones above Lausanne to collect images and use them for a new marketing strategy shall be subject to the FDP if the footage captured concern an identified or identifiable individual.

Regarding what types of operators are covered by the law, unlike the EU DPD, the Swiss FDP governs data processing operated by natural persons, legal persons, private persons and federal bodies.<sup>383</sup> However, data processing for exclusive personal use and those carried out in the context of civil or criminal proceedings are excluded from its scope. Regarding the processing of data by law enforcement authorities for public order or national security purposes and those carried out by journalists, nothing in the law suggests that they are exempt. By contrast, the processing of data for journalistic purposes is subject to a specific provision (Article 10) for such processing. Applied in the context of the RPAS technology, this means that the FDP should apply when the operator of drone collecting data is a private body, a federal authority, a journalist or an individual and, when that data are not used for criminal proceedings or for exclusive private purpose.

The FDP embodies the same principles as the EU data protection principles - lawfulness, purpose limitation, quality of data, proportionality - and a transparency obligation - duty to inform the subject concerned, notification and registration. It also affords similar individuals' rights (right to access, right to block the disclosure, right to correct). It also requires a collector to undertake "adequate technical and organisational measures"(Article 7).<sup>384</sup> The Federal Council issues detailed provisions on the minimum standards for data security". This provision is particularly interesting for RPAS, as one of the main issues with drones is that they usually capture other data than those that the data intends to capture. For instance, when a mapping company uses drones for its professional activities, it is likely that individuals appear in the collected footage. The processing of this personal data is not authorised within the meaning of the law as the individuals captured have not been informed of the collection. However, Article 7 provides the legal basis for this collection by empowering the Federal Council to impose a requirement, in some circumstances, on RPAS operators that they adopt technical measures.

Finally, the existence of an adequate protection regime in the case of cross-border disclosure is another similarity between the Swiss data protection law and the EU data protection law. Besides the likeness of the principles, the Art.29WP and the European Commission have both recognised that the Swiss law is adequate under the EU data protection, thereby approving all future personal data transfers to Switzerland.<sup>385</sup>

---

<sup>382</sup> Ibid.

<sup>383</sup> Ibid.

<sup>384</sup> Swiss DPA 1992, Article 7.

<sup>385</sup> Article 29 Data Protection Working Party, Opinion No. 5/99 on the Level of Protection of Personal Data in Switzerland, 7.06.1999, and Commission of the European Communities, The application of Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, SEC (2004) 1322, Brussels, 20.10.2004.

*Privacy in the telecommunication and Internet sectors: The Telecommunication Act*<sup>386</sup>

This section examines Swiss legislation protecting the privacy of communications as it relates to RPAS technology that is capable of carrying telecommunication systems and also to intercept electronic communications and their data (traffic and location data). The confidentiality of telecommunications and the prohibition on the interception and subsequent disclosure of private communications of private individuals are enshrined in the following texts: the Constitution (Article 13), the Criminal Code (Article 321ter), the Federal Personal Data Protection Act (as data related to telecommunications are personal data) and the Telecommunication Act (Chapter 7). The Telecommunication Act not only regulates the secrecy of electronic communications<sup>387</sup> and telecommunications, but also complements the personal data protection laws. Thus, the FDP concerns the processing of any type of data processed by any type of federal authority or private body, whilst the Telecommunication Act complements this by preserving the finalities for which a telecommunication service provider can process location data of its subscriber.<sup>388</sup> Furthermore, it provides a specific provision for data processed by external equipment (Article 45c):

*Processing of data on external equipment by means of transmission using telecommunications techniques is permitted only:*

*a. for telecommunications services and charging purposes; or*

*b. if users are informed about the processing and its purpose and are informed that they may refuse to allow processing.*<sup>389</sup>

The last provision of the Telecommunication Act implies that Swiss services providers using a drone for the transmission of telecommunication or broadband services could process location and traffic data only for the purposes described. It is noteworthy that the Telecommunication Act is currently under review and a proposal has already been adopted. This review has reinforced the importance of maintaining the confidentiality of communications and related data collected by telecommunication operators.<sup>390</sup>

Whereas the secrecy of communications is a fundamental principle in Switzerland<sup>391</sup>, it is noteworthy that the Federal Act on the Surveillance of Mail and Telecommunications 2002 empowers certain public authorities to intercept communications of individuals. However, the finalities for which such interceptions can be carried out are limited to the contexts of a criminal proceeding or a rescue operation of missing persons. In these circumstances, there is an obligation to inform individuals concerned that they are the subjects of tapping

---

<sup>386</sup> Swiss Parliament, Telecommunications Act, 30.04.1997 (“Swiss Telecommunications Act 1997”).

<sup>387</sup> “Obligation of confidentiality - No person who is or has been responsible for providing a telecommunications service may disclose to a third party information relating to subscribers’ communications or give anyone else an opportunity to do so”: Swiss Telecommunications Act 1997, Article 43.

<sup>388</sup> “Location Data - Providers of telecommunications services may process data concerning locations of customers only for the telecommunications services and charging purposes; they may only process it for other services if they have first obtained the consent of customers, or in anonymised form”: Swiss Telecommunications Act 1997, Article 45b.

<sup>389</sup> Swiss Telecommunications Act 1997, Article 45(c).

<sup>390</sup> Swiss Parliament, Proposal on Telecommunications, 19.05.2010, Chapter 7.

<sup>391</sup> Swiss Telecommunications Act 1997.

operations.<sup>392</sup> Additionally, it prohibits any preventative interception, and provides a list detailing the offences that interception can be undertaken in relation to.<sup>393</sup> Given the clarity of the law, it seems that requirements for tapping activities in Switzerland are unambiguous in contrast to their legislative counterparts in the EU Member States examined above. Moreover, the Federal Act on the Surveillance of Mail and Telecommunications requires that Swiss telecom providers retain the traffic data related to electronic communications for a duration of only six months. Under these last considerations, we can suppose that if law enforcement authorities in Switzerland are going to use drones for surveillance activities such as wiretapping, they will fall under the Federal Act on the Surveillance of Mail and Telecommunications.

Finally, this Swiss legislation does not include any specific regulation governing the use of automatic number plate reader (ANPR), biometric sensors, or GPS tracking devices. Therefore, nothing regulates the use of RPAS mounted with one of these systems. However, if an RPAS captures data, the Federal Personal Data Protection Act should apply to such processing operations as location data and licence plate number may be recognised as personal data.

### 5.5.2 *The United States*

#### **General**

The United States has also implemented initiatives to regulate the use of civil drones in their national airspace. The FAA Modernization and Reform Act of 2012 requires that the Federal Aviation Administration (FAA) puts in place the regulation needed to open the airspace to civil RPAS by 2015. Like the European Union, the US has also adopted a Roadmap and has announced that 30,000 civil RPAS should fly in the national airspace in less than 20 years. For now, the FAA “approves public entities (such as federal agencies, public universities, and local police departments) to operate UAVs on a case-by-case basis, [...] commercial users are seeking authorization to fly drones also, but so far FAA has only allowed test and demonstration flights by manufacturers”.<sup>394</sup> More recently, the FAA opened six test sites and issued some privacy requirements for the test sites where RPAS are tested.<sup>395</sup> Also aware of the privacy implications that RPAS raise, the U.S. Government is currently examining how to reinforce its privacy legislation to regulate RPAS technology. At the Federal level, multiple privacy bills related to RPAS were introduced in the 112<sup>th</sup> Congress and in 113<sup>th</sup> Congress, although these have not yet been adopted.<sup>396</sup> In 2013, 43 states introduced 130 bills and resolutions related to RPAS (not only privacy related) and 32 have been passed. If some of them are not privacy oriented, several address privacy issues and generally require a warrant for surveillance activities carried out by drones.<sup>397</sup>

---

<sup>392</sup> Ibid.

<sup>393</sup> Privacy International, EPIC and CMCS, op. cit., 2010, p.770.

<sup>394</sup> Elias, Bart, *Pilotless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace System*, CRS Report for Congress, 2012, p. 2.

<sup>395</sup> US Federal Aviation Administration, *Final privacy requirements Unmanned Aircraft System Test Site Program*, Washington, 2013.

[http://www.faa.gov/about/initiatives/uas/media/UAS\\_privacy\\_requirements.pdf](http://www.faa.gov/about/initiatives/uas/media/UAS_privacy_requirements.pdf)

<sup>396</sup> Villaseñor, John, “Observations from above: Unmanned Aircraft Systems and Privacy”, *Harvard Journal of Law & Public Policy*, Vol. 36 No. 2, 2012, p.509.

<sup>397</sup> National Conference of State Legislature, “2013 Unmanned Aircraft Systems (Uas) Legislation”, *NCSL online*, no date. <http://www.ncsl.org/research/civil-and-criminal-justice/unmanned-aerial-vehicles.aspx>

American privacy and data protection law has developed from case law precedents, and also have some basis in the Fourth Amendment of the United States Constitution. The Fourth Amendment guarantees U.S. citizens a certain degree of privacy against the intrusion of the government.<sup>398</sup> The privacy law applicable to the RPAS technology differs depending on whether the operator is a government agency or a private entity.

This section is subdivided in two sub-sections. The first one examines the privacy statutes applicable to civil RPAS operated by private entities and individuals, while the second section examines the rules applicable to RPAS operated by governmental bodies.

### ***Commercial and private RPAS: First Amendment, torts and statutes***

The First Amendment, protecting the freedom of expression, has been extended by the Supreme Court in order to encompass “a range of conduct related to the gathering and dissemination of information”.<sup>399</sup> This Constitutional right is, therefore, particularly relevant for potential RPAS cases related to the disclosure of photographs by journalists and paparazzi. John Villasenor emphasises the application of the “Trespass tort”. The effect of that Tort in some States means “trespassing statutes are worded in a manner that would encompass trespassory use of a UAS”.<sup>400</sup> Indeed, some states recognise “trespass” as a civil tort while others have enshrined it in their criminal statutes. In both cases, “trespass” is related to the protection of a property right and enables the property owner to restrict unlawful and unauthorised entry.<sup>401</sup> Therefore, this tort could especially prevent RPAS from flying above the property of someone.

Besides trespass, modern American Tort Law comprises four categories of invasion of privacy: intrusion upon seclusion, public disclosure of private facts, false light and appropriation. The tort of “Intrusion upon seclusion” which concerns any physical or electronic intrusion into one's private sphere (home, backyards etc.).<sup>402</sup> is relatable to the civil use of RPAS. Based on this tort, a person who has been filmed in his/her backyard or in his/her home through a window could commence an action against the perpetrator before an American court. Furthermore, this tort prohibits electronic intrusions and would extend to prohibit the use of domestic or commercial RPAS intercepting electronic communications or related data (traffic and location data). The tort of “Public disclosure of private fact” may also be applied in the context of the RPAS technology as it provides subjects a cause of action against operators who would have disclosed or published “drones footages of private individuals involuntarily caught up in newsworthy events”.<sup>403</sup>

In addition, all American states have statutes addressing stalking and harassment. Whereas stalking requires that a victim fears for her/his safety, the concept of harassment is generally

---

<sup>398</sup> Villasenor, op. cit., 2012, p. 475.

<sup>399</sup> United States Court of Appeals, *Glik v. Cunniffe*, 655 F.3d 78, 82(2011); Villasenor, op. cit., 2012, p. 499.

<sup>400</sup> Villasenor, op. cit., 2012, p. 499.

<sup>401</sup> Prosser, William, "Privacy", *California Law Review*, Vol 48, No. 3, 1960, pp. 383-423; “Privacy and Business: The Privacy Torts”, *privacilla.org online blog*, no date.  
<http://www.privacilla.org/business/privacytorts.html>

<sup>402</sup> Ibid.

<sup>403</sup> Villasenor, op. cit., 2012, p. 503.

worded broadly and could easily be used to describe the use of a RPAS mounted with a GPS or a camera track his/her victim.<sup>404</sup>

Finally, drones could also be used to perform corporate espionage.<sup>405</sup> Whereas some forms of espionage operated through the means of drones may be lawful, Villasenor explains that the use of a RPAS to intercept private communications or to record footage of a trade secret without authorisation would violate the Stored Communications Act and economic espionage statutes prohibiting such kind of surveillance.<sup>406</sup>

### ***Governmental RPAS: The Fourth Amendment and its case law***

The Fourth Amendment of the American Constitution provides:

*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*<sup>407</sup>

This Amendment places limits to monitoring activities of law enforcement authorities when these latter constitute “a search.”<sup>408</sup>

Although, the Supreme Court has not yet dealt with the question of RPAS technology in relation to the Fourth Amendment, it has set up some relevant principles for the RPAS technology that have their basis in legal precedents on the application of the Fourth Amendment to surveillance technologies. In *Katz v. United States*, the Court determined the concept of “search” and clarified that a search “occurs when a person has an expectation of privacy in the thing searched”.<sup>409</sup> In that respect, the Court held that warrantless tapping operations of private communications by the police constitutes an unreasonable search under the Fourth Amendment. Therefore, the surveillance of communication by the police in U.S. requires a warrant. In *California v. Ciarolo*<sup>410</sup>, *Florida v. Riley*<sup>411</sup> and *Dowe Chemical v. United States*<sup>412</sup>, the Court ruled that conducting monitoring surveillance activities, including photographing openly visible areas with a conventional camera (not highly sophisticated), through the means of a manned aircraft, by flying over residential and commercial areas, does not constitute a search under the Fourth Amendment, as these areas are open to the public view.<sup>413</sup> Hence, such monitoring activities carried out in public do not require a prior warrant. In *Kyllo v. United States*,<sup>414</sup> the Court held that the use of a sense enhancing technology, *in*

---

<sup>404</sup> Ibid., p. 505.

<sup>405</sup> Villasenor, op. cit., 2012, p. 507.

<sup>406</sup> Ibid., p. 508.

<sup>407</sup> Philadelphia Convention, United States Constitution, 21.06.1788, Fourth Amendment.

<sup>408</sup> Thompson, Richard, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Response*, CRS Report for Congress, 2013, p. 4.

<sup>409</sup> US Supreme Court, *Katz v. United States*, 389 U.S. 347 (1967); Schlag, Chris, “The New Privacy Battle: How the Expanding Use of Drones Continues to Erode Our Concept of Privacy and Privacy Rights”, *Journal of Technology Law & Policy*, Volume XIII, Spring 2013. <http://tlp.law.pitt.edu>.

<sup>410</sup> US Supreme Court, *California v. Ciarolo*, 476 U.S. 207 (1986) (“*California v. Ciarolo*”).

<sup>411</sup> US Supreme Court, *Florida v. Riley*, 488 U.S. 445, 450 (1989).

<sup>412</sup> US Supreme Court, *Dow Chem. Co. v. United States*, 476 U.S. at 239.

<sup>413</sup> *California v. Ciarolo*; Thompson, op. cit., 2013, p. 7.

<sup>414</sup> Supreme Court, *Kyllo v. United States*, 533 U.S. 27 (2001).

*casu* a thermal camera, to collect information regarding the interior of a home amounts to an invasion of an individual's reasonable expectation of privacy. Therefore, this activity constitutes a search under the Fourth Amendment and necessitates a warrant. In *United States v. Jones*<sup>415</sup>, the Court ruled that monitoring the location and movements of someone through the means of a GPS (Global Positioning System) attached to a vehicle constitutes a pervasive tracking and, thus, amounts to a Fourth Amendment search.

In light of these cases, it is not so clear when RPAS monitoring activities would constitute a search under the Fourth Amendment and require a warrant. However, it seems likely to depend upon four main factors: the privacy expectation of the society regarding the thing searched the area of the monitoring operation (public, private), the technology used and the duration of the surveillance.<sup>416</sup> In this regard, we cannot conclude that all monitoring activities operated through RPAS will necessarily be considered a search under the Fourth Amendment and require a warrant.

However, some more intrusive drones that are fitted with a range of technological payloads will likely lead to their consideration by the Courts, although it is unlikely that the Supreme Court will deliver just one clear precedent regarding RPAS technology.<sup>417</sup> It is noteworthy that a Federal Bill, the Unwarranted Surveillance Act of 2013, provides that law enforcement authorities must have a warrant before using RPAS for surveillance activities. Whilst this Bill has not yet been adopted, some States have already adopted warrant laws. Other states go even further by imposing a requirement on law enforcement agencies that they make available to the public information they collect with drones.<sup>418</sup>

### 5.5.3 Conclusion

In this chapter, we analysed the privacy legislation of two non-EU countries, Switzerland and the United States, in the context of legislative requirements applicable to RPAS technology. First of all, we observed that both of these countries have not adopted any specific privacy regulations for the RPAS technology. However, RPAS already operate in these third country airspaces. Secondly, after having analysed the Swiss privacy legislation framework, we remarked on the similarities between it and the European privacy and data protection legislation. In fact, this study shows that Swiss laws embody the main principles of the European Data Protection Directive and of the e-Privacy Directive. Thirdly, the privacy regime of the United States differs from the protective regimes of the EU Member States and Switzerland. We have seen that several American States have already enacted privacy regulation specific to the RPAS technology. It follows that almost all of these states have regulated governmental RPAS applications by submitting law enforcement authorities to obtain warrants before executing their surveillance mission. At the federal level, the analysis examined that the Congress has not adopted specific privacy regulations related to RPAS, despite many bills being debated. However, the FAA has enacted some privacy rules regulating the use of drones in tests sites. Moreover, we have observed that the First Amendment of the US Constitution, the Law of Privacy Torts, Statutes addressing harassment and stalking, and Statutes on corporate espionages may regulate some aspects of commercial

---

<sup>415</sup> Supreme Court, *United States v. Jones*, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring in the judgment).

<sup>416</sup> Villasenor, *op. cit.*, 2012; Thompson, *op. cit.*, 2013; Schlag, *op. cit.*, 2013.

<sup>417</sup> For more information about governmental RPAS use and the legislation see Villasenor, *op. cit.*, 2012; Thompson, *op. cit.*, 2013; Schlag, *op. cit.*, 2013.

<sup>418</sup> Villasenor, *op. cit.*, 2012

and private drones. Concerning RPAS used by government authorities, we observe that the Fourth Amendment and its related case law may be applicable to RPAS technology applications. In a second deliverable, we will assess their adequacy of cover in the context of civil drone usage, and will attempt to evaluate if these two legal privacy regimes could offer assistance to the European Union Member States when they consider regulating the RPAS technology.

## 5.6 International soft-law measures

Many authors<sup>419</sup> have recommended that RPAS technology actors (manufacturers, operators) ought to be regulated by privacy and data protection self-regulatory regimes such as guidelines, codes of conduct and/or codes of ethics this chapter concludes with an examination of existing soft law measures applicable to the privacy impacts of RPAS.

Following Roger Clarke, we recognise three types of self-regulation that may be relevant for RPAS technology.<sup>420</sup> *Organisational Self-Regulations*, where organisations of RPAS operators or organisations of RPAS commercial organisations limit their uses of drones to certain applications or set up some privacy guidelines such prohibiting vendors to sell some intrusive payloads to a certain category of people. By doing so “they recognise a responsibility to do so, or perceive it to provide them with a strategic or competitive advantage”.<sup>421</sup> *Industry-Self Regulation* happens when organisations of industries or sectors (journalism) “recognise the need for an industry-level commitment”.<sup>422</sup> *Co-Regulation* involves “one or more Codes negotiated between a regulator and an industry (manufacturers or corporates selling drones) or an organisation of operators, with the Code then being subject to enforcement”.<sup>423</sup> This sub-chapter examines two soft law measures related to RPAS technology as issued by aviation and drones experts - the Guidelines of the IACP, the Code of Conduct of the AUVSI and the Drone Journalism Code.

### 5.6.1 Recommended Guidelines for the Use of Unmanned Aircraft

The International Association of Chiefs of Police Aviation Committee has recently released guidelines concerning the RPAS.<sup>424</sup> Whilst this organisation self-regulation deals mainly with safety and technical aspects of RPAS use, it also acknowledges privacy as a concern: “where there are specific and articulable grounds to believe that the UAV will intrude upon reasonable expectations of privacy, the agency will secure a search warrant prior to conducting the flight”.<sup>425</sup> Moreover, it provides some pertinent stipulations concerning image retention:

---

<sup>419</sup> For example, Cavoukian, Ann, *Privacy and Drones: Unmanned Aerial Vehicles*, Information and Privacy Commissioner, Ontario, 2012; Clarke, Roger, “The Regulation of Civilian Drones’ Impacts on Behavioural Privacy”, *Computer Law & Security Review*, Vol. 30 No. 3, 2014.

<sup>420</sup> Clarke, op. cit., 2014.

<sup>421</sup> Ibid.

<sup>422</sup> Ibid.

<sup>423</sup> Ibid.

<sup>424</sup> IACP, “Recommended Guidelines for the Use of Unmanned Aircraft”, 2012.  
[http://www.theiacp.org/portals/0/pdfs/iacp\\_uaguidelines.pdf](http://www.theiacp.org/portals/0/pdfs/iacp_uaguidelines.pdf); Cavoukian, op. cit., 2012.

<sup>425</sup> IACP, op. cit., 2012.

1. *Unless required as evidence of a crime, as part of an on-going investigation, for training or required by law, images captured by a UAV should be retained by the Agency.*
2. *Unless exempt by law, retained images should be open for public inspection.*

Besides these privacy-related aspects, the Code also stipulates safety recommendations which may also be related to privacy:

1. *Equipping the aircraft with weapons of any type is strongly discouraged. Given the current state of the technology, the ability to effectively deploy weapons from a small UA is doubtful. Further, public acceptance of airborne use of force is likewise doubtful and could result in unnecessary community resistance to the program.*
2. *The use of model aircraft, modified with cameras, or other sensors, is discouraged due to concerns over reliability and safety.*<sup>426</sup>

### 5.6.2 Unmanned Aircraft System Operations Industry “Code of Conduct”

Through communication, education, advocacy, awareness and leadership, the trade group for the industry, the Association for Unmanned Vehicles Systems International (AUVSI), promotes and supports the unmanned systems and robotics industry. In 2012, this association has released an industry code of conduct<sup>427</sup>, which produces a set of guidelines and recommendations for a safe and non-intrusive use. This code is designed for manufacturers as well as operators. It includes ethical standards that are based on three themes: safety, professionalism and respect. Under the respect standard, the users are required to respect both privacy and the concerns of the public as they relate to unmanned aircraft operations. Furthermore, they also “support improving public awareness and education on the operation of UAS”.<sup>428</sup> Whereas the adequacy of such ethical recommendations will be assessed in the next deliverable, we can already affirm that some stakeholders were disappointed about the vague character of such points and the lack of privacy and data protection guidelines.<sup>429</sup>

### 5.6.3 Drone Journalism Code

One example of industry self-regulation included the Drone Journalism Code.<sup>430</sup> The College of the North Atlantic journalism instructor, Jeff Ducharme, has recently issued a code of ethics that he “plans to use when instructing his students on the use of drones for news

---

<sup>426</sup> Ibid.

<sup>427</sup> AUVSI, “Unmanned Aircraft System Operations Industry Code of Conduct”, no date. <http://www.auvsi.org/conduct>; Cavoukian, op. cit., 2012, p. 11.

<sup>428</sup> AUVSI, op. cit., no date.

<sup>429</sup> Vijayan, Jaikumar, “Drone industry's Code of Conduct Disappoints”, *ComputerWorld Blog*, 12 July 2012. <http://blogs.computerworld.com/privacy/20685/drone-industrys-code-conduct-disappoints>

<sup>430</sup> Ducharme, Jeff, “Drone Journalism Code”, *College of the North Atlantic Journalism Blog*, 2014. <http://www.cna.nl.ca/news/pdfs/Drone-code-of-conduct.pdf>

gathering”.<sup>431</sup> This Code encompasses 21 rules related to law, ethics and operation. Amongst the privacy rules, are the following:

- 1. The public has a right to know, but journalists must use common sense and compassion when determining what information and images will be released to the general public.*
- 3. Privacy laws for a drone are no different than for traditional photography and must be adhered to at all times.*
- 4. A drone is a powerful tool and it must be treated as such. A drone should only be used to gather information pertinent to a given story. Drones should not be used to search for stories.*<sup>432</sup>

However, despite the positive direction of this effort, the Drone Journalism Code has yet to gain much traction amongst professional journalists.

#### 5.6.4 Conclusion

In this chapter we examined examples of soft law measures applying to the civil use of RPAS. The result of this study is the observation that soft law measures provide only few, and make very broad, recommendations. However, soft-law examples make mention of privacy concerns, but any example provides enforcement mechanisms or setting up supervisory authority. Whilst the Guidelines attempt to discourage operators from equipping drones with payloads and weapons, they do not embody a rule of the data protection principles typical to legislative instruments in this area. Nevertheless, we agree with Ann Cavoukian, Privacy Commissioner of Ontario, when she says “this is a step in the right direction” but we note that enforcement mechanisms and privacy principles are lacking which would otherwise mean that these guidelines might have more influence.

### 5.7 General Conclusion

The present study enhances our understanding of the legal domestic privacy framework of the Member States applicable to the RPAS technology. The previous chapter argued that European data protection legislation is applicable to private agencies (including, corporates, journalists and other professionals) and public authorities using drones to record data. However, it also emphasised that private individuals and law enforcement using governmental drones for recording personal data remain practically un-regulated. Furthermore, the current European privacy legal framework does not offer specific CCTV regulations, and only privacy rights may apply in cases of visual surveillance without recording.

After having studied not only privacy legislation but also surveillance regulations of several Member States, our main conclusion is that at the domestic level, law enforcement authorities using RPAS are partially regulated by the data protection acts and private users of drones remain totally unregulated. Nevertheless, that besides privacy, Member States encompass

---

<sup>431</sup> The Western Star, “Instructor Develops Code of Ethics for Drone Journalism”, *News*, 2014.  
<http://www.thewesternstar.com/News/Local/2014-06-06/article-3752935/Instructor-develops-code-of-ethics-for-drone-journalism/1>

<sup>432</sup> Ducharme, op. cit., 2014.

other types of law which could apply to private users to regulate some aspects of domestic drones. Member States could extend the application of several rules of civil law, criminal law or property law to the RPAS technology, for example, in order to prohibit some uses of RPAS, payloads or areas where drones can fly. Particularly in the analysis of the United States legislation applicable to private and professional drones, there exist privacy torts that consist in a mix of property, civil and privacy laws applicable to RPAS. Finally, domestic regulations do not provide sector-specific privacy regulations applying to industries of sophisticated and intrusive technologies, neither at the manufacturing level nor at the distribution level. The adequacy of all identified laws and regulations in this first contribution will be further examined in the next deliverable; however, we can already say that the existing soft-law measures do not provide satisfactory privacy guidelines.

## 6 CONSULTING WITH KEY STAKEHOLDERS

In this section we examine the results of the consultation exercises with key stakeholders in the civil use of RPAS. These consultation exercises were two-fold. First, project partners undertook three face-to-face consultations with stakeholders, including one panel discussion with civil society organisation representatives organised during the annual Computers, Privacy and Data Protection conference in Brussels, a consultation with Data Protection Authorities organised by the Directorate General for Enterprise and Industry and a project workshop with stakeholders representing industry, data protection authorities, legal experts and policy-makers. The purpose of the consultation exercises was to understand the current positioning of stakeholders within the debates around privacy, data protection and the civil deployment of RPAS, with special attention to their particular stakeholder location.

Second, project partners designed, distributed and analysed a set of surveys on privacy, data protection and the use of RPAS for civil applications. The surveys were distributed to four different stakeholder categories:

- Industry representatives (including RPAS designers, manufacturers and operators)
- Data Protection Authorities
- Civil society organisations
- Civil Aviation Authorities

The researchers had varying levels of success in reaching each of these four groups. Industry representatives were the most highly represented organisation, while Civil Aviation Authorities proved difficult to incentivise to participate. For all organisations, the survey was used to assess their levels of awareness of RPAS capabilities and applications, as well as the associated threats to privacy, data protection and ethics. The survey also enabled an examination of the current consultation activities undertaken by each stakeholder group and any activities they have undertaken internally to address privacy and data protection concerns associated with civil RPAS. This chapter provides an analysis of the survey findings with key inputs from the stakeholder consultations included to provide context or specific information.

### 6.1 Industry analysis

#### 6.1.1 Overview

The organisations that responded to the survey were primarily based in Europe, although many operated in a number of European countries and had operations in third countries (i.e., outside of Europe). Furthermore, most of the respondents to the survey were high-level executives and/or directors. However, many of the companies were small enterprises, and in some cases, one-person enterprises. In total, 94 individuals responded to the survey.

The survey respondents indicated that their companies undertook a range of RPAS activities. 86% of respondents indicated that they were RPAS operators, while 40% and 38% indicated that they were RPAS designers and manufacturers respectively (respondents were invited to choose more than one option). 76% indicated that they design manufacture or operate Quad-copter type RPAS, while 51% indicated that they used fixed wing, plane-like RPAS. A further 18 respondents (20%) indicated that they were also designing, manufacturing and/or operating other types of remotely piloted vehicles, including boats, cars and crawlers. Furthermore, the range of companies that answered the survey is further indicated by the sales figures reported

by respondents, where many respondents indicated that they had sold one, two or only a handful of RPAS the previous year, while others indicated that they sold hundreds of units.

### 6.1.2 Capabilities and applications

The RPAS designed, manufactured and operated by our survey respondents tended to be small RPAS that could not fly very high, but which could carry a significant range of payloads. In relation to RPAS size, small RPAS weighing less than 20kg were the most popular. RPAS weighing less than 2kg were produced or used by 52% of respondents, those between 2-7kg were produced or used by 67% of respondents and RPAS between 7-20kg were produced or used by 37% of respondents, while only 16% of respondents indicated that they produced or used RPAS larger than 20kg. Furthermore, the vast majority of respondents indicated that their RPAS could stay aloft less than one hour (81%) and could fly less than 500m high (62%). Likely because of their low altitude capabilities, 83% of respondents indicated that their RPAS was visible from the ground.

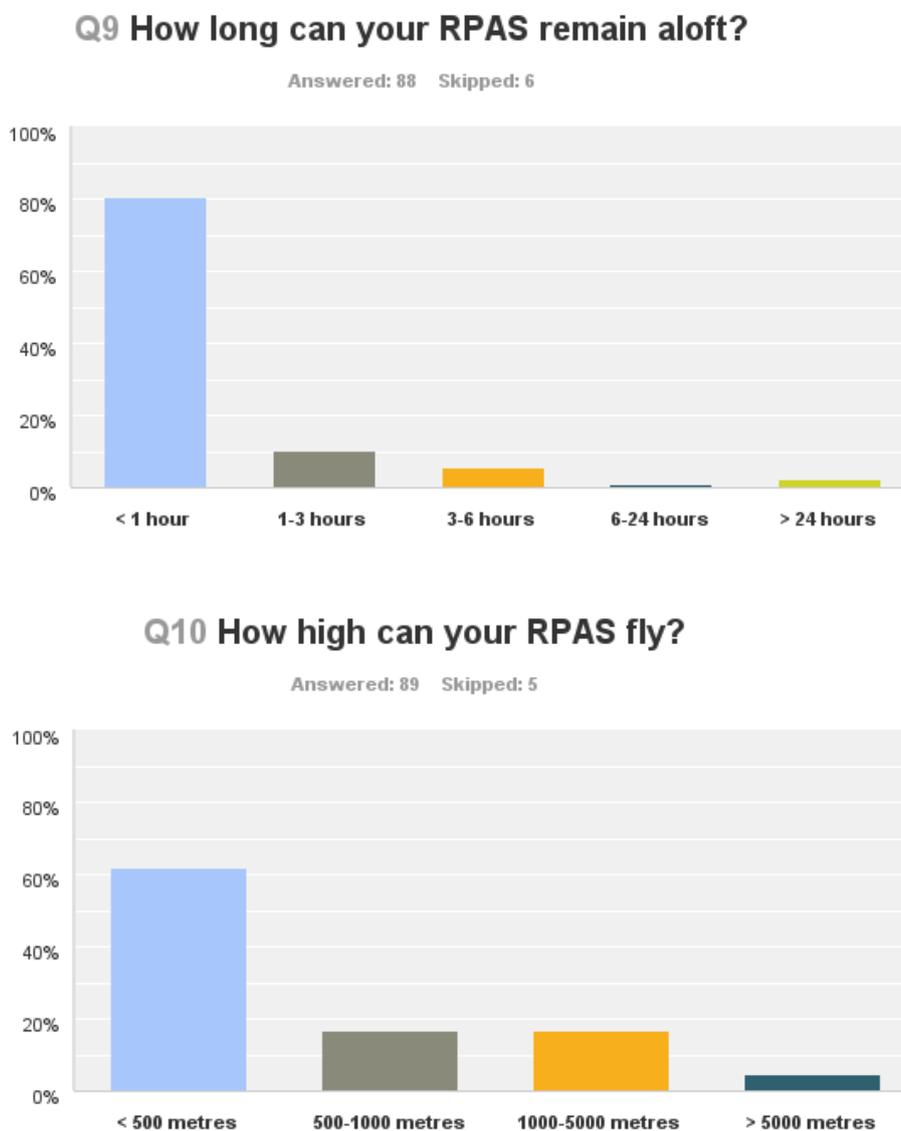


Figure 1: RPAS capabilities

In relation to the payloads they carried, survey respondents indicated that their RPAS could carry a range of payloads, including photographic and thermal imaging cameras, GPS location equipment and environmental sensors.

**What types of payloads do(es) your RPAS carry? (Please tick all that apply)**

Answer choices	
Photographic cameras	98%
Thermal imaging cameras	61%
Geolocation equipment	51%
Communication equipment	34%
Environmental sensors (e.g., toxins)	24%

Table 2: RPAS payloads

In the project workshop, participants confirmed that most RPAS applications used aerial photography payloads in their services. Although most of the geo-location equipment and communication equipment was geared towards RPAS flight control, such payloads could be, and possibly already are being, used to locate or communicate with objects external to the RPAS system.

Respondents who indicated that they are RPAS operators reported that their operations are primarily situated in the following sectors: commercial or corporate (94%), emergency services (29%), government (23%), private individuals (21%) and law enforcement (16%). This links relatively well with the information provided by RPAS designers and manufacturers who have indicated that other companies, government and private individuals are currently their primary customers.

**Q20 What types of organisations are your current customers? (Please tick all that apply)**

Answered: 54 Skipped: 40

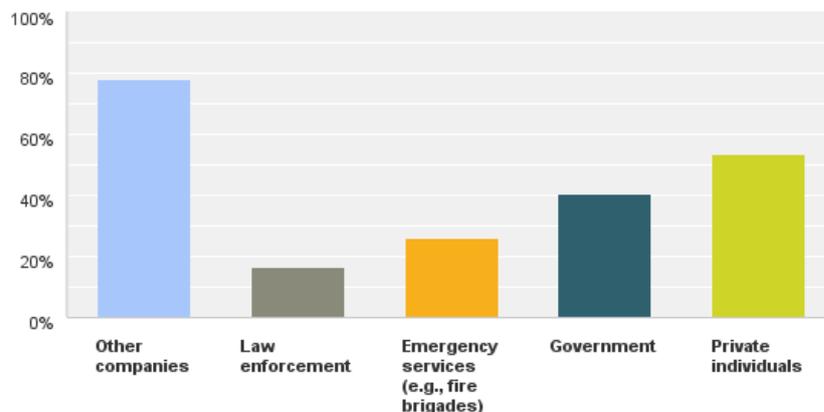
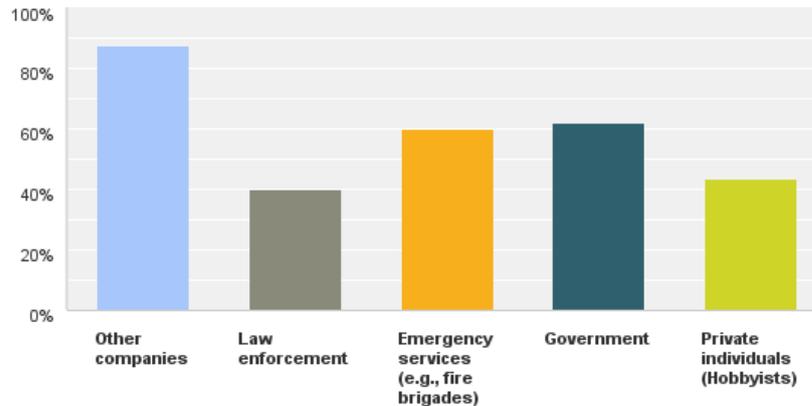


Figure 2a: RPAS manufacturers primary current and future customers

**Q21 What types of organisations are your potential customers? (Please tick all that apply)**

Answered: 55 Skipped: 39



*Figure 3b: RPAS operators primary current and future customers*

The graphics above (Figures 2 a and b) also indicate that the RPAS industry hopes to expand its already significant customer by building customers in emergency services and government agencies. The RPAS industry also seems interested in somewhat decreasing their private individual customer base. Finally, in relation to future capabilities, RPAS designers and manufacturers report that they would like to develop the capabilities in relation to environmental sensing (67%), video or photography (62%), wide area surveillance (51%), geo-spatial surveying (44%) and telecommunications (24%).

### 6.1.3 RPAS data collection

In relation to what types of data they collect, almost all industry representatives (99%) indicated that their RPAS collected visual or photographic images, while 53% collected geo-spatial data and 44% collected environmental data. However, one respondent clarified that the type of data collected depends “entirely on what sensors are added” to the remotely piloted aircraft system.

Although a significant minority of RPAS industry representatives indicated that their RPAS did not collect images of members of the public (45%), the majority (55%) stated that their systems either did capture members of the public, or that they did not know whether they captured members of the public. Furthermore, 97% of respondents indicated that the data captured by the RPAS was recorded, and 71 respondents (76%) indicated that the data recorded by the RPAS was stored. Storage times varied from 20 minutes to “indefinitely” and “until it is deleted”. Finally, others indicated that the data was turned over to the client and responsibility for storing or deleting the data transferred to the client. In the consultation workshop, industry representatives expressed confusion about data protection concerns associated with their use of RPAS, as most actual applications were confined to unintentionally capturing “the tops of people’s heads”.

#### 6.1.4 *Industry perspectives on privacy and data protection*

RPAS industry representatives are primarily focused on the technical capabilities of their RPAS and the skills needed to operate them effectively. As a result, it is not surprising that most RPAS industry representatives are not well informed about European and national privacy and data protection regulations. Specifically, 65% of respondents characterised their understanding of European privacy and data protection regulations as “Basic” or “Poor”. Similarly, half of the respondents characterised their understanding of national privacy and data protection regulations as “Very good” or “Good”, while the other half described them as “Basic” or “Poor”. In total, the most common answer for both questions was that the respondent had a “Basic” understanding. However, RPAS industry representatives did indicate that they had a comparatively better understanding of national legislation than European legislation.

This is supported by participants’ reports on the data protection and privacy issues raised by their use of RPAS. Specifically, although the majority of industry respondents indicated that their RPAS captured images of members of the public, and that this data was recorded and stored, the majority of respondents also indicated that their use of RPAS did not raise any privacy or data protection issues. Specifically 62% of RPAS manufacturers and operators indicated that their RPAS did not raise such issues. However, in relation to future capabilities only approximately half of respondents (48%) indicated that they did not raise privacy or data protection issues, with the other half answering that they did raise such issues or that they were not sure if they would raise such issues. Thus, it is possible that the focus on filming “the tops of people’s heads” was thought not to raise privacy or data protection issues due to the difficulty associated with identifying people from that angle. However, Data Protection Authorities and other legal experts pointed out that such filming, when combined with images of homes or landmarks could in fact be considered personal information.

However, despite the perceived lack of privacy and data protection issues relevant to the development and deployment of RPAS, many organisations had undertaken internal procedures to address these issues. Sixty-one per cent of RPAS manufacturers and 57% of RPAS operators indicated that they had considered the privacy and data protection issues associated with their RPAS. For manufacturers, this took place during the conceptual and design phase, with another interesting up-tick in the distribution phase, indicating that some RPAS manufacturers took responsibility for how the RPAS may be utilised once it left their control.

**Q27 If so, at what stage in the manufacturing process did this consideration take place? (Please tick all that apply)**

Answered: 41 Skipped: 53

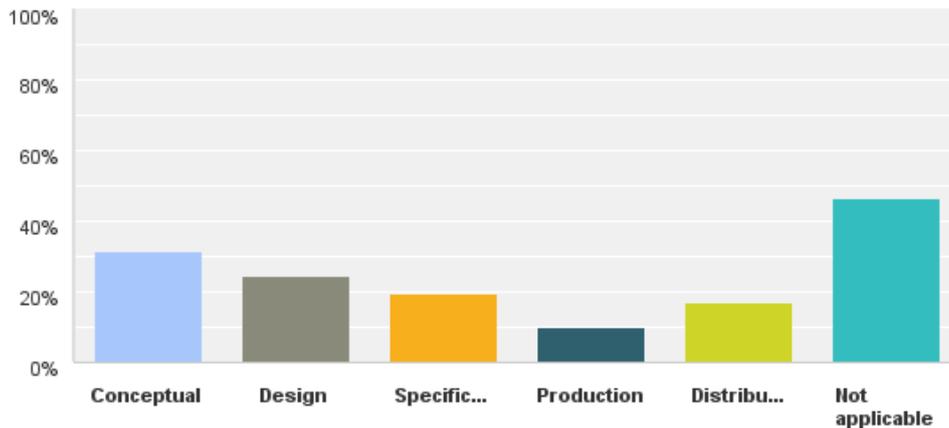


Figure 3: Privacy and DP impact assessment in RPAS manufacturing

When asked how this consideration took place, both RPAS manufacturers and operators indicated that risk assessment and codes of conduct were the most popular instruments utilised to conduct this assessment.

**Q28 Please indicate any instruments that you used to conduct this assessment. (Please tick all that apply)**

Answered: 40 Skipped: 54

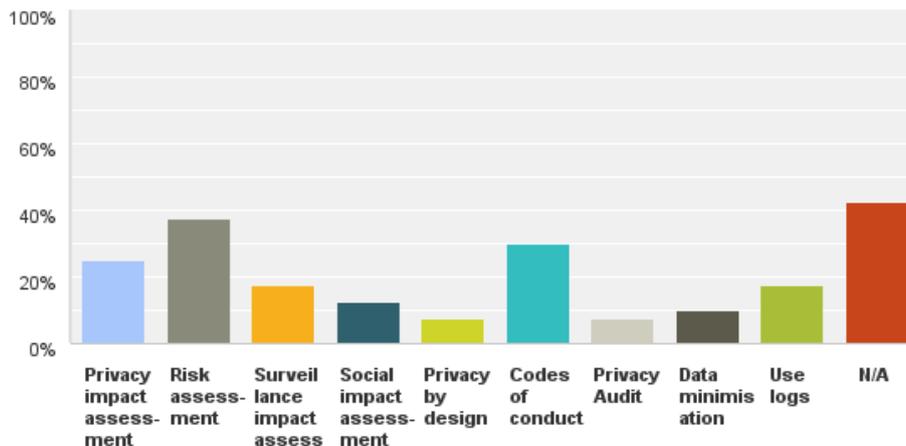


Figure 4a: Privacy and DP assessment by RPAS manufacturers

**Q35 If so, please indicate any of the instruments that you used to conduct this assessment. (Please tick all that apply)**

Answered: 48 Skipped: 46

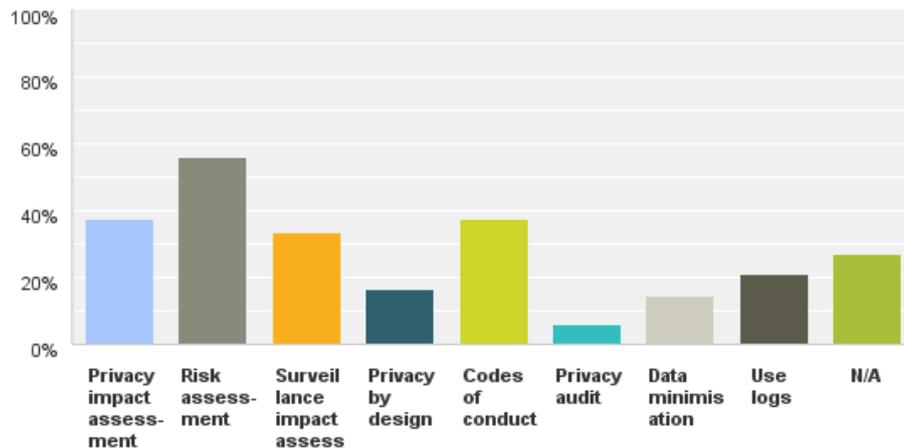


Figure 4b: Privacy and DP assessment by RPAS operators

The figures above (Figures 4a and b) indicate that some instruments for conducting privacy or data protection assessments are more popular than others. Comparatively, operators appear more likely to conduct such assessments than manufacturers; however the survey results indicate that for the majority of industry representatives who responded to the survey, such assessments are familiar and could be rolled out to a larger group of RPAS manufacturers and operators.

Although not widely reported, some of the “fixes” associated with addressing privacy or data protection issues include processes such as scrubbing, anonymisation and pilot training. For example, one UK RPAS proprietor described how images of people were dealt with. “Members of public only very rarely captured by accident at small unidentifiable size in background. All images are checked at editing stage and people removed from image.” In relation to anonymisation, one Spanish respondent describes blurring images of people or vehicles. Another respondent described a pilot operation assessment procedure, which includes a “risk assessment that includes data capture and privacy issues. Flight operation considers how to capture enough data to complete the job without excessive data capture that is not necessary.” Additional procedures reported in the workshop included announcing that the RPAS would be filming to the local area or arranging RPAS filming to coincide with lunch breaks in industry settings in order to minimise the amount of personal data collected.

### 6.1.5 Consultations and regulations

The survey results indicate that RPAS industry representatives are willing to participate in consultations and are familiar with submitting to regulation or oversight related to RPAS. The vast majority of RPAS industry representatives (73%) have participated in consultations regarding the use of RPAS in civil air space. These consultations were most likely to have been initiated by other industry organisations, but a significant number of respondents also

reported that national governments and civil society organisations also initiated consultations. However, very few (<10%) had been in contact with their national Data Protection Authority. In most cases (61%) this consultation was related to national policy, rather than European or local policy.

Furthermore, RPAS operators are relatively used to being regulated. Sixty-seven per cent of RPAS manufacturers and operators indicated that they were subject to regulation by a particular Civil Aviation Authority, 81% of RPAS manufacturers indicated that they had to obtain authorisation from their CAA before they flew. Furthermore, of those who did have to obtain authorisation, 44% of them did have to certify that they had considered the privacy and data protection issues relevant to their flight before proceeding. Thus, for a significant minority of RPAS operators, the privacy and data protection issues associated with RPAS are quite relevant. This is supported by 70% of respondents' indication that clear guidelines on privacy and data protection issues would assist them in their work.

### Q38 Would clear guidelines on the privacy and data protection issues related to RPAS assist you in your work?

Answered: 76 Skipped: 18

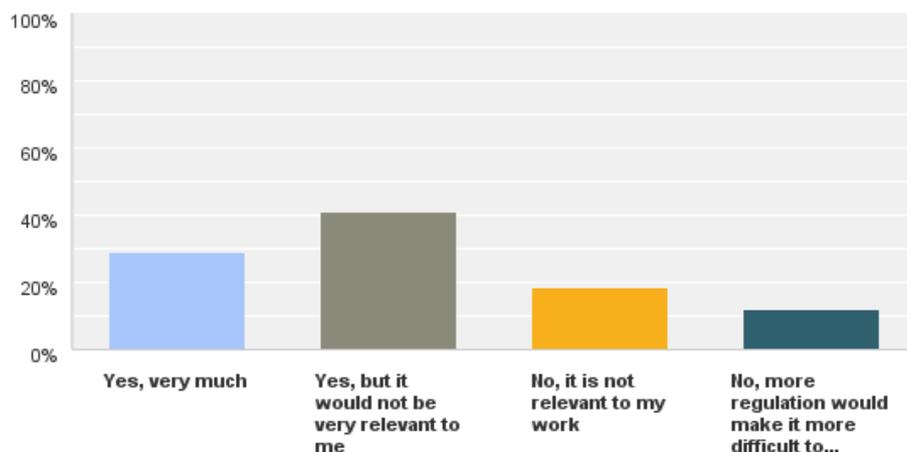


Figure 5: RPAS industry interest in guidelines

Thus, there is significant scope for improving the privacy and data protection advice offered to RPAS industry representatives. While this would be particularly useful for those who are operating RPAS professionally, and who take seriously their obligations under current legislation, RPAS industry representatives also point out that there is a significant minority of operators, in particular, who operate outside, or without consideration of, the law in this area. In these cases, better enforcement of existing regulations, rather than additional regulations would be most beneficial.

In summary, some RPAS industry representatives are relatively aware of their obligations in relation to privacy and data protection, but much more education is needed as a number of key gaps remain. Specifically, while many RPAS industry representatives feel that the privacy and data protection issues are not relevant to their work, a significant number of respondents indicated that their RPAS captures and records images of members of the public and that those images are stored and/or transferred to other organisations. This means that their use of

RPAS is capturing personal information and thus is subject to the Data Protection Directive as well as national data protection legislation. However, many organisations appear unaware of that the information they are collecting makes them subject to this legislation. While some organisations are evaluating the privacy and data protection impacts of their operations, this remains a minority, which must be expanded using some form of “soft law” measure or regulation.

## **6.2 DPA Analysis**

### *6.2.1 Overview*

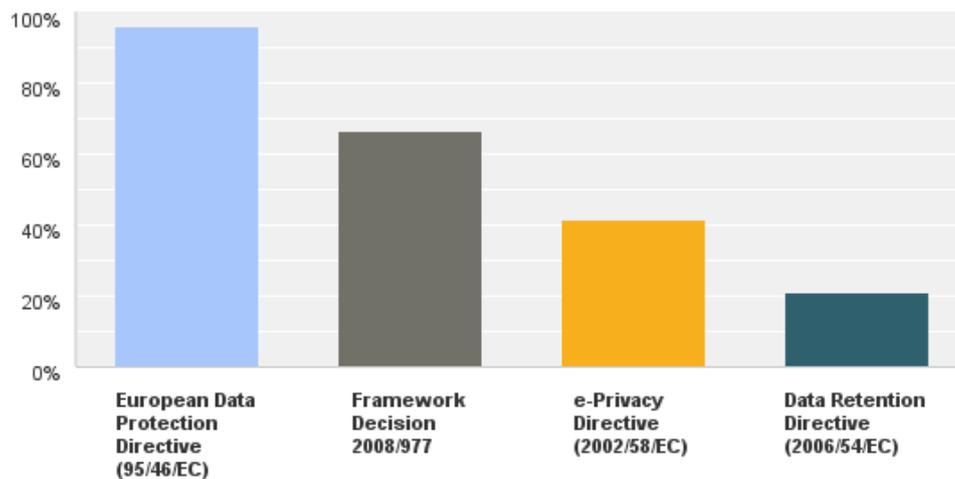
The survey of Data Protection Authorities achieved a fairly good response rate among DPAs in Europe. Specifically, the survey generated responses from 19 of the 28 European Member States. Most countries contributed one response, while a few (Slovenia, Slovakia and Germany) contributing multiple responses from within their organisation. In total, only three countries indicated that they currently have written positions in relation to the use of RPAS for civil applications - Belgium, the Czech Republic and Germany – while a further three - Hungary, the Netherlands and the UK – are currently drafting positions. In addition, six DPAs indicated that their countries are currently considering legislation to govern the use of RPAS. These countries considering legislation included the Czech Republic, Estonia, Hungary, Slovakia and Spain.

DPAs reported having a good knowledge of the technological capabilities and potential applications of civil RPAS, and appeared fairly informed. The majority of DPAs described themselves as having a good (44%) or basic (48%) understanding of the capabilities of RPAS, although only one respondent claimed to have “very good” knowledge (a respondent from Slovakia). The majority of DPA respondents also described themselves as having a “good” (63%) understanding of the potential civil applications of RPAS, while a further 29% reported a basic knowledge. However, given the subject matter of the questionnaire, it may be that this group was self-selecting, and DPAs with no in-house expertise or interest related to RPAS may have been among those who did not respond to the questionnaire.

In relation to the legal framework applicable to RPAS used for visual surveillance, DPAs cited many existing legislative instruments. At the European level, all of the DPAs who answered this question agreed that the Data Protection Directive (95/46/EC) was applicable to the use of RPAS for visual surveillance (96%), two-thirds agreed that the 2008/977 Framework decision was applicable and a significant minority felt that the e-Privacy Directive (41%) and the Data Retention Directive (20%) might also be applicable.

**Q4 Which elements of the European privacy and data protection legal framework are applicable to RPAS, especially as used for visual surveillance, in your opinion? (Please tick all that apply)**

Answered: 24 Skipped: 3



*Figure 6: RPAS applicable privacy and DP legislation*

All of the DPAs who answered this question also agreed that their national data protection laws were applicable to the use of RPAS for civil applications (96%). Sixty-two per cent agreed that their national privacy laws were applicable and 46% agreed that their national CCTV legislation was applicable. Of the respondents who indicated other, additional laws were applicable, many of these centred on laws surrounding police surveillance and one respondent mentioned local legislation.

### 6.2.2 Privacy, data protection and ethical issues

In relation to the **potential privacy impacts** of RPAS, there were significant differences in how DPAs viewed the risks, based on the stakeholder who was conducting the surveillance. The survey asked DPA respondents whether the use of RPAS for different purposes carried privacy risks related to the following: respect for home and family life and respect for communications (as enshrined by the Charter of Fundamental Rights of the European Union) as well as the right to be let alone, a more common-law understanding of privacy originating in US legal opinions. The questions examined the level of concern for privacy generated by law enforcement uses of RPAS, commercial uses of RPAS for infrastructure inspection (a very common application) and private users of RPAS.

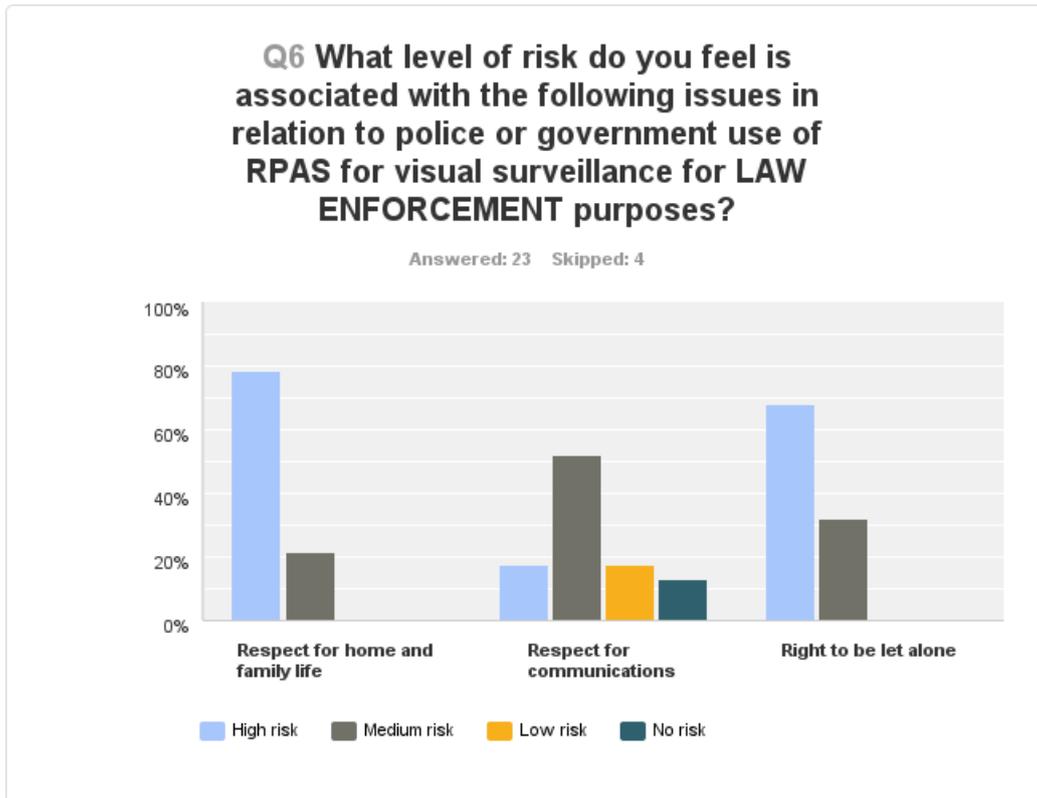


Figure 7a: DPA assessment of privacy issues and relative risk

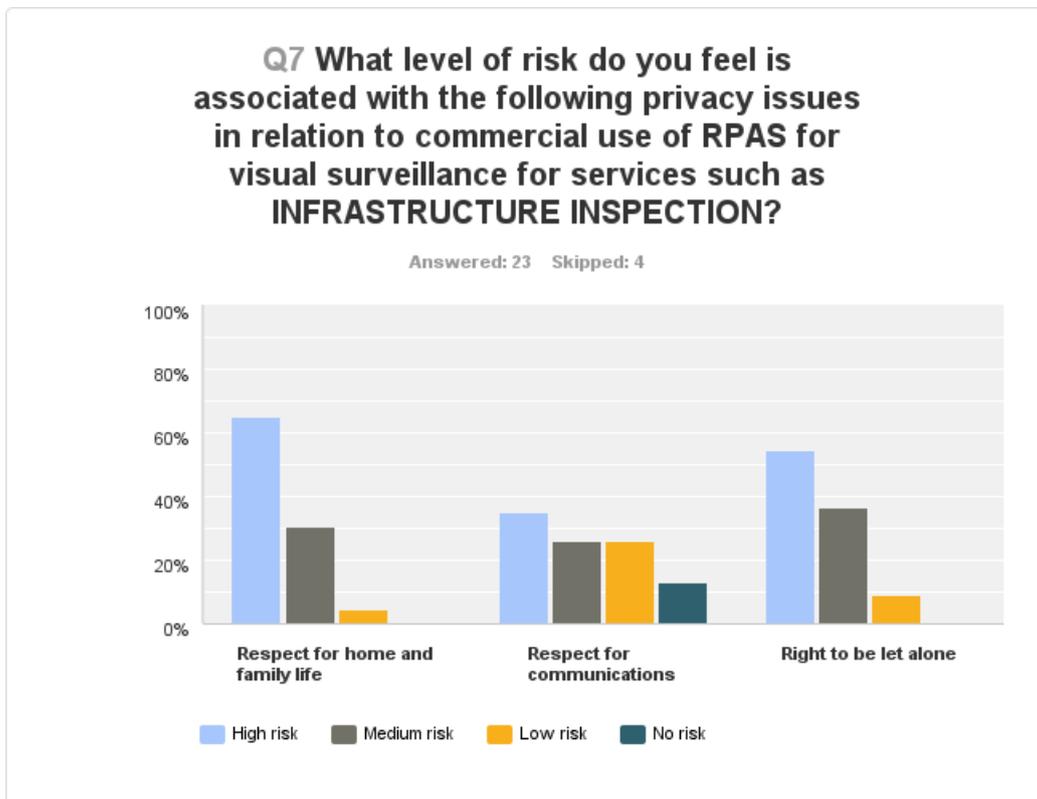


Figure 7b: DPA assessment of privacy issues and relative risk

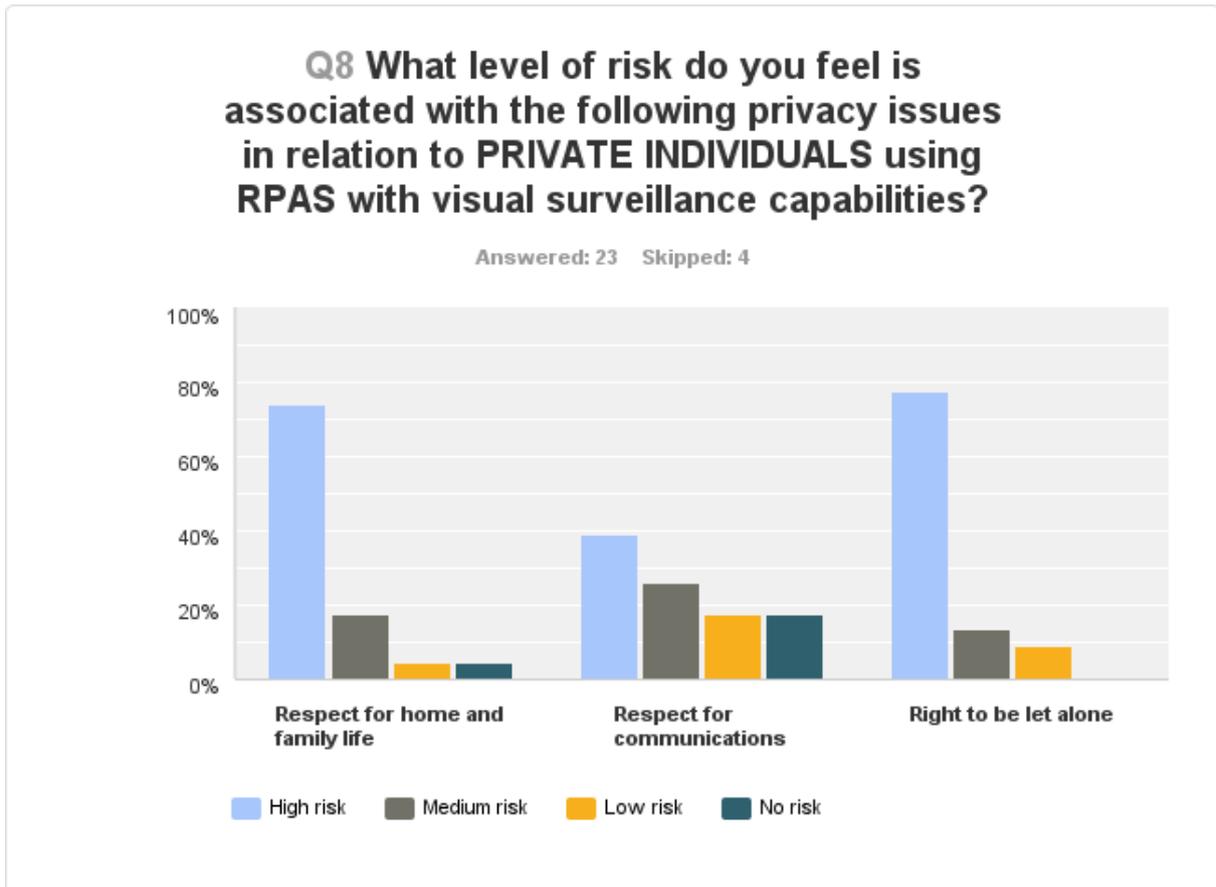


Figure 7c: DPA assessment of privacy issues and relative risk

Here the use of RPAS for visual surveillance seems to incite more concern with respect to its use by law enforcement and private individuals, than commercial users. Furthermore, in all cases, the right to home and family life and the right to be let alone emerge as higher “risk” issues than respect for communications. This is not surprising as visual surveillance does not specifically focus on communication (although in some cases communication can be inferred). Therefore, while all users of RPAS for visual surveillance seem to generate concern, corporate or commercial uses of RPAS appear to be the most trusted users and applications, relatively speaking.

In relation to **data protection**, the survey examined a number of issues emanating from the Data Protection Directive, and most of these issues emerged as being significant risk areas for the use of RPAS by all types of stakeholders. The data protection element of the DPA survey examined the following issues:

- Transparency
- Data minimisation
- Proportionality
- Purpose limitation
- Consent
- Accountability
- 
- Data security
- Rights of access
- Rights of correction
- Third country transfers
- Rights of erasure

In relation to police use of RPAS, transparency, data minimisation, proportionality, purpose limitation and rights of access emerged as high-risk issues. However, when combining high risk and medium risk, all of the data protection elements, aside from data security and third-country transfers, emerged as significantly risky, with more than 80% of respondents stating that each issue was either high risk or medium risk. In the DPA consultation workshop, proportionality emerged as a key risk in relation to RPAS filming using aerial photography. With regard to commercial use of RPAS for infrastructure inspection, all of the data protection elements were regarded as having significant risk (i.e., high risk or medium risk) by more than 80% of respondents, with the exception of third-country transfers. However, this risk was more evenly distributed between high risk and medium risk responses. Finally, in relation to private individuals using RPAS, *all* of the data protection issues examined, except third country transfers, were identified as high risk by the majority of respondents. This means that like privacy, law enforcement users and individual “hobbyists” were regarded by DPAs as the most high-risk RPAS users, with commercial users or uses being slightly less problematic. However, as a representative from the Slovakian DPA pointed out:

*Law enforcement agencies are very well aware of national data protection legislation and they are ready to adjust adequate legislation as soon as it is necessary to be able to use RPAS. We consider more problematic to set out the rules for commercial and civil use of RPAS.*

Thus, enforcement and accountability also emerged as a key element of data protection for some respondents.

The examination of **ethical issues** focused on a number of elements that were related to privacy and data protection, but which fell outside of their specific scope. The surveys examined ethical issues such as:

- Discrimination
- Chilling effect
- Dehumanisation of the surveilled
- Public dissatisfaction
- Function creep

As described in Chapter 4, a chilling effect refers to the anticipatory conformity associated with knowing surveillance may be occurring. Thus, the possibility of surveillance prompts people to behave as though surveillance were in place, even if none is occurring. Function creep refers to the expansion of a system originally designed or acquired for one purpose to additional purposes not originally envisaged.

**Q12 What level of risk do you feel is associated with the following ethical issues in relation to police or government use of RPAS for LAW ENFORCEMENT purposes?**

Answered: 22 Skipped: 5

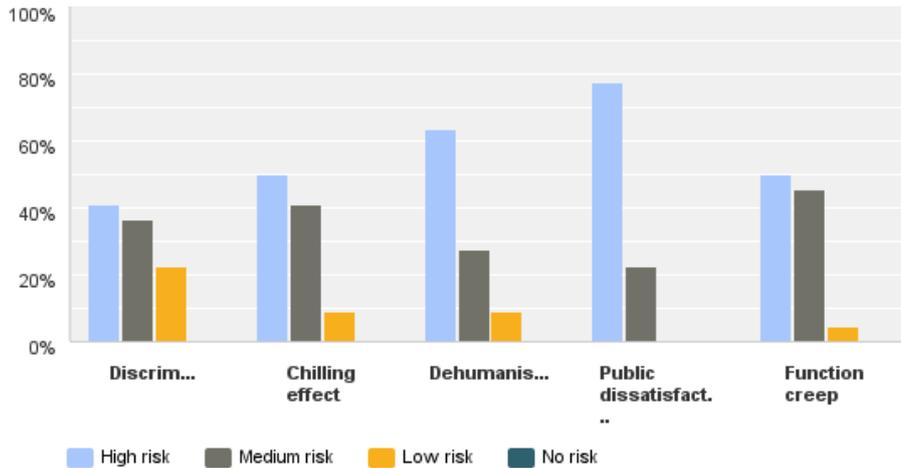


Figure 8a: DPA assessment of ethical issues and relative risk

**Q13 What level of risk do you feel is associated with the following ethical issues in relation to commercial use of RPAS for visual surveillance for services such as INFRASTRUCTURE INSPECTION?**

Answered: 23 Skipped: 4

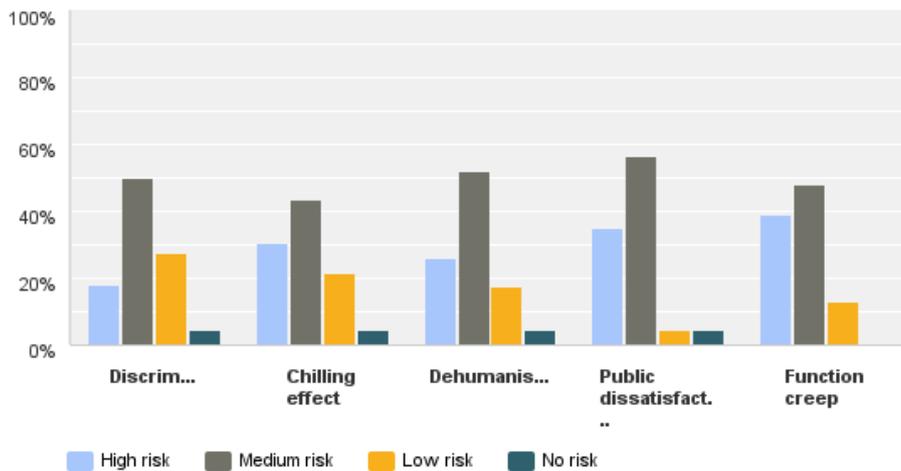


Figure 8b: DPA assessment of ethical issues and relative risk

**Q14 What level of risk do you feel is associated with the following ethical issues in relation to PRIVATE INDIVIDUALS using RPAS with visual surveillance capabilities?**

Answered: 23 Skipped: 4

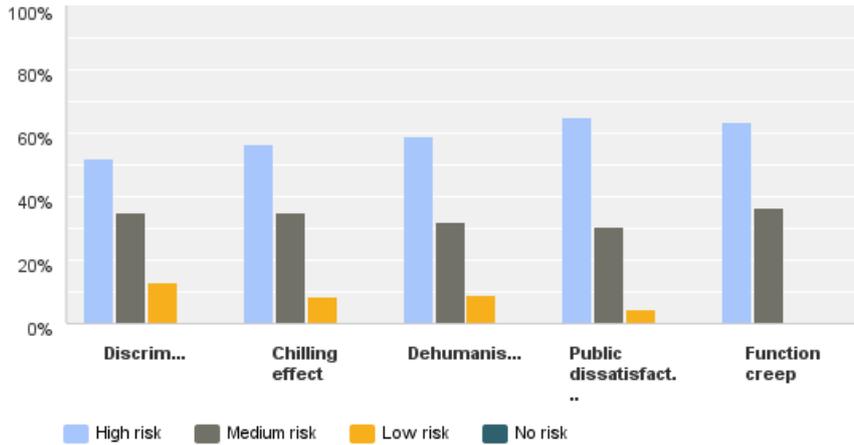


Figure 8c: DPA assessment of ethical issues and relative risk

According to the responses by Data Protection Authorities, these ethical issues were deemed to be of greater concern and higher risk in relation to law enforcement uses of RPAS for visual surveillance, and for private use of RPAS for visual surveillance. As in relation to the privacy issues, commercial uses were deemed to be more likely than these other categories to be of medium risk. However, the risk was considered significant across all three stakeholder categories.

**Q15 Given the issues identified above, what level of risk do you feel is associated with the commercial use of RPAS with thermal imaging capabilities in relation to:**

Answered: 23 Skipped: 4

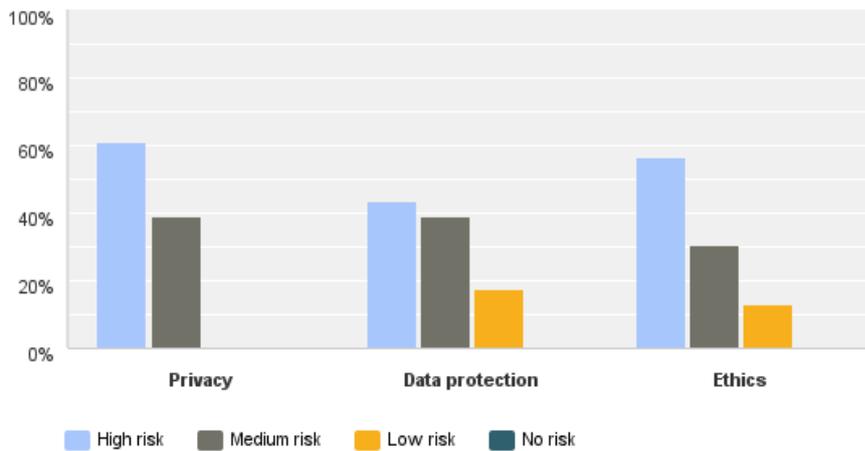


Figure 9a: DPA assessment of risks associated with future RPAS capabilities

**Q16 Given the issues identified above, what level of risk do you feel is associated with the commercial use of RPAS for providing communication services, such as mobile broadband, in relation to:**

Answered: 22 Skipped: 5

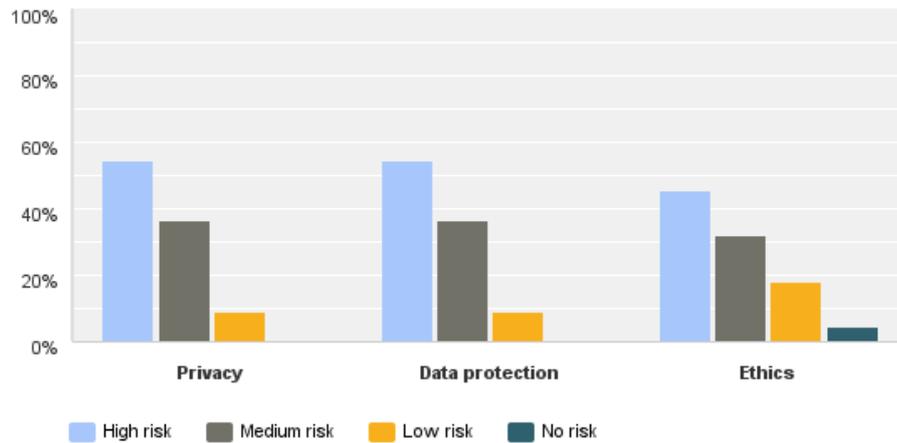


Figure 9b: DPA assessment of risks associated with future RPAS capabilities

**Q17 Given the issues identified above, what level of risk do you feel is associated with the use of RPAS for biometric identification, such as face recognition, in relation to:**

Answered: 23 Skipped: 4

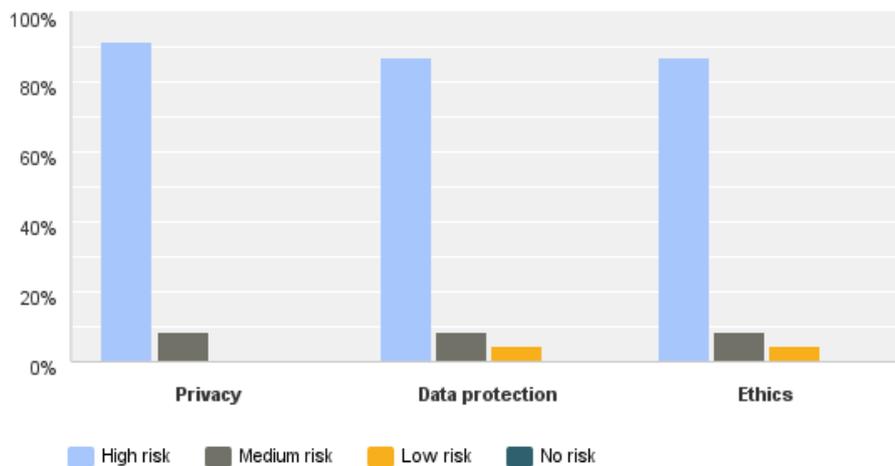


Figure 9c: DPA assessment of risks associated with future RPAS capabilities

Finally, with regard to additional capabilities of RPAS beyond visual surveillance, DPAs felt that different applications resulted in different levels of threat to privacy, data protection and ethics. Specifically, applications that processed sensitive data such as the use of facial recognition technology to process biometric data carried the greatest risk to all three areas. While enabling communication linkages through broadband provision and thermal imaging carried less risk, although the risks remained significant. This is particularly important as many of the industry participants indicated that capabilities such as thermal imaging and telecommunications.

### 6.2.3 Consultations and regulations

Some DPAs were involved in policy-making associated with RPAS, but this number remained relatively small. Only 1/3 (34%) of the DPAs who responded to this question indicated that they have participated in a consultation on the civil use of RPAs, in addition to the consultation carried out by the European Commission DG ENTR in May 2013. For the six who have participated in additional consultations, half of these respondents indicated that it was their national CAA that initiated this consultation (Belgium, Czech Republic and Germany), and two participants indicated that the consultation was initiated by the European government (Hungary, Slovakia) and their national government (Slovenia). One respondent, Belgium, indicated that a CSO initiated the consultation. This breadth of consultations demonstrates that there are a number of different stakeholder categories implicated in the development of civil deployment of RPAS; however, the lack of connection and communication between Data Protection Authorities and industry provides weight to the finding discussed in the previous section that many industry representatives do not recognise or are not interested in the potential privacy and data protection impacts introduced by their use of RPAS for civil applications.

In addition to consultations, some DPAs (18%) have indicated that they have taken independent actions in relation to the privacy and data protection aspects of RPAS. One participant, the UK, stated that RPAS use has been included in their CCTV code of practice. Germany has written to the national railway to enquire about their use of RPAS to monitor their tracks (The response was that no personal information was collected). Two countries, Portugal and Italy, have contacted their CAA directly. In some countries, these consultations have resulted in affirmations or legislation that instructs RPAS users that they are subject to national data protection legislation. For example, an Italian DPA survey respondent described the new legislation in Italy that resulted from their consultation with their national CAA:

*On 16th December 2013, ENAC adopted a Regulation on RPAS which contains a provision whereby compliance with data protection rules must be examined before granting any permission to operate a RPAS (Article 22: Data protection and privacy). According to its second comma, personal data must be processed in respect of the Italian Data Protection Code, particularly with regard to the use of modalities that allow for a person to be identified only in case of necessity, pursuant to Art. 3 of the Code, as well as in accordance with the measures and precautions to safeguard people concerned as prescribed by the Authority in charge of the protection of personal data.*

Finally, with respect to the further regulation of RPAS, and particularly their potential privacy and data protection impacts, DPAs provided mixed opinions as to whether CAAs were well placed to address these issues. A clear, but significant, minority (41%) reported that the CAAs are well positioned to enforce good practice in relation to the privacy and data protection elements of RPAS. However, other respondents who disagreed indicated that the CAAs are

not privacy and data protection specialists and are not focused on privacy and data protection as their primary goal, which represents a significant stumbling block for using the CAAs to enforce good practice in relation to privacy and data protection. As one respondent indicated, “They are mainly concerned with security, safety, insurance, certification processes rather than data protection”.

Although the DPAs reported good to basic knowledge of RPAS capabilities and applications, their main specialty lies in examining potential privacy and data protection issues. Thus, they are well situated to comment on the potential impacts of the use of RPAS for civil applications in these areas. However, the focus on the “potential” impacts of RPAS necessarily invites DPAs to consider worst-case scenarios rather than likely scenarios. Therefore, it is worth bearing in mind that better regulation could assist with bridging the gap between these potential impacts and the current and future actual uses of RPAS for civil applications.

### 6.3 Civil society organisation analysis

#### 6.3.1 Overview

The questionnaire (see Appendix X) was sent by e-mail to 75 civil society organisations (CSOs) in the EU and third countries with an interest in human rights, digital rights, surveillance or privacy issues. The target organisations were selected on the basis of their stated mandate and expertise, participation in previous public consultations on issues of privacy, civil liberties and fundamental rights, or having taken a public position or demonstrated an interest in the issue of (non-military) RPAS. A hyperlink to the questionnaire was also circulated on social media platforms and several websites. The survey received 17 responses from a range of countries, a subset of which are outlined below.

*Table 3: Civil society organisations consulted*

#	Organisation	Country
1	American Civil Liberties Union (ACLU)	USA
2	Australian Privacy Foundation	Australia
3	Big Brother Watch	United Kingdom
4	Chaos Computer Club	Germany
5	Digital Rights Ireland	Ireland
6	Electronic Frontiers Foundation (EFF)	USA
7	Initiative für Netzfreiheit	Austria
8	Institute for Human Rights	Germany
9	Panoptikon Foundation	Poland
10	Privacy International	United Kingdom
11	Statewatch	United Kingdom
12	Transnational Institute	Netherlands

While the pool of respondents is quite small, it nevertheless includes some of the best known CSOs working on privacy issues to have expressed a position on the use of RPAS for non-military purposes. While it is only possible to speculate as to the reasons why some CSOs responded to the questionnaire and others did not, this may reflect a lack of interest in the subject matter, a lack of capacity (many CSOs under-resourced and are unable to fulfil every external request that they receive), or even “consultation fatigue”. As to the geographical origins of the organisations that responded, a concerted attempt was made to engage CSOs from across the EU Member States. The reasons that CSOs from northern European and English-speaking countries are overrepresented may reflect the fact that the questionnaire was published only in English. On the other hand, there tends to be more active human rights and civil liberties organisations in these countries, which were also overrepresented in the target group. Moreover, these countries – particularly Germany, the Netherlands, the UK and USA – are also places in which there have been substantial public debates and interest in development and deployment of UAS in recent years.

CSOs were asked how well they understood the technical capabilities of RPAS, their potential applications (non-military) and national and European privacy and data protection legislation. In respect to the technical capabilities, 56% of the respondents felt that they had a “good” understanding and 31% a “very good” understanding. In terms of the UAS applications, 56% felt that they had a “very good” understanding and 38% a “good” understanding. These figures are outlined in the table below (Figure 15). In respect to national privacy and data protection legislation, 65% described their understanding as “very good” and 30% as “good”. For European privacy and data protection legislation the figures were 59% “very good” and 29% “good”.

**Q3 How would you describe your organisation’s understanding of the technical capabilities of remotely piloted aircraft systems (RPAS), more commonly known as drones?**

Answered: 16 Skipped: 1

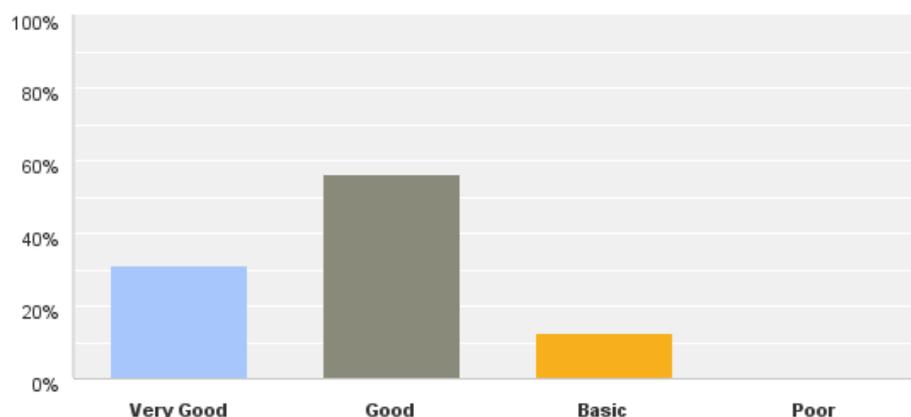
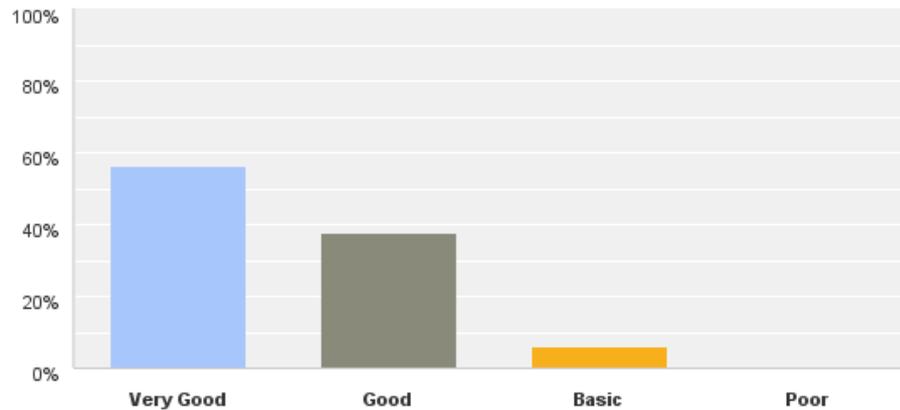


Figure 10a: CSO's understanding of RPAS technology

**Q4 How would you describe your organisation's understanding of the potential civil, non-military applications (commercial, non-commercial and government) associated with RPAS?**

Answered: 16 Skipped: 1



*Figure 10b: CSO's understanding of RPAS technology*

Just under half of the CSOs (47%) reported having undertaken an official activity relating to RPAS and privacy issues. These activities ranged from publishing reports, speaking at conferences, providing media comment and lobbying policymakers and legislators. Only three of the 17 respondents (18%) had a formal position on the civil use of UAS, and only two of these were public.<sup>1</sup> A fourth organisation was in the process of drafting such a position. A further five CSOs had published reports, briefing notes or articles highlighting concerns about the use of RPAS for law enforcement or commercial purposes. The issues raised in respect to the use of RPAS in these reports include privacy, civil liberties, data gathering and protection, police and government powers, private use, fundamental rights, the “surveillance society”, democracy, accountability, effectiveness, safety, liability, regulation and lobbying.

### 6.3.2 Privacy, data protection and ethical concerns

The concerns about RPAS expressed in the documents produced by CSOs were reflected in their responses to the survey. CSOs were asked specifically about their concerns with regard to the impact on privacy and data protection of the use of RPAS, the ethical issues raised and the risks associated with specific functionalities.

CSO respondents were asked to ascribe a level of risk (“high”, “medium”, “low” or “no risk”) to the right to privacy posed by the use of RPAS by three different user groups: law enforcement, commercial and private. Like DPAs, CSOs were asked to assess the threat to

<sup>1</sup> ‘Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft’  
ACLU: <https://www.aclu.org/files/assets/protectingprivacyfromaerialsurveillance.pdf>  
Australian privacy Foundation: <http://www.privacy.org.au/Papers/PS-Drones.html>

three different aspects of privacy: respect for home and family life, respect for communications and the right to be “let alone”. In each case CSOs perceived law enforcement use of RPAS as posing a “high” risk to the different aspects of privacy, and in each case saw them as presenting a more significant risk than commercial or private individual use. However, the majority of CSOs still identified a “medium” level of risk to home and family life and the right to be let alone by the commercial use of RPAS, and a “high” risk to these freedoms in respect to use by private individuals. The full results are shown in the Figure 16 (above).

**Q14 What level of risk do you feel is associated with the following privacy issues in relation to police or government use of RPAS for visual surveillance for LAW ENFORCEMENT?**

Answered: 14 Skipped: 3

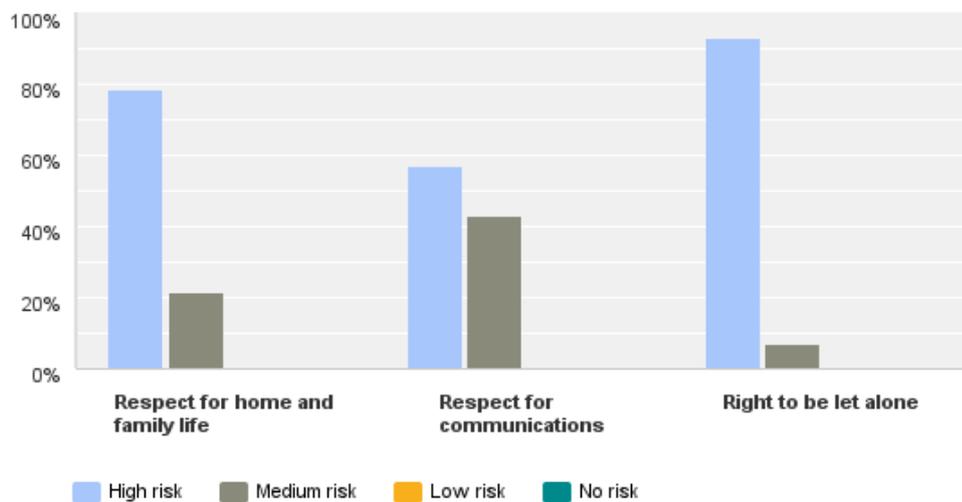


Figure 11a: CSOs and privacy assessment of RPAS applications

**Q15 What level of risk do you feel is associated with the following privacy issues in relation to commercial use of RPAS for visual surveillance for services such as INFRASTRUCTURE INSPECTION?**

Answered: 14 Skipped: 3

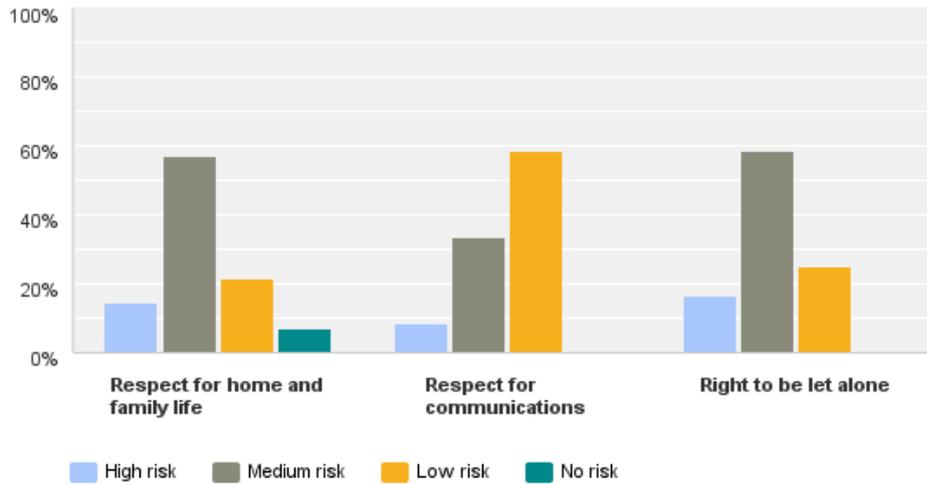


Figure 11b: CSOs and privacy assessment of RPAS applications

**Q16 What level of risk do you feel is associated with the following privacy issues in relation to PRIVATE INDIVIDUALS using RPAS with visual surveillance capabilities?**

Answered: 13 Skipped: 4

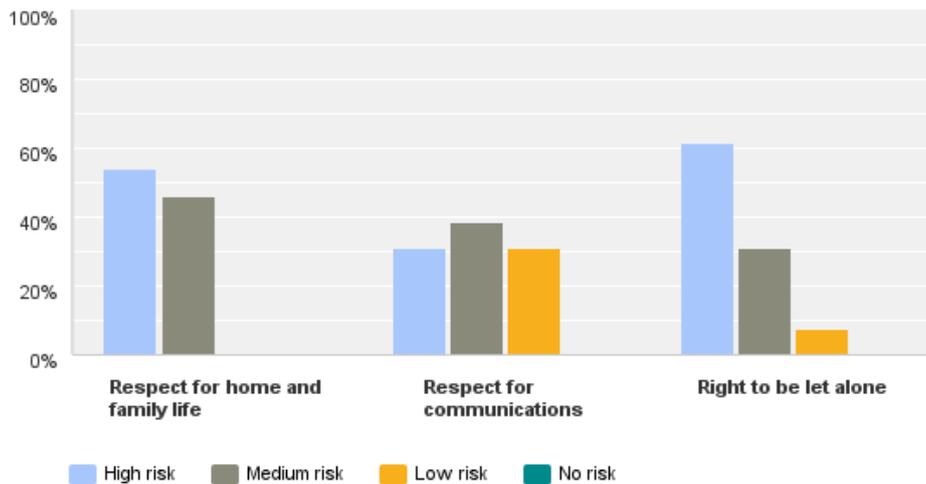


Figure 11c: CSOs and privacy assessment of RPAS applications

CSOs were also asked to ascribe a level of risk to the right to data protection posed by the use of RPAS by the three different user groups (law enforcement, commercial and private individuals). They were asked to assess the threat to the same 11 different elements of data protection as Data Protection Authorities. Overall CSOs perceive there to be substantial data protection concerns arising from the use of RPAS. Among the issues they are most concerned about are transparency, proportionality and the right of individuals to access data gathered about them. These specific data protection concerns were echoed in the CSO panel at the Computers, Privacy and Data Protection conference. The majority of CSOs perceived law enforcement use of RPAS as posing a “high” risk to almost all of the different elements of data protection (data security was the only “medium” risk). The data protection issues raising most concern among CSOs in regard to law enforcement use of RPAS are transparency, purpose limitation and consent to data collection, with 90% of respondents indicating these were highly at risk. CSOs also saw the growing use of RPAS by private individuals as posing a similarly “high” risk to data protection, though to a slightly lesser extent than by law enforcement agencies. With respect to the use of RPAS by private individuals, CSOs were most concerned about transparency, minimising the collection of personal data and individual rights to have data corrected or erased with more than 80% of respondents locating these as high risk. CSOs view commercial sector use of RPAS for surveillance purposes such as infrastructure protection as posing a “medium” to “high” risk to the different elements of data protection. In regard to the use of RPAS by commercial operators the biggest concerns were transparency, accountability and consent with at least 50% of respondents indicating these were high-risk issues.

CSOs were also asked about their perceptions of various ethical issues relating to the use of RPAS by law enforcement, the commercial sector and private individuals. They were again asked to ascribe a level of risk (“high”, “medium”, “low” or “no risk”) with respect to the following ethical issues:

- Discrimination
- Chilling effect
- Dehumanisation of the surveilled
- Public dissatisfaction
- Function creep

Overall CSOs perceive there to be a substantial risk of unethical practice arising from the use of RPAS. They reported most concern in respect to law enforcement use of RPAS, with a strong majority of CSOs worried about a “high” risk of discrimination, chilling and dehumanising effects, public alienation and “function creep”. CSOs expressed less concern about these issues in respect to the commercial use of RPAS, generally identifying a “medium” or “low” risk. Nevertheless they were still significantly concerned about “function creep”, the prospect of public dissatisfaction and a chilling effect. As one CSO representative explained in the consultation:

*Another important point is also that you don't know when someone is turning on the recording or not, if the drone has a camera or not, and if you don't know, you feel possibly being watched. The sole feeling of being watched changes your behaviour, you don't behave naturally in your own garden because you think someone is maybe watching me.*

CSOs also expressed a greater concern about the ethical use of RPAS by private individuals, though they expressed this less strongly than for the law enforcement sector. Here, they are

particularly concerned about the risk of discrimination and public dissatisfaction, both of which they ranked as “high”. The full results are shown in the following table.

**Q20 What level of risk do you feel is associated with the following ethical issues in relation to police or government use of RPAS for LAW ENFORCEMENT purposes?**

Answered: 12 Skipped: 5

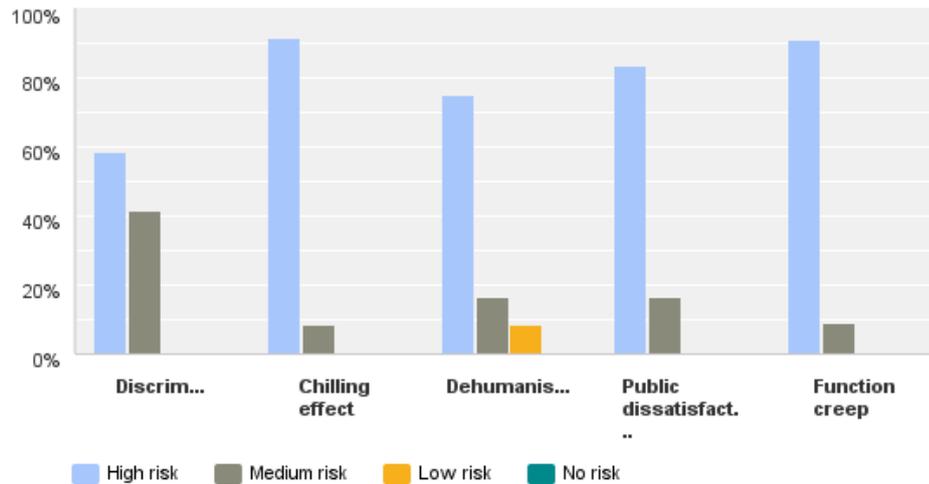


Figure 12a: CSOs and ethical risks of RPAS

**Q21 What level of risk do you feel is associated with the following ethical issues in relation to commercial use of RPAS for visual surveillance for services such as INFRASTRUCTURE INSPECTION?**

Answered: 12 Skipped: 5

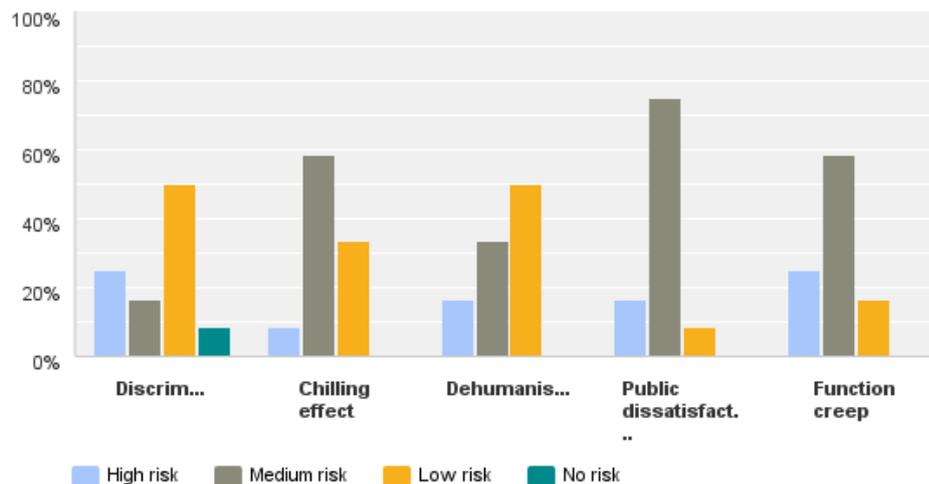


Figure 12b: CSOs and ethical risks of RPAS

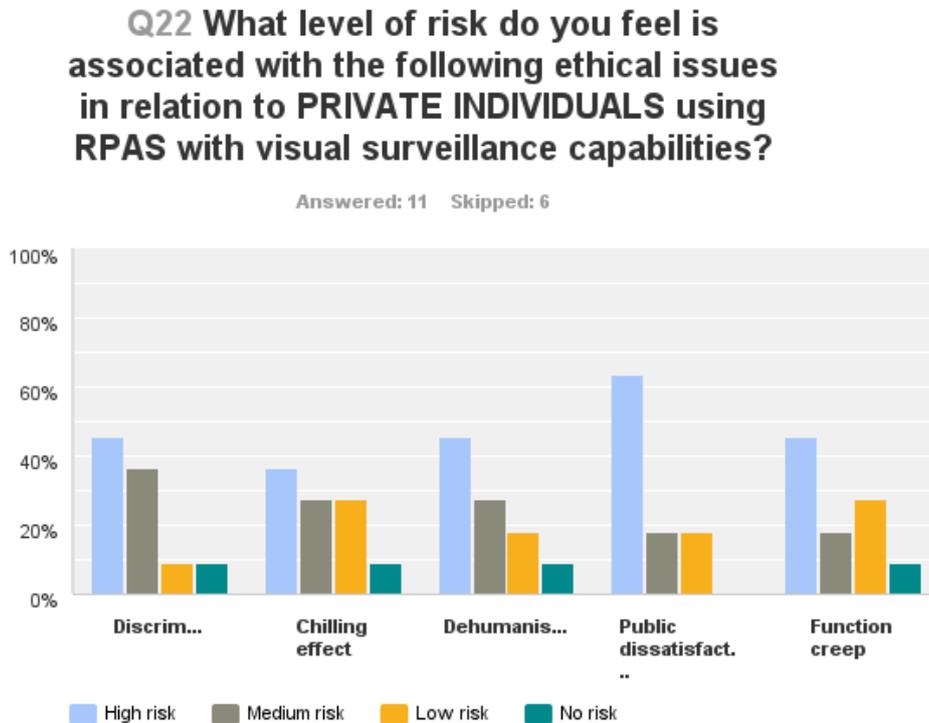


Figure 12c: CSOs and ethical risks of RPAS

Finally CSOs were asked about their perceptions of the privacy and data protection risks and ethical issues arising from three specific RPAS functionalities: thermal imaging, communications services (mobile broadband, etc.) and biometric identification, such as facial recognition. Overall CSOs perceived there to be substantial risks to privacy, data protection and ethical practice arising from each application. They reported most concern in respect to facial recognition and biometric identification technologies, which almost all (92%) saw as posing a “high” risk. CSOs also perceive significant risks in the use of thermal imaging capabilities (with more than 66% locating this as posing high-risks) and telecommunications services provided via RPAS (with the majority locating this as medium or high risk).

### 6.3.3 Consultations

Civil society organisations reported the fewest consultations with other organisations in relation to the civil deployment of RPAS. Fewer than half (35%) of the respondents have ever been consulted by their national government, local government or law enforcement agencies, industry or other civil society stakeholders about the civil use of UAS and issues of privacy and/or data protection. Of those CSOs that were consulted, they accepted the invitation to participate in every case (100%). The two CSOs based in the USA reported having been consulted by all four stakeholder groups (ACLU) and by national and local government and industry (EFF), while the Australian privacy Foundation was consulted by the Australian Parliament. By contrast, in the EU only a third the European CSOs (33%) reported any consultation on the use or development of RPAS: a civil society meeting in Germany, a

government policy consultation in the UK and a single EU consultation. Despite the relatively small sample this suggests that consultation has been more extensive to date in the USA than the EU. None of the CSOs in the survey reported any contact with national privacy or data protection authorities whether in the form of consultation by those authorities or contact initiated by the organisations themselves. Half of the respondents (50%) indicated that they would like to be consulted further should the European Commission chose to follow-up on this study.

In conclusion, while the survey was relatively small in terms of the number of respondents, it nevertheless provides some strong insights into how they civil society organisations perceive the development of RPAS and the specific concerns that they have. Six thematic conclusions are particularly relevant to the current deliberations by the European Commission and other stakeholders. First, the survey shows that CSOs consider themselves to be well or very well informed about the development of RPAS and their intersection with issues of privacy, data protection and ethical practice. The survey also showed that CSOs have both a wish and willingness to be consulted about these issues and suggests that consultation in Europe appears to lag well behind that undertaken in the USA. That there appears to have been little or no dialogue between CSOs and data protection authorities on relevant issues also suggests that more systematic consultation is necessary. Second, the survey clearly demonstrated that CSOs are playing an active role in fostering public debate about the development of RPAS through their publications, outreach, media and lobbying work. Third, CSOs are most worried about the use of RPAS by law enforcement agencies, though they still harbour significant concerns in respect to commercial RPAS applications and their use by private individuals. Fourth, CSOs perceive a substantial risk to the right to privacy from the use of RPAS, including a medium risk to privacy in telecommunications and a medium to high risk to civil liberties as expressed in terms of the “right to be let alone”. Fifth, CSOs perceive an acute threat to most elements of data protection from the use of RPAS. They are most concerned about the transparency of RPAS operations, consent to data gathering by RPAS, the proportionate use of RPAS, minimisation of the data gathered and individual rights to access data and have it corrected or deleted. Sixth, CSOs are also worried about the risk of discrimination against certain groups by RPAS operators and are concerned about growing public dissatisfaction. Seventh, it is suggested that different applications pose different levels of risk in terms of ethics, privacy and data protection and that the perceived risk with regard to applications such as biometric identification and thermal imaging are particularly acute. All of this underscores the need to ensure that civil RPAS are introduced and regulated with maximum regard to ameliorating these concerns and that such regulation needs to be discussed with a broad range of experts, including civil society organisations.

## **6.4 Civil Aviation Authority analysis**

### *6.4.1 Overview*

Of the four stakeholder groups targeted, this survey was least successful in generating responses, despite researchers undertaking three different follow-up contacts, including phone calls to specific CAA offices. Unlike other organisations contacted, one clear stumbling block was language skills, where CAA representatives seemed less able to complete the survey in English than other stakeholder groups. Despite this, the survey did generate eleven responses from eight different CAAs in Europe, including responses from Belgium, Ireland, Italy, Latvia, Luxembourg, Portugal, Sweden and the UK. All but one of the CAAs (91%) who answered the survey characterised their understanding of the technological capabilities and

the potential civil applications of RPAS as “good” or “very good”. They survey also generated significant interest from CAAs who are involved in drafting rules for the use of RPAS for civil applications, with 82% of the respondents reporting that their office has an official position on the civil RPAS. Finally, 10 of the 11 respondents (91%) also indicated that civil users of RPAS had to obtain authorisation from their office before flying RPAS. In the section that follows we examine exactly what these regulations entail.

#### 6.4.2 RPAS regulations

CAAs regulated a number of aspects of RPAS flights within their air space. Specifically, the CAA regulators who responded to the survey reported that they regulate the following aspects of RPAS operations:

#### Which types of authorisations do you issue? (please tick all that apply)

Answer choices	
Authorisation of particular flight A, with RPAS X, with controller Y and operator Z	73%
Licensing of the RPAS operator	55%
Certification and/or licensing of the remote pilot aka RPAS controller	45%
Airworthiness certification of the RPAS (compliance with safety and operational standards, etc.)	36%
None of the above	9%

*Table 4: CAA RPAS authorisations*

The table above indicates that very specific authorisations are the type most frequently granted by CAAs who do regulate the use of civil RPAS. This indicates that the flight area and path, the device and the operator and controller are all often examined in the course of providing authorisation. Furthermore, although these are likely focused on safety issues, the fact that the CAAs frequently license RPAS pilots and/or certify RPAS operators, means that they might be well positioned to include additional, privacy or data protection elements in their consideration of RPAS flights, pilots, controllers or operators.

This is further supported by the information below, which indicates that RPAS flights, operators and applications are regulated by the majority of CAAs who responded to the questionnaire. While the payloads that they carry are currently not frequently regulated, the fact that CAAs often examine the specificities of the flight (as indicated by Table 3 above) means that it may be possible to encourage CAAs to consider the payloads and the purpose of the mission alongside the airworthiness aspects of the flight and device. This is particularly important, as all of the following payloads are currently allowable under the majority of CAAs’ current regulatory regimes: Photographic cameras, thermal imaging cameras, environmental sensors, communication equipment and geo-location equipment. Significantly, many of these payloads were of particular concern and thought to carry significant risks to privacy, data protection and ethics by most DPAs and CSOs (as indicated in the sections above). Furthermore, the applications of RPAS currently allowable under CAAs who answered the survey included the following:

- Critical infrastructure surveying (100%)
- Agriculture (100%)
- Environmental monitoring (100%)
- Civil protection (e.g., Fire brigade) (91%)
- Media and broadcasting (91%)
- Law enforcement (82%)
- Communications (73%)
- Private security (64%)

Again, these areas of application are particularly significant as they include key areas where data protection authorities have significant concerns.

### Q8 Which of the following do you regulate? (please tick all that apply)

Answered: 11 Skipped: 0

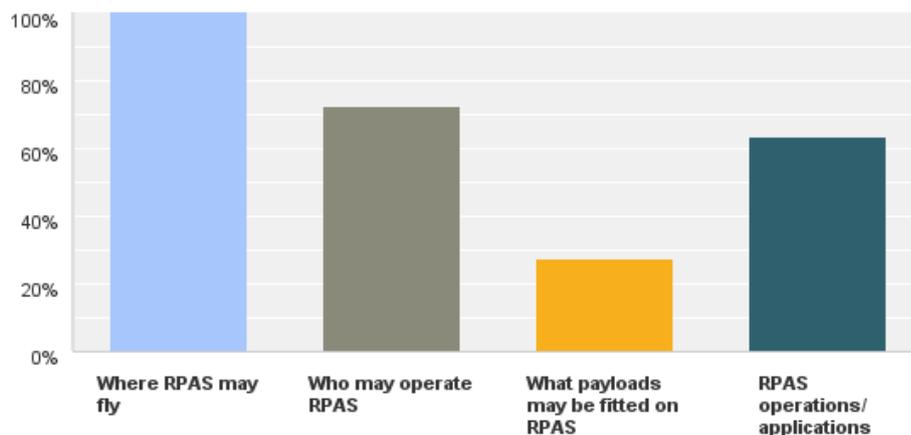


Figure 13: CAA regulatory operations

However, unlike the payloads and applications the survey indicates that currently RPAS operators are quite limited in where they can fly. Six of the ten respondents to this question indicated that RPAS could only fly in designated areas, and that RPAS may not fly in populated areas. While four respondents indicated that some RPAS may fly over populated areas, seven indicated the RPAS could not fly over people or animals – significantly limiting their areas of operation and their resulting privacy, data protection and ethical impacts. Finally, only two of the CAAs who responded to the questionnaire required operators to certify that they have considered the privacy or data protection issues associated with their operation of RPAS.

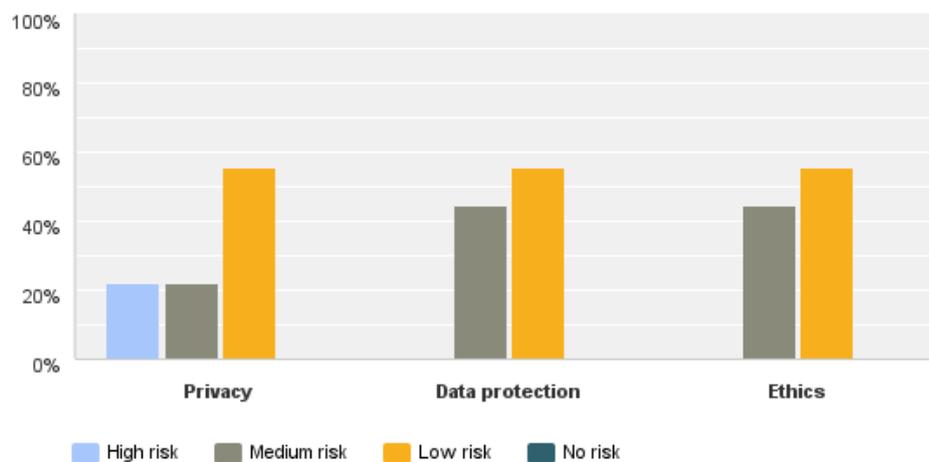
#### 6.4.3 CAA perspectives on privacy and data protection

Despite the lack of a traditional relationship between air transportation and privacy and data protection, the CAAs that responded to the survey reported a relatively good level of knowledge about privacy and data protection legislation and reported that they felt that RPAS did raise significant potential risks to privacy and data protection. However, the risks they reported were reduced in comparison to DPAs and CSOs.

CAAs reported a relatively good level of knowledge about privacy and data protection legislation. Specifically, half of the CAAs who answered questions about privacy and data protection reported a “good” or “very good” level of knowledge about European privacy and data protection legislation. Similarly, slightly more than half (55% of respondents) reported a “good” or “very good” understanding of their national privacy and data protection legislation. However, the results of this survey on the privacy and data protection issues associated with RPAS are based on responses from a sub-set of CAAs. Only 11 of the 28 European Member State CAAs responded to the questionnaire. While some may have been prevented from responding based on language issues, it is also likely that the CAAs with an interest in privacy and data protection were more sympathetic to the topic of the survey and more likely to respond.

**Q20 What level of risk do you feel is associated with the following issues in relation to police or government use of RPAS for visual surveillance for LAW ENFORCEMENT purposes?**

Answered: 9 Skipped: 2



*Figure 14a: CAA risk assessment of RPAS*

**Q21 What level of risk do you feel is associated with the following issues in relation to commercial use of RPAS for visual surveillance for services such as INFRASTRUCTURE INSPECTION?**

Answered: 9 Skipped: 2

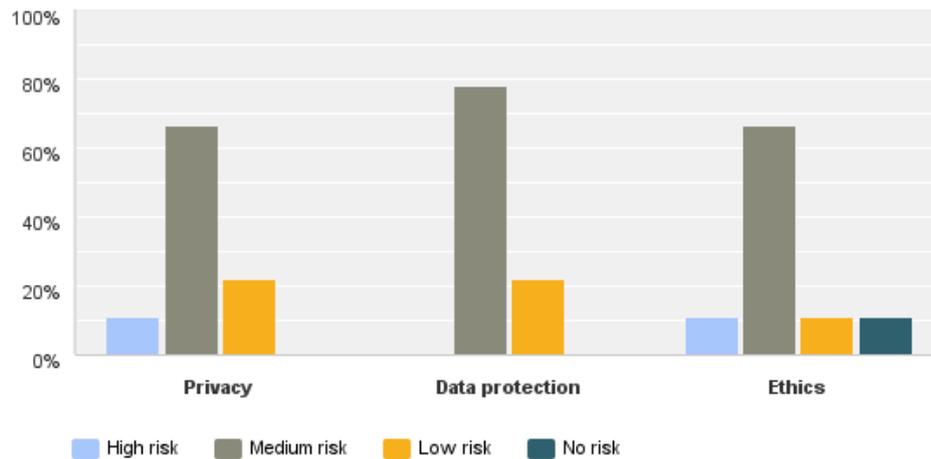


Figure 14b: CAA risk assessment of RPAS

**Q22 What level of risk do you feel is associated with the following issues in relation to PRIVATE INDIVIDUALS using RPAS with visual surveillance capabilities?**

Answered: 9 Skipped: 2

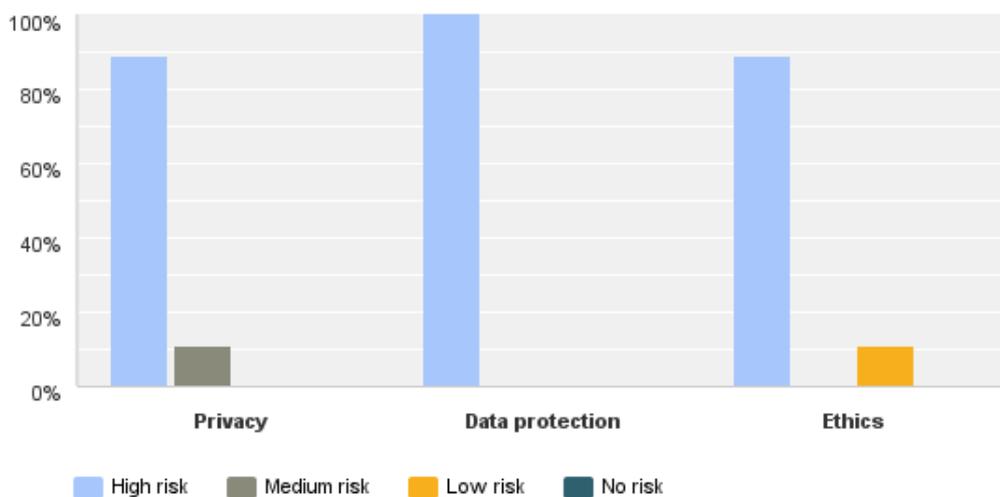


Figure 14c: CAA risk assessment of RPAS

Nevertheless, these CAA responses indicated that they viewed the use of RPAS as having some risks to privacy, data protection and ethics. In relation to the use of RPAS for visual surveillance purposes, CAAs were more likely to view individual use as more risky than law enforcement use or commercial use. While individual use is reported as being largely high-risk, commercial use was viewed as medium-risk and police use was viewed as low risk. This is particularly significant given the findings from other respondent organisations (e.g., DPAs) that located police as one of the most risky users of RPAS.

CAA respondents were also less likely than other groups to view the potential, future applications of RPAS as carrying high risks to privacy, data protection or ethics. These respondents all agreed that there were some risks associated with the use of RPAS with thermal imaging capabilities, with the capability to provide broadband communication links and with biometric capabilities. However, they viewed these risks as comparatively lower than other organisations. For example, with respect to thermal imaging, CAA respondents were far more likely to locate this as a medium risk (56%) or low risk (33%) capability. In relation to broadband communication, CAA respondents were most likely to view this as a low risk capability than other groups, with only 56% viewing it as a high risk or medium risk capability. Finally, in line with other groups, CAAs also agreed that the use of biometric capabilities in RPAS would carry the highest risks to privacy, data protection and ethics, with all respondents indicating that this carried high-risks or medium-risks.

However, despite these recognised risks, only four of the CAAs who responded to the survey indicated that their organisation had an official position on the privacy and data protection impacts of RPAS.

#### 6.4.4 Consultations and advice to RPAS users

Civil Aviation Authorities were the group that reported being the most likely to participate in consultations on civil RPAS, with nine of the eleven respondents reporting such involvement. These consultations largely took place with industry representatives (eight of nine respondents) and European, national and local government representatives (including law enforcement agencies and border patrol) (five of nine, four of nine and four of nine respectively). Finally, a few CAAs reported that they also participated in consultations with civil society organisations (four of nine) and data protection authorities (two of nine). In addition to these consultations, 70% of CAAs who answered this question indicated that they had been in contact with their national Data Protection Authority about these issues. This is particularly significant as it seems that the CAAs are willing to participate in consultations regarding RPAS, but these consultations appear to have been focused on their existing relationships with industry and government, rather than unfamiliar organisations such as CSOs and DPAs.

While some CAAs were clear that privacy and data protection issues fall outside their competence, a few CAAs (six) had taken some action with respect to privacy and data protection. Three of the respondents have provided advice for RPAS users and/or alerted them that their activities fall inside the scope of current data protection regulations. The UK CAA, in particular, reported that they have included the relevant information on their permission documents and their website:

*Basic details on requirements of data protection legislation are included on every small UAS permission that is awarded. "Careful note should be taken that the*

*collection of images of identifiable individuals, even inadvertently, when using surveillance cameras mounted on a small unmanned surveillance aircraft, will be subject to the Data Protection Act. As this Act contains requirements concerning the collection, storage and use of such images, Small Unmanned Aircraft operators should ensure that they are complying with any such applicable requirements or exemptions. Further information about the Data Protection Act and the circumstances in which it applies can be obtained from the Information Commissioner's Office and website: [www.ico.org.uk](http://www.ico.org.uk)". This information is also on the CAA website UAS pages.*

Here RPAS operators are specifically alerted to their obligations under the UK Data Protection Act, but the onus is on them to comply with this legislation. In other contexts, however, RPAS operators are subject to separate checking to ensure that they comply with privacy or data protection legislation. The Swedish CAA reported that "In order to take photos or record film you must have a separate approval from the military defense authorities", and the Latvian CAA reports that they have a separate Data inspection authority that deals with the privacy and data protection aspects of RPAS. However, despite this relatively significant interest in privacy and data protection issues, only four of the eleven respondents indicated that their organisation offers RPAS operators advice on privacy and data protection issues. Thus, there seems to be a clear gap in competence or authority in relation to these issues, rather than a gap in interest. This is particularly significant as the Czech CAA noted "privacy protection is probably not solved adequately. It is very hard to indicate the RPAS operator and to sue him after the problematic flight is made." Finally, despite this relatively high level of interest in or recognition of the privacy and data protection impacts of civil RPAS, all of the eight CAA respondents who answered this question of the survey indicated that they felt that their organisation did not have enough competence to evaluate privacy and data protection issues alongside their other responsibilities. As a UK CAA respondent noted, "the safe operation of [RPAS] is of a much greater concern to us at the moment."

In conclusion, despite CAAs' relatively central role within the RPAS regulatory landscape and their high level of understanding of privacy and data protection issues as well as their relatively strong recognition of the significance of these issues, CAAs seem relatively unwilling to take on additional regulatory responsibilities related to privacy and data protection. Instead, CAAs are willing to link with DPAs and to provide advice about privacy and data protection issues on their public information portals. It is possible that this relationship can be further exploited to assist RPAS users in complying with relevant legislation.

## **6.5 Summary and conclusions**

Although these consultation exercises were subject to a number of limitations, the results point to some interesting areas of commonality and divergence relation to the four stakeholder groups. First, both exercises were exploratory in nature, and not intended to be representative. The survey was intended to be as representative as possible, but language limitations, lack of a well-defined sample population and /or the short time frame of the survey all resulted in a sample of individuals who were not necessarily representative of the overall populations of interest to the research. Furthermore, participation in these exercises was also likely limited by people's expertise in relation to the intersecting issues of privacy, data protection and RPAS technologies. Those with expertise in privacy and data protection, may not have

adequate expertise in RPAS technologies and vice-versa. This was largely played out in the survey responses of industry representatives in particular, who reported good or basic knowledge of privacy and data protection issues. However, privacy and data protection experts were more likely to report good or very good knowledge of RPAS technology than their industry counterparts were to report good knowledge outside their main area of expertise. Relatedly, the relative “newness” of RPAS technology and the number of consultation activities associated with this new and emerging area may also have resulted in some “consultation fatigue” for those with expertise in all of these areas.

Despite these limitations, the consultations did reveal some important findings. First, commercial use of RPAS, particularly for the inspection of critical infrastructure seems to be the user/application combination that is viewed as carrying the fewest and least intense privacy, data protection and ethical risks. This is played out in relation to DPA, CSO and CAA opinions about these risks as well as the information gathered from industry representatives. In contrast, police uses of RPAS for visual surveillance and the use of RPAS for visual surveillance by private individuals were thought to carry the highest risk (although CAA respondents viewed police uses as relatively low-risk). However, these two groups are also subject to the fewest regulations surrounding RPAS usage as both of these groups are largely exempted from privacy and data protection legislation (as described in Chapter 5).

With regard to privacy, different stakeholders largely agreed that respect for home and family life and the right to be let alone were most likely to be threatened by the use of RPAS for visual surveillance. They also located the following data protection issues as being most likely to be impacted by RPAS: transparency, data minimisation, proportionality, purpose limitation, consent and rights of access. Again, law enforcement and private individuals emerged as the highest risk RPAS users, with risks emanating from commercial organisation less high, but still significant. In relation to ethical issues, public dissatisfaction and function creep were most likely to be identified as high risk issues, although DPA respondents were fairly consistent in rating all of these issues as significantly risky. Finally, while the use of biometric identification capabilities in RPAS is somewhat far off, many industry representatives and CAAs located the potential use of RPAS for communication services and/or thermal imaging applications as desirable and/or allowable in the near future. The relative proximity of these potential future applications is especially significant given that most organisations that were asked to rate the potential privacy, data protection and ethical impacts associated with RPAS rated these applications as being either high risk or medium risk.

With respect to consultations, many of the respondents who participated in this consultation reported actively participating in others as well. While this likely a somewhat self-selecting group, the overall responses indicate that much discussion is happening between industry representatives, policy-makers and regulators at the national level and the European level. Civil society organisations were least likely to report having participated in consultation exercises with industry or policy-makers. Significantly a number of DPAs and CAAs appear to be in contact, and have provided links to one another’s materials on their websites or in their position papers, which could lead to fruitful collaboration at the national level.

Another indication that the potential privacy and data protection impacts of the use of RPAS for civil applications is being considered is the use of impact assessment mechanisms by a number of RPAS industry representatives. While RPAS operators were more likely to use such instruments than RPAS designers and manufacturers, instruments such as codes of conduct, risk assessment and privacy impact assessment were relatively popular and could be encouraged or mandated as good practice more widely. Nevertheless, a significant amount of

education for RPAS industry is needed, as many RPAS industry representatives indicated that their use of RPAS did not generate any privacy or data protection issues, but that the RPAS captured members of the public, recorded the images and stored the images. This means that the RPAS was collecting personal information through visual surveillance, and that the RPAS users were likely subject to many elements of applicable data protection legislation.

In relation to the competence of Civil Aviation Authorities with respect to addressing privacy and data protection impacts, most stakeholders agreed that the primary focus of CAAs was safety rather than privacy or data protection. However, the results of the survey indicated that many CAAs were undertaking very detailed authorisations, including examining the flight, the operator, the application and the RPAS itself. Furthermore, they act as an agreed and familiar gatekeeper in relation to the civil use of RPAS. Should the European Commission mandate a roll-out of instrument such as privacy impact assessments or codes of conduct, CAAs may be an appropriate authority to certify that such a consideration has been taken place, and to refer any suspect or complex usages of RPAS to their counterpart Data Protection Authority.

## 7 RPAS CAPABILITIES AND APPLICATIONS

### 7.1 Introduction

Although it is widely assumed that RPAS are a quintessentially modern technology, their development can be traced all the way back to the late nineteenth century and the hydrogen-filled airships controlled by spark-emitting radio signals that were flown around theatre auditoriums to entertain music hall crowds. Subsequent attempts to create a “flying bomb” inspired by World War I produced the first remotely piloted aircraft flight – a modified “N9” U.S. Navy seaplane – in 1918.<sup>1</sup> For the next 75 years or so RPAS remained largely the preserve of the defence sector, which continued to develop the technology for missile guidance, target practice and surveillance purposes, and hobbyists and their suppliers, who developed the technology for the love of flight. The idea that RPAS could ultimately perform many if not all of the tasks currently performed by on-board-piloted aircraft gained currency in the 1990s and in particular after the NATO intervention in Kosovo, when UAS were used for real-time surveillance and target acquisition in the former Yugoslavia.<sup>2</sup> Today there are hundreds of different models and thousands of organisations engaged in their design, manufacture and use. According to UVS International, by 2011 the production of more than 400 different UAS was spread across at least 21 EU countries.<sup>3</sup>

This examination of civil applications is the first systematic attempt to outline the capabilities of RPAS, the payloads they may carry and the contexts in which they operate. It is based on an examination of research reports, academic journal articles and other publications, mass media materials, industry websites, policy documents and materials from civil society organisations. However, it is important to note that the RPAS sector is a quickly evolving industry, and due to its dynamic nature, this taxonomy may be quickly out-dated as miniaturisation of RPAS and payloads, technological development and the identification of novel applications continue.

The recent development of RPAS owes as much to the rapid expansion of computational power, digital imaging and data transmission capabilities as advances in aeronautical technology. Real-time video streaming is a standard feature of beyond the line of sight RPAS, enabling pilots and controllers to fly the aircraft using a “first person view” of live images streamed to the ground station. Many models carry additional surveillance equipment to provide operators with aerial imagery, geospatial analysis and other types of data that can be captured using dedicated on-board equipment. This is why many RPAS raise so many data protection concerns, even when operated by private actors for purposes other than “surveillance”. In the sub-sections that follow, we provide more information about the potential capabilities and applications of civil RPAS. Given the distinct privacy and data protection legal framework within which different categories of RPAS operators (commercial, law enforcement, telecommunication providers, journalists and private individuals) are situated, the organisation of this section follows the different contexts and applications for

---

<sup>1</sup> See further the account of the historical development of unmanned aircraft systems in John Villasenor, “Observations From Above: Unmanned Aircraft Systems and Privacy”, *Harvard Journal of Law and Public Policy*, Vol. 36, No. 2, 2013, pp. 462-464.

<sup>2</sup> European Advisory Group on Aerospace, “STAR 21: Strategic Aerospace Review for the 21st Century”, Brussels, 2002.

<sup>3</sup> Van Blyenburgh, Peter, “UAS Industry and Market Issues”, *European Commission UAS Panel, 1st Workshop*, 12 July 2011.

which different operators may use RPAS. It examines the missions that RPAS may accomplish in these contexts, the equipment that may be used and the types of data that may be collected. Where it is possible to collect personal data during these missions (either intentionally or unintentionally), the discussion concludes with a likely mission scenario that demonstrates the types of data that may be collected as well as the potential impacts on individuals.

This chapter provides an overview of the different types of remotely piloted aircraft systems (RPAS) that are currently in use or under development and which may one day be operated within the European Union. The purpose of this is to gain an understanding of how RPAS are being used, what payloads they may carry and what contexts they are operating within, in order to provide a foundation for examining the privacy, data protection and ethical issues they may raise. This chapter is organised by the types of operators that may use RPAS, and for each examines typical missions including the payloads associated with those missions, the target of the mission and the types of data that may be collected. Where the RPAS mission may include the collection of personal data, each sub-section concludes with a specific, typical RPAS scenario that will be used to analyse the privacy, data protection and ethical issues in Chapter 8.

## 7.2 Commercial operators

Commercial operators are the stakeholder that are currently driving the push to utilise RPAS for civil applications, primarily because of the benefits, jobs and economic growth expected to be generated by the proliferation of RPAS in Europe. Furthermore, they are a key stakeholder group in terms of RPAS operators, as they are subject to the full privacy and data protection legal framework outlined in Chapters 4 and 5. The information presented in this sub-section is based on literature review, as well as information from the stakeholder consultation exercises described in Chapter 6.

### 7.2.1 Infrastructure inspection

As identified in the survey of RPAS manufacturers and operators, the inspection of infrastructure is the most popular mission associated with commercial use of RPAS. The target of these operations is the inspection of objects, particularly for missions such as oil and gas pipeline monitoring, the inspection of mobile phone towers, bridges and wind turbines, nuclear installation inspections and industrial sites. Specifically, oil refineries, chemical plants, nuclear plants, electricity plants, dams, pipelines and renewable energy may all one day employ RPAS for monitoring and safety purposes.<sup>4</sup> Many of these infrastructural sites are in difficult to reach or rural areas, which often necessitates the use of RPAS in order to provide safety for human inspectors and enable the inspection to occur efficiently. While commercial organisations are the primary operators of such missions, in some cases government bodies may carry out these inspections or monitoring activities. The inspection and monitoring of these sites is primarily visual, whereby information is recorded about the object to be inspected via high-resolution video and still image capture using high-definition cameras. One of the key benefits of such high-definition images is the ability to undertake post-collection processing of the data in question – e.g., to zoom in on specific areas of

---

<sup>4</sup> Snider, Annie, “Drones fly into nascent civilian market ripe with energy, environmental applications”, *E&E Publishing*, 25 February 2012. <http://www.eenews.net/stories/1059958938>

interest, return to particular segments of footage and compare images across inspections.<sup>5</sup> Such inspections may also include thermal images, particularly to identify “hot spots” along power lines or power sub-stations.<sup>6</sup> While the inspection is focused on the object in question, visual images of workers at the site, of individuals in nearby residential areas<sup>7</sup>, of cars and other objects, such as vehicles, that could be linked with particular individuals may be captured on the footage inadvertently. Furthermore, the benefits of such high-resolution images may allow for the zooming in on and identification of these individuals and objects<sup>8</sup>, especially using contextual information, such as particular landmarks, or by combining this information with other available data sources (e.g., property deeds and titles, motor vehicle records, etc.).

Operator(s)	Mission	Target	Examples	Equipment	Data collected
Commercial /government (institutional)	Infrastructure inspection	Objects	Inspection of mobile phone towers, bridges, power lines, wind turbines, nuclear and industrial installations	High resolution video and still cameras, thermal cameras	Photographs and video images of the infrastructure, personal data may be collected inadvertently

A typical scenario for such infrastructure inspections is the following:

*An RPAS operator is charged with inspecting a mobile phone tower in a rural location that provides mobile phone coverage to a few homes in the area and drivers on the near-by highway. The RPAS is fitted with a high-definition video camera, which the operator tests by scanning the landscape and taking a few close-up images of the base of the tower. Satisfied that the images are of sufficient quality for later analysis and can be enhanced to provide close-up footage of cracks or damage, the operator begins his inspection. As the RPAS ascends into the air, the operator circles the mast, moving steadily upwards. The video footage is focused on the mast, but the landscape behind the mast is visible in the shot as he makes his way around the mast and higher into the air. Although the operator and the mobile phone provider are not interested in the farms or vehicles in the background, (often blurry) images of these are captured and included in the footage provided to the mobile phone company and saved in the RPAS operator’s archives.*

---

<sup>5</sup> Haala, Norbert, “Photogrammetry & RPAS”, *Remotely piloted aircraft systems: Civil operations*, Brussels, 9-11 December 2013.

<sup>6</sup> Barnard Microsystems, “Thermal imaging applications”, 2013.  
[http://www.barnardmicrosystems.com/UAV/features/thermal\\_imaging.html](http://www.barnardmicrosystems.com/UAV/features/thermal_imaging.html)

<sup>7</sup> Sky Photo, “Cell tower aerial photos: Infrastructure inspection”, 6 November 2012.

<http://www.skyphoto.com/tower-aerial-industrial-photography-and-inspection/>

<sup>8</sup> Sky Photo, “Imaging”, 2014. <http://www.skyphoto.com/imaging/>

### 7.2.2 Other visual services

In addition to these inspection services, RPAS that utilise optical imaging payloads, including high-resolution video and still cameras may also be used for other visual services outside of inspection. These may include visual services such as capturing footage for sales or publicity purposes<sup>9</sup>, image capture for commercial stock footage<sup>10</sup>, as well as others. While the equipment utilised by RPAS manufacturers and operators for these services are similar to infrastructure inspection, the key difference is the sometimes unavoidable presence of people in the footage that results from these services.

Typical scenarios for such visual services include the following:

*An RPAS operator is contracted by a real estate company to make a video showcasing a home for sale. The operator flies about 200m above the house, filming the building, the land included with the sale and the immediate surrounding neighbourhood. The left neighbour's car and toys in their back yard are clearly visible, as is the right-side neighbour walking from her front door to her car. The RPAS operator saves a copy of the video and transfers the second copy to the real estate client.*

*The organisers of an outdoor concert have contracted a drone operator to fly above the concert taking footage of people in the crowd enjoying themselves. Attendees of the event were informed of the filming via a short notification in the terms and conditions statement when they bought their tickets online.*

*A commercial RPAS operator flies high over a historical city taking footage of various landmarks. The footage focuses in on the ruins of a castle, a park and the picturesque marina. Because of the height of the RPAS, the images of the people on film appear to be unidentifiable. The RPAS operator sells the image to a stock image database/catalogue, where it is stored indefinitely and made available for purchase by other entities.*

### 7.2.3 Mapping

In addition to close inspection, RPAS are capable of monitoring and collecting information about wider areas, which makes them useful for geo-spatial mapping. Due to a combination of the height at which they fly and the resolution of the cameras they carry, higher altitude RPAS are particularly useful for wide-area mapping. Their mobility also gives them a great advantage over satellites in lower orbits that can acquire very detailed images but not on a continuous basis.<sup>11</sup> Some high altitude drones can also be fitted with daytime and infrared cameras and synthetic aperture radar capable of providing photographic-like images through clouds, rain or fog, and in daytime or night-time conditions.<sup>12</sup> At much lower altitudes even

---

<sup>9</sup> Drones iView “Drones iView – Sample Real Estate video”, YouTube, 5 October 2013. <https://www.youtube.com/watch?v=RXWy1il6CGA&list=PL9EWGetnOtH5fqPkb8TX05UHm-6Cj16k> and <https://www.youtube.com/watch?v=gDI muzArIZU>

<sup>10</sup> YouFlyTube, “YouFlyTube”, 2014. <http://youflytube.com>

<sup>11</sup> See further Villasenor, op. cit., 2013, p. 495.

<sup>12</sup> Barnard Microsystems, “Synthetic Aperture RADAR”, 2013. [http://www.barnardmicrosystems.com/UAV/features/synthetic\\_aperture\\_radar.html](http://www.barnardmicrosystems.com/UAV/features/synthetic_aperture_radar.html)

small, hand-launched RPAS can cover relatively large areas.<sup>13</sup> RPAS payloads may also include photogrammetric equipment that promises faster and cheaper 3D-imaging (digital elevations and surface maps, etc.) than traditional LiDAR remote sensing techniques.<sup>14</sup> These applications appear particularly promising from a commercial point of view, with a growing number of dedicated providers – for example Isis Geomatics, Orbit GeoSpatial Technologies and Swissdrones – offering a geospatial analytics and geographical information service using small and light RPAS.

These uses of RPAS may also include missions related to construction planning, mining and geographical surveying. RPAS may be used to assist in mapping the path of a new road<sup>15</sup> or the layout of a new housing estate. The aircraft can be employed in aspects of oil, gas and mineral exploration requiring aerial reconnaissance and geographical surveying. In the event of crises such as earthquakes, landslides, flooding RPAS may be used to identify affected areas and/or changes in the landscape. For man-made disasters like the discharge of hazardous materials, e.g., oil spills, RPAS missions may include the mapping of contamination or the spread of pollutants. The data collected via these missions includes landscape, foliage and buildings.

As there is little likelihood of collecting personal data during these missions, no associated scenario is included in this sub-section. However, some mapping operations – e.g., mapping for an underground network – may collect images of residential or commercial properties in the area. The privacy and data protection issues associated with these collections are similar to those examined in section 7.2.2 above, and so are not discussed separately here. Furthermore, the proliferation of RPAS and the fact that people on the ground may not be aware of the purpose for which it is being used does raise privacy and transparency issues. It is important for people to be able to access this information if they are interested in doing so.

Operator(s)	Mission	Target	Examples	Equipment	Data collected
Commercial /government (institutional)	Geo-spatial mapping	Objects, landscape, foliage	Mapping and surveying for exploration, planning and crisis management	High resolution cameras, infrared cameras, synthetic aperture radar, photogram-metric equipment	Images of the objects or spaces targeted, personal data unlikely to be collected.

---

<sup>13</sup> Claussen, Johanna, “MAVinci's next generation aerial image UAS: From flight planning to professional orthofoto and DEM”, *DIY Drones*, 18 April 2011.  
[http://diydrone.com/profiles/blog/show?id=705844%3ABlogPost%3A339917&commentId=705844%3AComment%3A342268&xg\\_source=activity](http://diydrone.com/profiles/blog/show?id=705844%3ABlogPost%3A339917&commentId=705844%3AComment%3A342268&xg_source=activity)

<sup>14</sup> LiDAR is a remote sensing technology that measures distance by illuminating a target with a laser and analysing the reflected light.

<sup>15</sup> Orbit, “Orbit UAS mapping”, *Orbit Geospatial Technologies*, 2014.  
<http://www.orbitgis.com/store/product/orbit-uas-mapping>

#### 7.2.4 Earth observation

Earth observation and remote sensing currently carried out using imagery provided by satellites or samples collected by conventional aircraft will also be enhanced by the availability of low-cost RPAS. Much of the data used to monitor climate change and atmospheric pollution or to produce environmental impact assessments may be collected more efficiently using unmanned systems. Environmental organisations and governments are already using unmanned systems to protect green space, track wildlife and prevent soil erosion.<sup>16</sup> These systems are particularly useful for covering large areas of land, particularly when ground operations are difficult or dangerous. Archaeology, geology, meteorology, oceanography and seismology are among the sectors that could benefit from the use of RPAS for the purposes of earth observation.

The use of RPAS equipped with sampling and detection technologies by the commercial and public sectors is likely to grow significantly where they provide a safer or more cost-effective way of gathering samples in places that are difficult or dangerous to reach. RPAS can be mounted with biological sensors capable of detecting the airborne presence of various microorganisms and chemical sensors that use laser spectroscopy to analyse the concentrations of airborne elements.<sup>17</sup> In Japan RPAS are being used to prevent crews being exposed to harmful levels of radiation at the Fukushima Daiichi nuclear plant which was damaged by an earthquake and tsunami in March 2011.<sup>18</sup> Information from these chemical and biological sensors, such as the ones being used in Japan, may be combined with location data and visual images to link readings to particular locations. In the future, RPAS may also be able to manipulate the environment, for example in China one company is testing a “smog clearing drone” in an attempt to tackle the chronic air pollution in that country.<sup>19</sup>

As stated above, there is little likelihood of collecting personal data during these missions, and no associated scenario is included in this sub-section. Despite this, like mapping, the use of RPAS for earth observation, especially in inhabited areas for purposes such as pollution monitoring, contributes to a potential that people on the ground may feel discomfort with the number of RPAS in operation and may be unsure where to go to find out more information about specific RPAS operations. Furthermore, in relation to safety, the use of RPAS for some monitoring activities may disturb or pose risks to animals and plant life, particularly in protected areas.

---

<sup>16</sup> AUVSI “The Benefits of Unmanned Aircraft Systems: Saving Time, Saving Money, Saving Lives”, *Association for Unmanned Vehicle Systems International (AUVSI)*, no date. <http://epic.org/events/UAS-Uses-Saving-Time-Saving-Money-Saving-Lives.pdf>

<sup>17</sup> Omara, David, “Deploying Ruggedized Systems in Unmanned Military Vehicles for Advanced Air-Sea-Land Applications”, *Kontron Whitepaper*, no date.

[http://www.kontron.com/resources/collateral/white\\_papers/whitepaper-aplabs-part1\\_en.pdf](http://www.kontron.com/resources/collateral/white_papers/whitepaper-aplabs-part1_en.pdf)

<sup>18</sup> For examples of the use of UAVs for civil contingencies see AUVSI, “Disaster Response” Increasing Human Potential, 30 April 2014. <http://increasinghumanpotential.org/category/news/spotlight/disaster/>

<sup>19</sup> Badkar, Mamta, “China May Use Drones To Kill The Smog Problem”, *Business Insider*, 5 March 2014. <http://www.businessinsider.com/china-is-testing-smog-clearing-drones-2014-3>

Operator(s)	Mission	Target	Examples	Equipment	Data collected
Commercial /government (institutional)	Environmental monitoring	Air, water or other natural resources	Pollution monitoring, hazardous material sensing, air/water quality testing, weather monitoring	Biological, chemical, meteorological, and GPS sensors, cameras	Chemical samples, meteorological readings and some visual images, personal data unlikely to be collected.

### 7.2.5 Precision agriculture

The potential use of RPAS in agriculture, forestry and fisheries includes a range of resource management and monitoring applications.<sup>20</sup> Close-up surveillance of farm plots can provide high-resolution data capable of identifying invasive species, drought and blight, and other diseases. For remote sites or terrain that is difficult to cover by land vehicle, RPAS can provide quick and effective monitoring of food crops and livestock. Spraying fertilizers, pesticides and fungicides could also be done by RPAS with increasing autonomy capable of minimising human input. Surveying equipment mounted on RPAs can be used to plan planting and drainage and to map and estimate crop yields.

A number of payloads can be used to provide RPAS-assisted farming. RPAS may be used to collect visual images of plants, animals and terrain to identify potential problems. In addition to visual information, temperature sensors or hyperspectral or thermal imaging can be used to identify plants that are under stress for a variety of potential reasons.<sup>21</sup> These missions are unlikely to collect personal data, aside from the potential, inadvertent capture of images of neighbours' property or objects. However, as above, there is a small possibility that RPAS operations could impact the safety of living things on the ground. However, given the similarity of the potential issues raised with the infrastructure inspection mission, no individualised scenario is examined for this mission.

Operator(s)	Mission	Target	Examples	Equipment	Data collected
Commercial / private individuals	Precision agriculture	Crops, landscape and animals	Crop inspection, herd inspection, crop spraying	Cameras with thermal, hyperspectral and optical capabilities, chemical sensors, temperature sensors	Images from across the visual and non-visual spectrum, temperature readings, personal data of neighbours may be collected inadvertently.

<sup>20</sup> For example of these applications see Farmingdrones.com, "Farming Drones: UAVs in the Agriculture Industry", 2013. <http://farmingdrones.com/>

<sup>21</sup> Rohr, Rachel, "Meet the new drone that could be a farmer's best friend", *Modern Farmer*, 21 January 2014. <http://modernfarmer.com/2014/01/precision-hawk/>

### 7.2.6 Novel services

One of the key associated benefits of RPAS is their versatility. They come in a range of sizes, with a range of flight capabilities and may be fitted with a range of different payloads. This versatility is one of the main drivers of RPAS' ability to engender new and innovative services and industries.<sup>22</sup> While it is difficult to predict what these new services may be, many of them will likely involve the collection of data in populated areas. For example, in relation to transport, the retailer *Amazon* made headlines recently when it suggested that UAS could one day be used to deliver its products to consumers in an exercise widely regarded as a publicity stunt.<sup>23</sup> Similarly, the United Arab Emirates says it plans to use unmanned aerial drones to deliver official documents and packages to its citizens as part of efforts to upgrade government services.<sup>24</sup> Other novel services could result from new payloads or the extension of current RPAS uses in law enforcement and/or other sectors to generate new consumer services. For example, in real estate, thermal imaging is being used to test the energy efficiency levels of residential and commercial buildings. For large buildings and sites, an RPAS may be more efficient than a "walk-through". The rapid expansion of RPAS usages and relevance means that the types of data collected will be dynamic and shifting. Furthermore, policy support for big data, and the efficiencies and novel services that could be created through linking data<sup>25</sup>, will also likely impact the types of services that RPAS may provide. Some companies, such as Precision Hawk, have already begun re-orienting their services to highlight the data capture and analysis elements of their service, rather than the use of remotely piloted aircraft systems to collect the data in question.<sup>26</sup>

Given the diversity of these different capabilities and applications, there is a significant possibility that some of these applications and missions may involve the collection of personal data by commercial organisations. Given this possibility, these organisations must be encouraged, or required, to consider the potential privacy and data protection impacts associated with these new applications and services on a case-by-case basis. The scenario below sets out one potential example of linking data for innovative service provision.<sup>27</sup>

---

<sup>22</sup> European RPAS Steering Group, *Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System*, June 2013.

<http://ec.europa.eu/enterprise/sectors/aerospace/uas/>

<sup>23</sup> See for example, "Amazon testing drones for deliveries", *BBC News*, 2 December 2013.

<http://www.bbc.co.uk/news/technology-25180906>

<sup>24</sup> "UAE to use drones for citizen services", *Al Jazeera*, 12 February 2014.

<http://www.aljazeera.com/news/middleeast/2014/02/uae-use-drones-government-services-20142121717319272.html>

<sup>25</sup> European Commission, Communication from the Commission: Towards a thriving data-driven economy, COM(2014) 442 final Brussels, 2 July 2014. <https://ec.europa.eu/digital-agenda/en/news/communication-data-driven-economy>

<sup>26</sup> PrecisionHawk, "PrecisionHawk UAV and Data Software", *YouTube*, 13 January 2014.

[http://www.youtube.com/watch?v=V244qPNz\\_4k](http://www.youtube.com/watch?v=V244qPNz_4k). See also PrecisionHawk, "Mission", 2014.

<http://precisionhawk.com>

<sup>27</sup> Studio Fly, "Thermographie aérienne de maison par drone", 24 April 2013.

<http://www.studiofly.fr/thermographie-aerienne-pavillons-prives-maisons-drone/>

Operator(s)	Mission	Target	Examples	Equipment	Data collected
Commercial	Varied	Objects, animals, landscapes, people, the environment, and others	Varied	Varied	Significant potential for personal information to be collected, or to be discovered via combining data collected by RPAS with other data sets.

A typical scenario for such new services is the following:

*An energy company uses a commercial RPAS equipped with a GPS sensor and a thermal camera to film houses and other buildings in several residential areas. Using the information collected from the thermal camera, the energy provider identifies a number of homes and businesses with poor insulation. The energy company then uses the GPS coordinates to match the thermal data with individual customers' addresses. This information is used to send out discount offers on roof insulation under the auspices of meeting national carbon reduction targets.*

This sub-section demonstrates the varied uses to which RPAS may be deployed in the commercial sector. The analysis finds that many of the potential RPAS applications examined in relation to commercial missions are not targeted at people and often do not collect personal information. However, some operations are (or may be) targeted at people or may inadvertently collect personal information. In these circumstances, it is very important that RPAS operators adhere to their obligations under relevant legislation. This is especially important as compliance with existing law and the provision of robust protections for citizens is one of the best ways to foster public acceptance of the civil use of RPAS.

### 7.3 Law enforcement and government operators

The literature review and stakeholder consultation exercises has found that law enforcement and other public authorities are clear potential users of civil RPAS, but that they often represent the most potentially controversial users. Furthermore, they are not subject to many of the privacy and data protection laws to which commercial users must adhere. However, despite this legal room to manoeuvre, public sentiment and expectations around their privacy and the protection of their data can have a significant impact on the feasibility of using RPAS for civil law enforcement or government purposes. As noted above, this is a key aspect of fostering positive public reactions. This section examines the potential use of RPAS for the surveillance of people, civil protection, search and rescue and regulatory enforcement.

#### 7.3.1 Surveillance of people

The use of RPAS for policing and law enforcement purposes has provoked widespread criticism and concern from non-governmental organisations. However, police drones may be the exception rather than the rule, at least in the short term. The use of UAS for public order purposes is still controversial, but they have been tested for a number of missions including:

- monitoring crowds at events such as festivals<sup>28</sup>, protests<sup>29</sup> and sporting events<sup>30</sup>,
- prevent anti-social behaviour<sup>31</sup>,
- detect marijuana cultivation<sup>32</sup>, and
- support police in pursuits and operations<sup>33</sup>.

Less controversial police operations have been limited to obtaining after-the-fact crime scene images, search and rescue, and providing imagery for structure fire suppression and arson investigations.<sup>34</sup> Nevertheless a much wider range of applications for surveillance, tracking and public order purposes has been envisaged, although their use remains subject to the resolution of the regulatory and considerable data protection and human rights issues at stake. Police helicopters are very expensive to keep in the air and it is widely expected that UAVs could provide the same kind of aerial surveillance for a fraction of a cost. In addition to domestic law enforcement, RPAS and UAS are also likely to play some role in EU maritime security policy, whether as part of the EUROSUR (border surveillance) system or for common EU security and defence operations, such as the on-going international anti-piracy mission of the Somali coast.

In order to assist in these various law enforcement applications, RPAS may be fitted with a number of different types of payloads. For example, for crowd monitoring and surveillance, or for the monitoring of people or vehicles on the move, RPAS would require high definition video and still image cameras as well as GPS capabilities. To detect marijuana cultivation or support police operations in similar fashion to helicopters, RPAS would require thermal imaging capabilities. Finally, RPAS may also assist police through audio sensing and recording capabilities. The audio devices that can be fitted to RPAS range from the simple microphones that accompany basic video recording systems to much more complex acoustic systems including passive radar for detecting noise emitting objects.<sup>35</sup> The former are limited because of the noise created by the engines and motors used to propel RPAS; the latter have been deployed in military UAS to “acoustically map” battlefield situations by locating and classifying all sources that are below an RPAS in order to detect gunshots, armoured vehicles and other assets.

In addition to these physical payloads, software payloads are also being explored to assist police. To prevent anti-social behaviour, illegal intrusions onto protected spaces or other behavioural problems, RPAS cameras and other sensors could be fitted with emerging

---

<sup>28</sup> Randerson, James, “Eye in the sky: police use drone to spy on V festival”, *The Guardian*, 21 Aug 2007. <http://www.guardian.co.uk/uk/2007/aug/21/ukcrime.musicnews>

<sup>29</sup> Whitehead, John W., *Drones Over America: Tyranny at Home*, The Rutherford Institute, Charlottesville, VA, 28 June 2010. [http://www.rutherford.org/articles\\_db/commentary.asp?record\\_id=661](http://www.rutherford.org/articles_db/commentary.asp?record_id=661)

<sup>30</sup> Eick, Volker, *The Droning of the Drones: The increasingly advanced technology of surveillance and control*, Statewatch Analysis, No. 106, 2009, p. 1. <http://www.statewatch.org/analyses/no-106-the-droning-of-drones.pdf>

<sup>31</sup> Randerson, op. cit., 2007.

<sup>32</sup> McCullagh, Declan, “Drone aircraft may prowl U.S. skies”, *CNET News*, 29 March 2006. [http://news.cnet.com/Drone-aircraft-may-prowl-U.S.-skies/2100-11746\\_3-6055658.html#ixzz1JURmGB4a](http://news.cnet.com/Drone-aircraft-may-prowl-U.S.-skies/2100-11746_3-6055658.html#ixzz1JURmGB4a)

<sup>33</sup> Hull, Liz, “Drone makes first UK ‘arrest’ as police catch car thief hiding under bushes”, *Daily Mail*, 12 Feb 2010. <http://www.dailymail.co.uk/news/article-1250177/Police-make-arrest-using-unmanned-drone.html#ixzz1JV7EKR1N> and Eick, op. cit., 2009, p. 4.

<sup>34</sup> Villasenor, op. cit., 2013, p. 467.

<sup>35</sup> Adams Technology Pvt. Ltd., “Battlefield Acoustics – Microflown”, *Adams Technology*, no date. <http://adams-tech.net/battlefield-acoustic.html>

“smart” software. “Smart surveillance” systems that are already in use include the detection of abnormal or suspicious behaviour using visual cameras, profiling and data mining techniques.<sup>36</sup> Fitting RPAS with ANPR capabilities is one such example. In addition, the Japanese company Secom is already marketing a “private security drone” that can “take to the air if there's a break in and record what's happening” and “track moving subjects with a laser sensor”.<sup>37</sup> As noted above, many are equipped with night-vision cameras or forward-looking infrared (FLIR) cameras that detect radiation emitted heat sources. RPAS may also be fitted with infrared search and track (IRST) systems capable of detecting and tracking objects that give off infrared radiation.<sup>38</sup> These functionalities will enable RPAS to search for and identify items, to track targets and deliver payloads autonomously. In addition, some researchers are adding facial recognition technology to RPAS, causing alarm among civil liberties organisations.<sup>39</sup> Although they carry a heightened risk in terms of their impact on data protection and fundamental rights, the development of “smart surveillance” technologies has the potential to minimise the amount of data that is collected by employing triggers and filters (or “artificial vision technologies”) that block out certain data or relay limited pictures – in much the same way as the new generation of body scanners.<sup>40</sup>

Given these different payloads, the amount of data that could be collected by police and government agencies is substantially varied. Image data, including thermal and infrared images may be collected. These may be either purposely-collected images from targeted surveillance or response activities as well as unintentionally collected images. Audio data may also result from audio sensors, although these types of recordings are substantively controlled and are unlikely to collect personal data of non-targeted subjects. Finally, identity and behavioural data may also be collected, in particular sensitive data like biometrics may soon be collectable via RPAS. This significantly expands the potential privacy, ethical and data protection risk that may arise, particularly in relation to citizens’ concerns rather than legal prohibitions.

---

<sup>36</sup> See Wright, David, Michael Friedewald, Serge Gutwirth, Marc Langheinrich, Emilio Mordini, Rocco Bellanova, Paul De Hert, Kush Whadwa and Didier Bigo, “Sorting out smart surveillance”, *Computer Law & Security Review*, Vol. 26, 2010, pp. 343-354.

<sup>37</sup> Fingas, Jon, “Secom offers a private security drone, serves as our eyes when we're away”, *Engadget*, 27 December 2012. <http://www.engadget.com/2012/12/27/secom-offers-a-private-security-drone/>

<sup>38</sup> Axe, David, “The Pentagon Has Figured Out How to Hunt Enemy Stealth Fighters”, *Medium.com*, 27 February 2014. <https://medium.com/war-is-boring/3acf9d25cd44>

<sup>39</sup> Conte, Andrew, “Drones With Facial Recognition Technology Will End Anonymity, Everywhere”, *Business Insider*, 27 May 2013. <http://www.businessinsider.com/facial-recognition-technology-and-drones-2013-5>; “Domestic Unmanned Aerial Vehicles (UAVs) and Drones”, *Electronic Privacy Information Centre*, no date. <http://epic.org/privacy/drones/>

<sup>40</sup> The aforementioned 3i project, for example, is using UAS equipped with “[A]utomated triggers and filters in the vision software that can filter images before they are recorded. So that any privacy sensitive images that are not of interest to the mission can be filtered out. The triggers can also be used to start recording only when an anomaly has been detected, e.g. a fire or an oil spill on the surface of the water”. See 3i project website, <http://www.2seas-uav.com/>

Operator(s)	Mission	Target	Examples	Equipment	Data collected
Law enforcement / public authorities	Law enforcement surveillance of people	People	Infrastructure protection against theft, etc. (railways, etc.), targeted criminal investigation, crowd monitoring, border control, anti-social behaviour, supporting police response	High-tech camera, audio recording, infrared / thermal camera, GPS, ANPR, biometric and behaviour recognition software	Significant potential for personal information to be collected, including sensitive data.

A typical scenario for such law enforcement missions is the following:

*A local police force launches a new surveillance mission aiming to identify a group of young offenders committing petty crimes and anti-social activities for the last month. The police station launches two drones fitted with tracking devices (GPS) and multi-function (optical, thermal and infra-red) cameras. The remote pilot flies the RPAS above the social housing estate that has recently been affected by the youth. Although the officers did not locate the youth on the first day, footage from the thermal camera did indicate instances of abnormal hydroponic heat and light usually used for the growth of cannabis plants. The remote pilot shoots some footage of the properties in question and this information is sent to the narcotics team.*

### 7.3.2 Civil protection

Civil protection and contingencies includes emergency planning and response and the monitoring of critical infrastructure. It involves a wide range of public services and private actors and the sector is expected to see a strong take-up of RPAS. After natural or manmade disasters the aircraft can be used to monitor and assess damage, to deliver supplies and equipment, or to detect chemical, nuclear or biological hazards. In relation to disaster relief, fire and rescue services are already using pilotless aircraft to ascertain the spread and extent of fires and to map the surrounding areas for hazardous materials. Agencies responsible for search and rescue and emergency response are using RPAS for navigating areas too dangerous or remote for them to reach using conventional equipment.

These missions are accomplished using RPAS that offer aerial photography and video streaming, chemical, biological and other sensors, air quality sensors and thermal imaging payloads. Aside from search and rescue missions, the data collected is unlikely to include personal information, as it is focused on chemical information or landscape monitoring. However, search and rescue missions may be combined with payloads that enable the identification of mobile phone signals, abnormal behaviour detection and other capabilities in addition to optical and thermal imaging. Therefore, there is some possibility that personal information of lost individuals as well as other individuals in the vicinity may be collected.

Operator(s)	Mission	Target	Examples	Equipment	Data collected
Law enforcement / public authorities	Civil protection	Landscapes, people	Infrastructure monitoring, search and rescue, firefighting, hazard detection, crisis response	High-definition optical camera, audio recording, infrared / thermal camera, GPS, mobile phone sensors, behaviour recognition software	While most applications are not focused on people, those that are may collect personal data.

A typical civil protection scenario includes the following:

*Emergency services deploy an RPAS equipped with thermal imaging, a mobile phone signal sensor and GPS capabilities to search for hikers lost in the woods. The search picks up mobile phone and heat signatures from a number of hikers, generating “false alarms” which must be investigated by matching phone signals to individual mobile phone accounts. The correct lost hikers are found after a few hours, and the data from the “false alarms” is immediately discarded.*

### 7.3.3 Regulatory enforcement

Finally, government or law enforcement authorities may use RPAS to enforce sector-specific rules and regulations. This may include the use of RPAS to monitor air, land and water for pollution, illegal logging and other prohibited activities.<sup>41</sup> In addition to law enforcement authorities, these systems may be used by forest rangers, environmental protection authorities and local councils as well as other authorities. The payloads that may be used for these purposes include optical, thermal and infrared cameras, sensors that collect air, water or soil samples and GPS sensors. Furthermore, as possibilities for RPAS usage in this area expands and develops, the sensors with which the RPAS may be fitted will also likely expand. Because their precise mission will vary, they may be focused on collecting data from landscapes, the environment (air, water, soil, etc.) as well as people (e.g., those carrying out activities such as illegal logging). However, those operations which are not focused on people are very unlikely to collect personal data, given that the optical capabilities will likely be focused on the monitoring of remote areas, while the monitoring of pollution in populated areas will likely focus on other, chemical sensors. As such, the activities focused on monitoring people could be combined with the issues associated with monitoring people, while the activities focused on chemical data collection could be considered under mapping and earth observation. Nevertheless, a short scenario is presented to highlight some issues.

<sup>41</sup> AUVSI “The Benefits of Unmanned Aircraft Systems: Saving Time, Saving Money, Saving Lives”, Association for Unmanned Vehicle Systems International (AUVSI), no date. <http://epic.org/events/UAS-Uses-Saving-Time-Saving-Money-Saving-Lives.pdf>

Operator(s)	Mission	Target	Examples	Equipment	Data collected
Law enforcement / public authorities	Regulatory enforcement	Landscapes, people	Pollution monitoring, fisheries monitoring, monitoring for illegal logging, and others	High-definition optical camera, infrared / thermal camera, GPS	While most applications are not focused on people, those that are may collect personal data.

A typical scenario examining such regulatory enforcement includes the following:

*The Environmental Protection Agency hires a commercial RPAS operator to undertake a range of surveillance necessary to enforce restrictions against logging and monitor for forest fires and air pollution in a nature reserve. The RPAS is fitted with high definition video surveillance, thermal imagery and environmental sensors. It patrols a specific area and takes regular photos and readings. These photos and readings are transmitted back to the forest rangers' office. Occasionally hikers, campers and other nature enthusiasts are captured in the images, and authorities occasionally follow up on suspicious images or readings by visiting campsites or seeking out groups of people. No arrests have been made.*

In relation to law enforcement and other uses by public authorities, many of the RPAS missions examined here include a focus on people, or at least a secondary focus on people. This means that a significant amount of personal data may be collected, and that significant potential impacts related to privacy and ethics must be considered. All of the missions described above involve some collection of personal data, especially images, location data and even names and addresses. While public authorities are relatively trusted collectors and users of such data, the potential intrusions associated with these missions have considerable potential impacts of the life chances of individuals targeted by this surveillance.

#### 7.4 Journalists and filmmakers

In addition to law enforcement and government authorities, journalists (and filmmakers) are also subject to exceptions in relation to data protection and privacy legislation. The film industry has already added mounted high-resolution cameras on RPAS to provide aerial footage. Furthermore, many are excited about the prospect of “drone journalism”,<sup>42</sup> and commercial broadcasters are using them for newsgathering. Yet, while this exemption was intended to protect freedom of the press and freedom of expression, it may also unintentionally enable some irresponsible practices. Some stakeholders are worried that RPAS will be used irresponsibly by “paparazzi” prepared to ignore any privacy and aviation regulations.<sup>43</sup> The use of RPAS for media and private photography purposes could also breach some national laws on trespass, stalking/harassment and commercial secrecy. Additionally,

<sup>42</sup> Goldberg, David, Mark Corcoran and Robert G. Picard, *Remotely Piloted Aircraft Systems and Journalism: Opportunities and Challenges of Drones in News Gathering*, Reuters Institute for the Study of Journalism, University of Oxford, 2013.

<sup>43</sup> According to Villasenor, “it would be optimistic to the point of naïveté to expect them to always operate UAS in a manner respectful of privacy considerations and in compliance with FAA safety regulations”. Villasenor, op. cit., 2013, p. 499.

the use of RPAS for filmmaking will be interpreted differently depending on the organisation that is carrying out the mission and the organisation that commissioned it.

The uses of RPAS for journalism or filmmaking will likely focus on visual and audio capabilities, and people will be a significant sub-set of the likely targets of data collection. (Other targets may include landscapes for films/stories focused on the environment, buildings, animals, etc.) Such journalistic filming may be overt or covert. The types of data collected are likely to include personal data, especially images of individuals and recordings of their activities and communications. While the targets, equipment and data collected are similar for both of these categories, two different scenarios are presented below to highlight some of the distinctions, particularly in relation to public opinion, surrounding these missions.

Operator(s)	Mission	Target	Examples	Equipment	Data collected
Journalists / filmmakers	Journalism, filmmaking	Varied – landscapes, animals, buildings, people	Live journalistic reporting, investigative reporting, documentary filmmaking, promotional videos, fictional filmmaking	High-definition optical camera, infrared / thermal camera, GPS, audio sensors	Likely to collect personal data

This sub-section presents two scenarios, separately, that represent typical uses of RPAS for filmmaking and journalism.

*A local council decides to encourage tourism by commissioning a collection of videos and still photos of village life, as captured by an RPAS. The RPAS zipped through the streets, capturing images of people shopping, sunbathing and relaxing in the local gardens. Residents were not informed of the filming, although some saw the RPAS and its operator and assumed it was a toy. A few residents complained when images of them and their families were released via the Internet, but the council has argued that videoing in public places is just like CCTV.*

*An enormous car accident occurs on a main highway and the first reports from the scene are from a car driver describing events on the local radio. A photographer who specialises in breaking news drives directly to the scene and parks close to the accident site. He launches his RPAS equipped with a high-definition video camera directly connected to his computer, which streams live feed to his personal website. Flying above the highway he spots a car overturned in a field along the road and approaches with his RPAS. He begins streaming the footage to his website and captures and transmits images of two dead bodies just over two meters from the stricken vehicle.*

As noted in relation to law enforcement and other authorities' use of RPAS, the missions associated with some filmmakers and journalists are likely to focus on people as the targets of investigation. This may result in the collection of significant amounts of personal data, including visual images, audio data, location data as well as others. While artists and filmmakers are protected categories of data collector, their activities may also have potential impacts on the life chances of individuals, particularly when sensationalist journalists (e.g.,

paparazzi) or filmmakers are considered alongside reputable journalists and filmmakers. The impacts associated with this data collection are considered in detail in the next chapter.

## 7.5 Telecommunication providers

However, stakeholders are also investigating the provision of communication networks as a potential application area for RPAS. Interest in this sector piqued recently with the announcement that Facebook is in advanced talks to buy Titan Aerospace, a producer of solar-powered RPAS.<sup>44</sup> RPAS can be used as proxy satellites to carry communications systems and provide broadband services. Titan Aerospace’s “Solara 50” and “Solara 60” models can be launched at night using power from internal battery packs, then, when the sun rises, can store enough energy to ascend to 20 kilometres above sea level where they can remain for five years without needing to land or refuel. As a communications relay, one Solara UAV can provide coverage for a radius of around 18 miles with a “constellation” of the craft able to create a persistent communications network.<sup>45</sup> Facebook is partnering with six telecommunications partners in a project called *Internet.org*, which aims to provide affordable Internet access to the five billion people for whom it is currently out of reach.<sup>46</sup> Google is involved in a similar initiative using a network of unmanned hot air balloons (a type of UAS) at the same altitude.<sup>47</sup> These initiatives are expected to provide broadband telecommunications services at a fraction of the cost of their satellite-based counterparts. In addition to providing telecommunications services over small or wide areas, RPAS can also be fitted with equipment that enables the local interception of telecommunications.<sup>48</sup> The data that could be collected includes traffic data, location data, content of communications (in some circumstances) and personally identifiable information such as device data.

Operator(s)	Mission	Target	Examples	Equipment	Data collected
Telecommunications companies	Telecommunications service providers	Telecommunications and computing devices	Mobile phone service provision, mobile broadband, Wi-fi broadband	Communication relay equipment	Likely to collect personal data

---

<sup>44</sup> Perez, Sarah, “Facebook Looking Into Buying Drone Maker Titan Aerospace”, *Techcrunch.com*, 3 March 2014. <http://techcrunch.com/2014/03/03/facebook-in-talks-to-acquire-drone-maker-titan-aerospace/>

<sup>45</sup> Gallagher, Sean, “Almost orbital, solar-powered drone offered as ‘atmospheric satellite’”, *Ars Technica*, 18 August 2013. <http://arstechnica.com/information-technology/2013/08/almost-orbital-solar-powered-drone-offered-as-atmospheric-satellite/>

<sup>46</sup> Internet.org, “Making the Internet affordable”, no date. <http://internet.org/>

<sup>47</sup> Its project is called Google, “Project Loon”, no date. <http://www.google.com/loon/>

<sup>48</sup> The technology that these UAVs are equipped with are known as ‘IMSI catchers’ or ‘stingrays’: essentially a false cell phone tower used for the interception and tracking of mobile phones that is virtually undetectable by the targets of surveillance (IMSI stands for International Mobile Subscriber Identity and is the unique identifier found in all ‘SIM cards’). IMSI catchers can be produced at very low cost and pocket-sized models are now available. See Robinson, Clarence. A. Jr., “Petite Cyber Drone Packs Punch”, *Defense Media Network*, 24 September 2011. <http://www.defensemedianetwork.com/stories/petite-cyber-drone-packs-punch/>

A realistic scenario for the use of RPAS to provide telecommunication services includes the following:

*A national telecommunications provider launches a new service intended to provide high-bandwidth, mobile broadband to under-served rural areas. The RPAS routes local mobile signals to the company's communications satellite, and no data is stored by the RPAS. However, a local teenager has found a way to hack into the wireless signal and can view information about her neighbours' communications and whereabouts.*

This scenario represents the potential for RPAS to be implicated in the collection of personal, communication data by a telecommunication provider. Although this type of data is among the most sensitive, telecommunication providers are required to retain some of it and are required to process it in order to provide the service in question. The next chapter examines how the potential insecurity of the communication linkages between the RPAS and the telecom provider may impact the privacy, data protection or ethical expectations of members of the public.

## **7.6 Private individuals using RPAS for household or personal uses**

As noted already, the capabilities of RPAS are wide and varied and new capacities are continually being devised. It is also important to note that for all the concern about the use of RPAS by governments, there are already more drones being flown by hobbyists than there are by the military. Thanks to the “smartphone revolution” and other rapid advances in consumer electronics, private individuals have all the necessary elements to create their own RPAS and use them for household or personal uses.<sup>49</sup> These technological developments underpinned the emergence of “personal drone” communities dedicated to open-source drone research and development that are in turn creating commercial spin-offs and accelerating the already dynamic pace of innovation. In 2013 “DIY Drones”, an online social network, boasted more than 36,000 members worldwide.<sup>50</sup> Furthermore, the household exemption means that existing data protection legislation does not cover most uses of RPAS by private individuals. Instead, they are covered by regulations related to model aircraft, which often make no mention of privacy or data protection.

Most private uses of RPAS are centred around high-definition optical cameras, e.g., GoPro cameras, and the data collected is primarily collective visual and audio data. This footage may range from amateur photographers taking still photos of wildlife and landscapes, to amateur filmmakers recording fictional scenes, to irresponsible individuals taking covert, voyeuristic recordings of neighbours. Despite this current focus on optical cameras and audio microphones, other types of payloads may become more popular as the sector develops. For example, amateur meteorologists may begin fitting RPAS with environmental sensors intended to measure air moisture, pressure, wind speed and other factors.

---

<sup>49</sup> Corcoran, Mark, “Drone journalism takes off”, *ABC News Online - Foreign Correspondent Special Report*, 21 February 2012. <http://www.abc.net.au/news/2012-02-21/drone-journalism-takes-off/3840616>

<sup>50</sup> See DIY Drones, “DIY Drones: The leading community for personal UAVs”, 2014. <http://diydrones.com/>

Operator(s)	Mission	Target	Examples	Equipment	Data collected
Private individuals	Varied	Landscapes, buildings, wildlife, people	Varied: Amateur photography and filmmaking, amateur meteorology, etc.	High-definition optical cameras, thermal cameras, audio and other sensors	Likely to collect personal data

A typical scenario for the use of RPAS by private individuals includes the following:

*A local aircraft enthusiast purchases a drone to curb anti-social behaviour in his neighbourhood. He films teenagers' hanging out in his neighbour's front garden, and sometimes uses the drone to follow young people home and identify where they live. The drone is small and very quiet, and the teens are often unaware that they are being filmed.*

According to the consultation exercises described in Chapter 6, members of the public represent the most risky users of RPAS, especially as most of the potential missions for which they can be used involve the collection of personal data on other members of the public. This collection may involve visual, audio, location or other types of data, that may reveal sensitive information about people, and which may be collected covertly. Furthermore, the analysis above indicates that members of the public are often not subject to data protection legislation through the household exemption. However, there is little to indicate what RPAS regulators could do to adequately address these risks.

## 7.7 Summary

This chapter has demonstrated the varied uses for which RPAS may be deployed. It is framed by the different categories of user that may deploy RPAS and examines the potential missions, targets and examples associated with those uses. Based on a review of RPAS capabilities and payloads, it also examines the equipment that may be fitted to the RPAS to achieve those missions and the types of data that may be collected. This information is summarised in the table below.

Operator(s)	Mission	Target	Examples	Equipment	Data collected
Commercial	Infrastructure inspection	Objects	Inspection of mobile phone towers, bridges, power lines, wind turbines, nuclear and industrial installations	High resolution video and still cameras, thermal cameras	Photographs and video images of the infrastructure, <b>personal data may be collected inadvertently</b>

	Other visual services	Objects and people	Footage for sales, marketing or publicity purposes	High resolution video and still cameras	Photographs and video images – <b>many applications likely to collect personal data</b>
	Geo-spatial mapping	Objects, landscapes, foliage	Mapping and surveying for exploration, planning and crisis management	High resolution cameras, infrared cameras, synthetic aperture radar, photogram-metric equipment	Images of the objects or spaces targeted, <b>personal data unlikely to be collected</b>
	Environmental monitoring	Air, water or other natural resources	Pollution monitoring, hazardous material sensing, air/water quality testing, weather monitoring	Biological, chemical, meteorological, and GPS sensors, cameras	Chemical samples, meteorological readings and some visual images, <b>personal data unlikely to be collected</b>
	Precision agriculture	Crops, landscapes and animals	Crop inspection, herd inspection, crop spraying	Cameras with thermal, hyperspectral and optical capabilities, chemical sensors, temperature sensors	Images from across the visual and non-visual spectrum, temperature readings, <b>personal data of neighbours may be collected inadvertently</b>
	Varied	Objects, animals, landscapes, people, the environment and others	Varied	Varied	<b>Significant potential for personal information to be collected</b> , or to be discovered via combining data collected by RPAS with other data sets.

Law enforcement / public authorities	Law enforcement surveillance of people	People	Infrastructure protection against theft, etc. (railways, etc.), targeted criminal investigation, crowd monitoring, border control, anti-social behaviour, supporting police response	High-tech camera, audio recording, infrared / thermal camera, GPS, ANPR, biometric and behaviour recognition software	<b>Significant potential for personal information to be collected</b> , including sensitive data.
	Civil protection	Landscape s, people	Infrastructure monitoring, search and rescue, fire fighting, hazard detection, crisis response	High-definition optical camera, audio recording, infrared / thermal camera, GPS, mobile phone sensors, behaviour recognition software	While most applications are not focused on people, those that are <b>may collect personal data</b> .
	Regulatory enforcement	Landscape s, people	Pollution monitoring, fisheries monitoring, monitoring for illegal logging, and others	High-definition optical camera, infrared / thermal camera, GPS	While most applications are not focused on people, those that are <b>may collect personal data</b> .
Journalists / filmmakers	Journalism, filmmaking	Varied – landscapes, animals, buildings, people	Live journalistic reporting, investigative reporting, documentary filmmaking, promotional videos, fictional filmmaking	High-definition optical camera, infrared / thermal camera, GPS, audio sensors	<b>Likely to collect personal data</b>
Telecommunications companies	Telecommunication service providers	Telecommunication and computing devices	Mobile phone service provision, mobile broadband, Wi-fi broadband	Communication relay equipment	<b>Likely to collect personal data</b>

Private individuals for private purposes	Varied	Landscape s, buildings, wildlife, people	Varied: Amateur photography and filmmaking, amateur meteorology, etc.	High-definition optical cameras, thermal cameras, audio and other sensors	<b>Likely to collect personal data</b>
--	--------	--	---	---	--

The analysis reveals that in the commercial sphere, some missions and payloads, specifically infrastructure monitoring, precision agriculture and other services, are likely to collect personal data, both intentionally and inadvertently. Chapter 6 revealed that many responsible commercial operators are undertaking risk assessments to manage the data that they collect. However, while the intentional collections of personal data are likely to be considered by responsible commercial operators, the inadvertent personal data collection may not be subjected to such rigorous risk assessment due primarily to a lack of awareness.

Other operators, such as law enforcement and other authorities, journalists, filmmakers and members of the public are likely collecting personal information, but are not subject to the same regulations. While many reputable professionals are likely seriously considering whether their operations are collecting personal data and the ways in which this may impact members of the public, there is little data on this. This is especially problematic, as many of these operators’ missions focus on people as the targets of information collection.

The following chapter analyses the privacy, data protection and ethical issues associated with each of the scenarios presented in this chapter. It details precisely what aspects of privacy, data protection and ethics might be impinged in the scenarios, and it indicates straightforward solutions to assist stakeholders in addressing some of the impingements identified.

## 8 PRIVACY, DATA PROTECTION AND ETHICS IN RPAS SCENARIOS

### 8.1 Introduction

This chapter links all of the above chapters together by undertaking a privacy, data protection and ethical analysis of the typical and realistic RPAS scenarios presented in Chapter 7. The purpose of this examination is to link actual practices to the legal framework and to identify realistic risks to privacy, data protection and ethics based on information gleaned from the consultation exercises in Chapter 6 and the literature reviews in Chapters 3 - 5. This information is used to assign a risk “level” for each issue, and is intended as a guide to assist RPAS operators in identifying what the level of risk associated with particular RPAS applications may be. The analysis focuses on each of the five categories examined in the previous chapter, including commercial, law enforcement and other public authorities, journalists, filmmakers, telecommunications providers and private individuals.

Following these scenarios, the chapter examines the ethical, privacy and data protection risks raised in each of these scenarios. In order to do so, we rely on the privacy, data protection and ethical risks identified in Chapters 3 and 4.

For **privacy**, we examine:

<b>A chilling effect</b>	This refers to situations where individuals are unsure about whether they are being observed, and “attempt to adjust their behaviour accordingly”. <sup>1</sup>
<b>Dehumanisation of the surveilled</b>	This may occur when RPAS pilots are physically and psychologically removed from the act of observation or information collection, and do not consider the impacts of their activities on individuals on the ground.
<b>Transparency and visibility</b>	This refers to the fact that individuals on the ground may not know an RPAS is in operation, and if they do, may be unsure about who is operating the RPAS and the purpose for which it is being used.
<b>Function creep</b>	This occurs when the purposes of RPAS usage expand, either to additional operations or to additional activities within the originally envisaged operation. <sup>2</sup>
<b>Body privacy</b>	This refers to “the right to keep body functions and body characteristics (such as genetic codes and biometrics) private”. <sup>3</sup>

---

<sup>1</sup> Finn, Rachel L., David Wright and Michael Friedewald, “Seven types of Privacy”, in Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (Eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013, p. 16.

<sup>2</sup> Statewatch, “Commission Wants Drones Flying in European Skies by 2016”, *Statewatch News Online*, September 2012. <http://www.statewatch.org/news/2012/sep/eu-com-drones.htm>

<sup>3</sup> Finn, et al., op. cit., 2013, p. 15.

<b>Privacy of location and space</b>	This “encompasses the right of individuals to move in their ‘home’ and other public or semi-public places without being identified, tracked or monitored”. <sup>4</sup>
<b>Privacy of association</b>	This refers to “the freedom of people to associate with others”. <sup>5</sup>

In addition to privacy, this analysis also examines the **data protection issues** associated with each of these scenarios. As noted in Chapter 5, these data protection issues are limited to instances where “personal information”, including identifiable images, is collected and processed. Practically speaking, understanding ways in which each data protection principle can be observed can also assist RPAS operators in understanding the interrelationship between some of the principles. In turn, understanding how the principles are related, enables RPAS operators to take practical steps to observe one principle that enables them to indirectly meet the requirements of another, related principle. For example, understanding how the transparency principles may be observed and taking practical steps in that regard (such as notifying individuals of the purpose of the data collection) may also satisfy the consent principle, because individuals will not be able to provide consent if they are not informed about the activity to which they are consenting. Based on the information in Chapter 5, the following data protection issues will be considered for each scenario, both individually and where relevant, when there exists a relationship between the principles that assists RPAS operators to effectively discharge all of their obligations under the data protection framework.<sup>6</sup>

<b>Transparency</b>	This principle requires that the data collector notify the data subject of the personal information collected, the purpose of that collection and use of the data, as well as details of the RPAS operator to enable the data subject to exercise their rights of <u>access, correction and erasure</u> . <u>Transparency</u> is also related to the principle of <u>Consent</u> in that informing the data subject of the purpose and extent of the data collection places the data subject in a position to provide “free and informed consent”, which is the degree of consent required by the Data Protection Directive. <u>Transparency</u> is also related to the principle of <u>purpose limitation</u> in that the purpose for which the data is used reflects only that purpose that the data subject was informed about, and consented to.
<b>Data minimisation</b>	Data must be “relevant” to the purpose for which it is being collected and the data collected must be the minimum amount of data necessary for the purposes pursued. <u>Data minimisation</u> is related to the principle of <u>proportionality</u> , and ensuring that data collected is minimised assists in observing the principle of <u>data proportionality</u> .
<b>Proportionality</b>	The data must not be “excessive in relation to the purposes for which they are collected and/or further processed” and data collectors must assess whether they are using the least intrusive means to collect the data required.
<b>Purpose limitation</b>	The collector must “specify the purpose of the collection and process

<sup>4</sup> Ibid., p. 16.

<sup>5</sup> Ibid.

<sup>6</sup> Unless indicated otherwise, all quotes come from the text of the 1995 Data Protection Directive 95/46/EC.

	the data collected only for purposes compatible with that collection”. <sup>7</sup> <u>Purpose limitation</u> is related to the principles of <u>transparency</u> and <u>consent</u> , as set out above.
<b>Consent</b>	Individuals must give consent to their data being collected, either through explicit consent, or by entering public spaces where they have been informed that data collection is taking place. Consent is closely related to the principle of <u>transparency</u> in the manner outlined above.
<b>Accountability</b>	This refers to the fact that the data controller must be identifiable and accountable to individuals and regulatory authorities. It requires data controllers to make themselves known to individuals and authorities in order to enable individuals to exercise their rights and to enable authorities to pursue investigations. Thus, <u>Accountability</u> is related to <u>transparency</u> .
<b>Rights of access, correction and erasure</b>	This ensures that individuals retain control over the information that is collected about them. This is related to the principle of <u>transparency</u> by which data subjects are made aware of their rights in this regard.
<b>Data security</b>	This refers to the fact that data controllers are obligated to ensure that personal data are stored and processed securely and protected from inadvertent disclosure and unlawful intrusion.
<b>Third country transfers</b>	Data controllers must ensure that any country to which personal data are transferred has an “adequate” level of data protection regime. This requires the data controller to have secure and total control over the data collected, and also understand which third countries that the European commission has deemed not to offer “adequate protection.”

In practical terms, an understanding of the data protection principles provide RPAS operators with separate opportunities to address the risks posed to privacy and data protection when employing RPAS. For example, RPAS operators could review their intended operations in light of the principles to ensure that they meet their obligations under the data protection framework by asking specific questions about their intended operations. Questions such as “who knows that this operation is being conducted – do those individuals know that they are being recorded?”, “how is this data secured?”, “can I affix my logo to the RPAS?”, and “is this image of the individual necessary to meet the purpose of operation and that purpose which I have informed the individuals about?” are simple, practical steps that can be undertaken by RPAS operators. These practical steps translate the legalese of the relevant data protection sections into meaningful operational tools for RPAS operators. Further, as mentioned above, an understanding of the practical application of these principles also assists in the understanding how RPAS operators can observe other, related principles. For example, transparency is related to a number of other principles and by observing this principle, RPAS operators have automatically taken steps towards meeting the requirements of other principles, including the principle of consent, accountability, and the rights of access, correction and erasure.

Finally, the analysis examines **ethical issues** related to the scenarios. These include:

---

<sup>7</sup> Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN, WP 203, Brussels, 2 April 2013, pp. 4-5. [http://idpc.gov.mt/dbfile.aspx/Opinion3\\_2013.pdf](http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf) (“A29WP Opinion 03/2013”).

<b>Safety</b>	This refers to the possibility that living things or buildings could be harmed or damaged by crashes or other negative impacts (e.g., noise) associated with RPAS use.
<b>Public dissatisfaction</b>	This refers to the possibility that people could become disillusioned with RPAS use based on the possibility that they are compromising safety or privacy and data protection rights.
<b>Discriminatory targeting -</b>	This refers to the fact that RPAS use (and the potential safety, privacy and data protection impacts) may be more prevalent in relation to certain populations or areas which are less likely to be able to effectively voice or act upon those concerns (e.g., marginalised populations or areas).

The analyses that follow examine each of these issues in relation to the scenarios presented. While it is not possible for this report to consider all of the potential infringements associated with RPAS, especially as RPAS capabilities and applications expand, the report is meant to act as a starting point to assist detailed a consideration of potential RPAS impacts in order to facilitate responsible and informed RPAS operations.

## 8.2 Commercial operators

As evidenced by the survey results examined in Chapter 6, the use of RPAS by commercial operators is primarily focused on infrastructure inspection, mapping, earth observation, precision agriculture and other, creative services. Commercial operators are bound by privacy laws via the Charter of Fundamental Rights of the European Union and the European Convention of Human Rights, as well as the Data Protection Directive and the privacy and data protection legislation of the Member States in which they are operating. Furthermore, they will be subject to obligations under the General Data Protection Regulation when the European Commission enacts it. However, as described in Chapters 3 and 4, the applicability of these measures are dependent upon the types of data collected via the target of the mission and the equipment that is utilised. Some of the commercial applications were not focused on people and were unlikely to collect personal information, and had no associated scenario. This sub-chapter examines five specific scenarios, some of which may inadvertently and intentionally collect personal data.

### 8.2.1 Infrastructure inspection

As noted in Chapter 7, one of the most common current missions associated with RPAS is their use for infrastructure inspection. A typical scenario for such infrastructure inspections is the following:

*An RPAS operator is charged with inspecting a mobile phone tower in a rural location that provides mobile phone coverage to a few homes in the area and drivers on the near-by highway. The RPAS is fitted with a high-definition video camera, which the operator tests by scanning the landscape and taking a few close-up images of the base of the tower. Satisfied that the images are of sufficient quality for later analysis and can be enhanced to provide close-up footage of cracks or damage, the operator begins his inspection. As the RPAS ascends into the air, the operator circles the mast, moving steadily upwards. The video footage is focused on the mast, but the landscape behind the mast is visible in the shot as he makes his way around the mast and higher into the air. Although the operator and the mobile phone provider are not interested in the farms or vehicles in the background, (often blurry) images of these are*

*captured and included in the footage provided to the mobile phone company and saved in the RPAS operator's archives.*

This scenario may result in the collection of personal data about individuals living near the mast, individuals passing by and the employees who may be captured by the footage. While the footage of people may be restricted to “the tops of people’s heads”, once these images are contextualised by particular landmarks or other information, they may become identifiable. For example, if there is only one farm near a mast, and there is only one individual with brown hair who frequents the farm. In addition, individuals passing on the highway may be identifiable if the footage includes images of their number plates, which can be linked to their personal information. However, one industry respondent from the consultation exercises has pointed out that such background images are likely to be “blurry”. Nevertheless, the potential impacts are considered below.

The **privacy issues** associated with these usages of RPAS fall under the following broad categories – a chilling effect, dehumanisation of the surveilled, transparency and visibility, function creep, body privacy, privacy of location and space and privacy of association.

#### Chilling effect (medium risk)

The use of RPAS for infrastructure inspection may result in a situation whereby individuals who live near, travel past or encounter such infrastructure are unsure about whether an RPAS is in operation, or are unsure as to what a visible RPAS can see, whether it is recording and the purpose for which it is being used. This could lead individuals to adjust their behaviour as though they are under surveillance, even when they are not being monitored. These effects could be minimised by a public information campaign that provides information about what the RPAS is doing, when it will be operating and what it may record.

#### Dehumanisation of the surveilled (medium risk)

RPAS operators undertaking infrastructure inspections are not interested in the individuals on the ground. However, information about them may be captured inadvertently, and the very fact that the RPAS operator is not interested in these individuals may lead him/her to discount the potential impact of the RPAS operation on such individuals.

#### Transparency and visibility, accountability and voyeurism (high risk)

While a chilling effect indicates a change in behaviour, issues around transparency and accountability reflect a general discomfort. Thus, as noted above, there is a significant possibility that individuals on the ground may be unaware of what the RPAS is doing, what it is recording, who is operating it, etc. This could create significant discomfort and public backlash around the use of RPAS for such operations. There is also some risk that irresponsible operators could engage in voyeurism, given the capabilities of the cameras fitted onto the RPAS.

#### Function creep (high risk)

The risks for function creep are indicated as “high” for two reasons. First, the wide-spread use of RPAS for infrastructure inspection may “normalise” RPAS and result in a situation where RPAS are more common, are used for more intrusive operations and where individuals stop questioning their precise operators and functions. This could lead to widespread

infringements, particularly by irresponsible and/or private users. Second, while the operator of the RPAS is only interested in the infrastructure inspection, the communications company, as well as other clients, may be interested in the information that is captured in the background. This would, thus, expand the purpose for which the RPAS is being used, with potential effects on individuals on the ground (e.g., the workforce).

#### Body privacy (negligible risk)

RPAS being used for infrastructure are very unlikely to collect biometric or other information that could intrude on bodily privacy.

#### Privacy of location and space (low risk)

As noted above, RPAS operators undertaking infrastructure inspection are not interested in individuals on the ground. Therefore, they are unlikely to use the recording to attempt to identify individuals visible on the footage and what they are doing. However, as the operator, in this instance, is turning the footage over to the communications company, they may have an interest in identifying who is on the footage. Nevertheless, RPAS operators have pointed out that such images are likely to be blurry, and identification may be difficult.

#### Privacy of association (very low risk)

RPAS operators are very unlikely to be interested in the persons with whom individuals on the footage are meeting and the groups to which they may belong. There is some possibility that the communications company may be interested in this information, but as noted above, the quality of the footage is unlikely to yield any useful information.

In this scenario, personal data may be collected inadvertently through the normal operation of the RPAS when scanning the landscape to ensure the camera is working properly (if these images are recorded) and while capturing images of buildings, cars, etc. in the background during the mast inspection. While many of the images inadvertently captured in the background will be blurry (due to the focus on the mast), those familiar with the area and/or familiar with the individuals who may be in the vicinity may be able to identify them. For example, the communications company may be able to identify their own employees. As such, if persons or vehicles are captured on the footage, the data collected by the RPAS operator and stored by the operator and the communication company should be considered personal data because it can lead, either directly or indirectly, to the identification of those persons. Therefore, in relation to **data protection**, the scenario is associated the following risk levels:

#### Transparency (medium risk)

In the scenario above it is not clear whether the RPAS operator or the communications company has alerted individuals on the ground that personal data may be collected. Furthermore, it is not clear whether the RPAS itself has markings on it to identify the data collector. Finally, it is not clear whether individuals would be aware that both the RPAS operator and the communications company would store the collected data. These issues could be mitigated or addressed by alerting people in the vicinity of the mast that the RPAS operation is taking place, the type of data that will be collected, the purpose of the collection, how the data will be stored, used and/or processed and the right to object to the collection of

personal data. Details of the RPAS operator can also be provided as part of this process of informing the public.

#### Data minimisation (medium risk)

Although the images collected by the RPAS during the mast inspection are automatically blurred, due to the lens focusing on the mast, it is not clear whether the RPAS operator has taken specific steps to minimise the amount of data collected during the operation. Some opportunities for doing so would be to wait to begin recording until after the camera test, and to review the images to check whether individuals, vehicles or other identifying objects are visible in the background. If so, the operator could further blur the background images.

#### Proportionality (medium risk)

The proportionality issue was discussed at length during the 28 Feb 2014 consultation with data protection authorities, where a shortened version of this scenario was presented. Data protection authorities felt that it was certainly the case that a less intrusive technology could be used to collect the data in question, and that the use of an RPAS for this purpose might be disproportionate. Thus, alternative means of capturing this footage ought be considered, such as camera and vide footage taken from the ground. This would ensure that only images of the relevant infrastructure are recorded.

#### Purpose limitation (low risk)

As noted above, there is a small risk that the communications company may wish to process the data to monitor employee actions or for some other purpose not originally envisaged in the operation. This would not be the responsibility of the RPAS operator, however responsible practices, such as blurring of the images, by the RPAS operator could discourage such additional usages. However, if this is the case, employers need to decide the exact purpose of the data collection, prior to it taking place. This will minimise the risk of the footage being called upon at a later date to be used for company human relations purposes for example.

#### Consent (medium risk)

Individuals in the vicinity may not be aware that RPAS are in operation, and thus would not have the opportunity to consent to the collection of their personal data. While some may argue that the use of RPAS in public space, the use of CCTV in public space must be announced by signage, which is not possible with a mobile technology such as RPAS. Furthermore, although some may argue that RPAS information collection is similar to information collection via helicopters, helicopters have a clear auditory signal that they are approaching. In order to reduce risks around consent, RPAS operators must find ways of alerting the public that such information collection is taking place, so that they may give consent, or alternatively, object to the collection of their personal data. In this situation, where no sensitive data is collected, such consent could be implicitly gained through notifications suggested under transparency.

#### Accountability (medium risk)

Related to issues of transparency and consent is the issue of accountability. RPAS operators who collect personal data must be accountable to individuals who wish to exercise their rights

as well as regulators who may wish to enquire about or investigate data. If RPAS operators do not meet their transparency obligations, then it is also difficult for them to meet their accountability obligations. Since, in the scenario above, it was unclear whether the RPAS operator had informed nearby individuals that the filming would be taking place, it would be difficult for third parties to hold the operator accountable for his actions. The accountability principle could also be met by RPAS operators affixing a company logo to the RPAS, as well as including the contact details or the name of the RPAS operator on signage in the areas near whether the RPAS operation will be conducted.

#### Data security (low risk)

It is unlikely that third parties could access the data collected. However, it is important for RPAS operators to store any personal data they collect in a secure manner, and to ensure that it is not stored for excessive lengths of time. Anonymisation of the data could assist RPAS operators in meeting this obligation.

#### Third country transfers (low risk)

It is unlikely that the RPAS operator, in this scenario, would be transferring personal data outside of the European Union. However, if this were the case, the RPAS operator would be restricted from sending footage that included personal data to countries that have “adequate” data protection regimes. Or through contractual agreements that accord with the contract derogation at Article 26 of the Data Protection Directive or the national or state equivalent law.

#### Rights of access, correction and erasure (medium risk)

Given the interplay between transparency, consent and accountability, the ability of individuals to exercise their rights of access, correction and erasure also represent a medium risk. It is possible that personal information will be collected in this scenario, and individuals have a right to access that material and to request that the data controller delete that material (although this right is not absolute). However, if individuals are not aware who is operating the RPAS, then it is nearly impossible for them to be able to exercise this right. Adequately addressing transparency and accountability as detailed above would be a necessary step forward in meeting this obligation.

The data protection analysis of this scenario indicates that there are some relatively significant risks to data protection when using RPAS to inspect infrastructure. However, many of these risks can be mitigated and addressed though taking transparency seriously and mobilising privacy enhancing features, such as blurring images, or data minimisation practices, such as only recording operational information.

Finally, in addition to these privacy and data protection issues, **ethical issues** such as safety, public dissatisfaction and discriminatory targeting pose some risk in this scenario. In general, these are relatively low risks, because the RPAS is operating in a rural area and the operation is not focused on people. However, the operation does contribute to a general proliferation of RPAS, which may be viewed negatively by the public.

### Safety (low risk)

The operation is occurring in a rural area, and therefore, it is unlikely that the operation poses a significant risk to people or animals. There is no information to indicate that the RPAS operation is noisy, frequent or may negatively impact the environment in terms of noise pollution or by disturbing wildlife excessively. Any damage caused by a crash would likely impact the infrastructure being inspected.

### Public dissatisfaction (medium risk)

As with any RPAS operation, the use of RPAS for infrastructure inspection may contribute to members of the public feeling “over-run” by RPAS, particularly when RPAS used for other missions do collect personal data, or when RPAS used by private individuals result in privacy breaches that are difficult to prevent or prosecute. Transparency and responsible operation can mitigate this potential ethical issue.

### Discriminatory targeting (low risk)

There is a small possibility that people in rural locations, who are spread out, may have difficulty voicing their discomfort over the use of RPAS near their homes. This may be exacerbated if these individuals are economically disadvantaged. RPAS operators could mitigate this through awareness raising, transparency and through taking seriously any issues raised by residents, no matter how small the number.

The use of RPAS for infrastructure inspection is associated with relatively few serious privacy, data protection and ethical risks. These missions are focused on objects, rather than people, and may only collect personal information inadvertently or in unusual circumstances. Furthermore, commercial operators are largely viewed as “trustworthy” users of RPAS by DPAs and civil society organisations, as noted in Chapter 6. However, it is important that RPAS operators educate themselves and members of the public about their use of RPAS and the images they collect, and provide specific information about when RPAS are being used and the purpose for which they are being used. RPAS operators should also consider privacy enhancement and data minimisation practices like blurring irrelevant images or limiting their recording to images essential for the mission. These simple activities will assist RPAS operators in meeting privacy expectations, meeting data protection obligations (where they collect personal information) and meeting ethical standards, particularly in combatting public discomfort with RPAS.

### *8.2.2 Other visual services*

As noted in Chapter 7 and above, infrastructure inspection is largely focused on an object or piece of property but may collect images of people inadvertently. Other visual services, which use the same payloads and technologies as infrastructure inspection, are being commissioned in situations that are very likely to collect images of people or personal data. These may include services such as real estate showcasing, stock image production and the production of footage for publicity purposes.

*An RPAS operator is contracted by a real estate company to make a video showcasing a home for sale. The operator flies about 200m above the house, filming the building, the land included with the sale and the immediate surrounding neighbourhood. The left neighbour’s car and toys in their back yard are clearly visible, as is the right-side neighbour walking from her front door*

*to her car. The RPAS operator transfers the footage to the real estate client and does not keep a copy.*

In this scenario, the RPAS operator is in a similar position to the infrastructure inspection scenario whereby the operator is not concerned about the neighbours or capturing footage of individuals on the ground. Instead, the operator is quite focused on the house that is for sale. However, due to the fact that this operation is occurring in a residential area, and will include footage of neighbours and their property, it raises more significant risks than the infrastructure inspection scenario. Specifically, the footage includes images and location information for identifiable individuals and their vehicles, as well as information about their homes, belongings and behaviours. As such, the operator has a clear obligation to reduce the risks to privacy and personal data of the people and private properties that may be captured on the footage, and the operator has a clear obligation to meet the data protection requirements associated with the collection and processing of these images. However, the fact that the RPAS operator does not keep a copy of the footage means that the operator is only liable for the risks associated with the collection and processing of the data in question.

The **privacy issues** associated with this usage of RPAS falls under the following broad categories – a chilling effect, dehumanisation of the surveilled, transparency and visibility, function creep, body privacy, privacy of location and space and privacy of association.

#### Chilling effect (medium risk)

The use of RPAS for real estate showcasing may result in a situation whereby individuals who live in the immediate homes and streets are unsure about whether an RPAS is in operation, or are unsure as to what a visible RPAS can see, whether it is recording and the purpose for which it is being used. This could lead individuals to adjust their behaviour as though they are under surveillance, even when they are not being monitored. These effects could be minimised by the RPAS operator, in partnership with the real estate company, providing information about what the RPAS is doing, when it will be operating and what it may record.

#### Dehumanisation of the surveilled (high risk)

RPAS operators undertaking this real estate filming are not interested in the individuals on the ground or their property (although they may be interested in showcasing the immediate neighbourhood and scenery). However, in this scenario information about neighbours was captured inadvertently, and the private spaces and personal property belonging to the neighbours was also included in the footage. As such, it seems that in this scenario, the RPAS operator has discounted the potential impact of the RPAS operation on these individuals.

#### Transparency and visibility, accountability and voyeurism (high risk)

In this scenario, there is a significant possibility that individuals on the ground may be unaware of what the RPAS is doing, what it is recording, who is operating it, etc. This could create significant discomfort and public backlash around the use of RPAS for such operations, which is augmented by the fact that the RPAS is collecting information about private spaces and property. There is also some risk that irresponsible operators could engage in voyeurism, given the capabilities of the cameras fitted onto the RPAS.

### Function creep (medium risk)

In addition to the issues associated with a generalised proliferation of RPAS, this scenario raises significant issues related to function creep in relation to secondary use of the footage. Specifically, if such footage was made generally available on the Internet, there is a risk that the footage could be used to “scope out” neighbourhoods to identify targets for theft. This is particularly the case where vehicles and other property are visible on the footage alongside location information. Although this is quite similar to mapping programmes such as Google Street View, Google takes steps to prevent the filming of purely residential neighbourhoods and is a recognised entity to whom individuals can apply to ensure that footage relating to them is removed or blurred. There is no indication here that such transparency and accountability measures have taken place.

### Body privacy (negligible risk)

RPAS being used for such purposes are not collecting biometric or other information that could intrude on bodily privacy.

### Privacy of location and space (high risk)

In this scenario, there is a significant intrusion on privacy of location and space in that individuals’ private spaces (e.g., yards and gardens) are being captured by the footage. Furthermore, the footage also makes it possible to link people with particular places at particular times or to link people with particular addresses. In order to mitigate this, operators should limit their collection of data about the other homes and surrounding area, or blur this footage immediately upon processing the data in order to mitigate this risk.

### Privacy of association (medium risk)

RPAS operators are unlikely to be interested in the persons with whom individuals on the footage are meeting and the groups to which they may belong. However, the footage may indicate the number of adults living in a house (based on the number of vehicles) the relationships between those people (e.g., family groups) and other information about those individuals. This represents a clear intrusion on privacy of association.

In this scenario, there are clear risks to privacy, including high risks associated with a dehumanisation of the surveilled, transparency and voyeurism and privacy of location and space. Limiting or minimising the amount of data collected about the people and properties near the home that is for sale could significantly reduce these risks. This may include flying at a lower altitude to ensure less background data is collected, anonymising particular pieces of property that can be linked to specific individuals (e.g., vehicle number plates or images) and also blurring images captured in the background.

In addition to these privacy risks, there are clear risks associated with the **protection of the personal data** in this scenario. Furthermore, this scenario indicates a situation where *RPAS operators are legally obligated to address the following data protection issues* as they are very likely to collect and process personal data.

### Transparency (medium risk)

In this scenario transparency emerges as a key issue as it is not mentioned whether individuals in the surrounding area have been notified about the collection of visual images. In this respect, both the RPAS operator and the real estate company should work together to ensure that people in the surrounding area are informed that such images of themselves and their property may be collected. This could be achieved by a letterbox drop to the neighbouring properties that might be included in the footage. While the real estate company would be obligated to inform individuals about what they plan to do with the data, the fact that the images are not stored by the operator at all mean that the operator is not responsible for ensuring that this information is provided.

### Data minimisation (high risk)

This scenario clearly involves the collection of images that are extraneous for the purpose of showcasing the property in question. Images of neighbours, their homes and their property are clearly outside the scope of this mission. Furthermore it does not appear that the RPAS operator has taken or plans to take any steps, such as blurring, anonymisation, etc. to minimise the amount of personal data collected. Some opportunities for doing so would be to wait to begin recording until the RPAS is in place, and to edit the images to ensure that no people, vehicles or other identifying objects are visible in the background. However, the fact that the RPAS operator does not store a copy of the data is a useful data minimisation feature.

### Proportionality (high risk)

In this scenario it seems clear that a less intrusive technology (e.g., still camera footage from the ground) could be used to collect the data in question, and that the use of an RPAS for this purpose might be disproportionate. Although the still image capture would not give the “bird’s eye view” of the property that the RPAS offers, this vantage point introduces unnecessary risks to the RPAS operator and the real estate company in terms of liability and obligations. Furthermore, it also introduces unnecessary risks to people on the ground.

### Purpose limitation (low risk)

As noted above, there is a small risk that if the footage is posted on the Internet that it could be used for other purposes. However, this issue is not necessarily the responsibility of the RPAS operator in this scenario. Nevertheless, to protect themselves, RPAS operators should consider how these images could be utilised for other purposes and take steps to reduce this risk and discourage additional uses (e.g., anonymisation, data minimisation, etc.).

### Consent (high risk)

There is no indication in this scenario that individuals on the ground were informed about the collection of data in this instance. It is the responsibility of the RPAS operator and the real estate company to describe what data is likely to be collected and how individuals can opt out of this information collection. One possibility is to distribute fliers describing the time and date of the filming, the information likely to be collected and the contact information for the RPAS operator and real estate company in order to allow individuals to contact either organisation and opt out.

### Accountability (medium risk)

In this scenario, it is not certain whether the real estate agent or the RPAS operator have informed the neighbours of the intended RPAS operation. It is also not certain whether the RPAS is fitted with any identifying information, such as a company name, in the event that concerned neighbours wish to contact the company about the RPAS operation. Without transparency or obtaining consent from residents and neighbours of the area, it is almost impossible for the RPAS operator to meet his obligations around accountability. RPAS operators who collect personal data must be accountable to individuals who wish to exercise their rights as well as regulators who may wish to enquire about or investigate data. Since, in the scenario above, it was unclear whether the RPAS operator had informed nearby individuals that the filming would be taking place, it would be difficult for third parties to hold the operator accountable for his actions.

### Data security (low risk)

It is unlikely that the data collected in this scenario could be accessed by third parties. However, it is important for RPAS operators to store any personal data they collect in a secure manner, and to ensure that it is not stored for excessive lengths of time. Anonymisation of the data could assist RPAS operators in meeting this obligation. In this scenario, the operator could blur the images of people inadvertently caught on the footage, as well as all house numbers and car registration and plate numbers.

### Third country transfers (low risk)

It is unlikely that the RPAS operator, in this scenario, would be transferring personal data outside of the European Union. However, if this were the case, the RPAS operator would be restricted from sending footage that included personal data to countries that have “adequate” data protection regimes. Or through contractual agreements that accord with the contract derogation at Article 26 of the Data Protection Directive or the national or state equivalent law.

### Rights of access, correction and erasure (medium)

Given the interplay between transparency, consent and accountability, the ability of individuals to exercise their rights of access, correction and erasure also represent a medium to high-level risk. It is possible that personal information will be collected in this scenario, but that they may be aware of who to contact should they wish to request that the data controller delete that material. Adequately addressing transparency and accountability would be a necessary step forward in meeting this obligation.

Therefore, RPAS operators may potentially breach a number of requirements of the data protection framework by failing to observe a number of the data protection principles. RPAS operators are at a high risk of compromising the principles of data minimisation, proportionality and consent. There is also some risk that RPAS operators may breach the related principles of transparency, accountability and rights of access, correction and erasure, there is less risk of this occurring during this scenario, and even less risk that the principles of data security and third party transfers will be compromised.

In addition to these privacy and data protection issues, **ethical issues such** as safety, public dissatisfaction and discriminatory targeting pose some risk in this scenario. In general, these are low to medium risks, as the operation is not focussed on people. However, the operation could inadvertently jeopardise the safety of property or local residents, but only to the extent that the equipment malfunctions. However, the operation does contribute to a general proliferation of RPAS, which may be viewed negatively by the public, especially as this operation is undertaken in a residential area comprising private properties.

#### Safety (medium risk)

There is a medium risk to safety because the operator flies at 200m above buildings, the neighbours inadvertently captured in the footage, and other items around the home, including the car and toys. However, damage is only likely to occur if the RPAS malfunctions. Whilst the scenario does not raise any noise related issues, such as noise pollution, any noise from the RPAS flying at such a low height could pose a risk of noise pollution.

#### Public dissatisfaction (medium risk)

Due to the relative nearness of the drone to the house and the neighbouring house, there is an increased risk of public dissatisfaction in drone use. This is especially so, if residents feel that they are under surveillance (even though they are not), and/ or if the operation causes noise pollution or other disturbance. The level of risk of public dissatisfaction is increased in this scenario because this is a residential area comprising private properties, and as such residents of this neighbourhood are likely to consider this area their personal living space. RPAS could be of nuisance, or cause discomfort in residents who fear their privacy is being violated.

#### Discriminatory targeting (low risk)

It is not clear from the facts of the scenario whether the RPAS is being operated in a marginalised or disadvantaged area where residents may feel less secure in coming in forward about their concerns. From the facts of the scenario, it seems more likely that it is in a suburban setting.

Therefore, this scenario does not present any serious ethical risks. Nonetheless, the operators must still inform the residents and surrounding neighbours of the operation. They must also operate with great caution given the close proximity to objects and people, not only so as not to be of nuisance, but to ensure that they do not inflict any damage to the property, objects around the property and neighbouring properties, and importantly, people that may be appear unpredictably.

Overall, the use of RPAS in this situation presents some risks to privacy, data protection and ethical risks. However, these are not serious risks as the operation is focussed on real estate, and the surrounding land, rather than people. Further, commercial operators tend to be considered as “trustworthy” users of RPAS by DPAs and civil society organisations, as noted in Chapter 6. Nevertheless, there is a low to medium chance that this operation could impact unintentionally or indirectly upon civilian rights and values, especially as individuals are inadvertently captured in the footage, as are their homes and other neighbourhood characteristics that could lead to the identification of residents. However, these risks can be minimised by the real estate agency and the RPAS operator notifying the residents of the intended operation in advance. They could also inform residents of the purpose of the operation, the images to be captured, and the subsequent use of the footage. The agency and

the operator could also make the images of individuals unidentifiable by blurring them, and doing the same with any house numbers or car number plates. Alternatively, the RPAS operator could erase the footage of the individuals that was inadvertently captured, as this footage is not imperative to the overall operation. Such steps are significant in reducing the risk to privacy, data protection rights and ethical values. This proactive approach is more favourable than the operator simply relying on an intention not to retain a copy of the footage, as the scenario stipulates.

*The organisers of an outdoor concert have contracted a drone operator to fly above the concert taking footage of people in the crowd enjoying themselves. Attendees of the event were informed of the filming via a short notification in the terms and conditions statement when they bought their tickets online.*

In this scenario, the RPAS operator is concerned primarily with capturing footage of individuals and as a result raises a number of concerns relating to privacy, data protection and ethical values. Specifically, the footage includes images and location information for identifiable individuals as well as information about their social behaviours and associations. However, due to the fact that this operation is occurring in a public space, and the attendees have been notified prior to their attendance at the concert, these risks are reduced somewhat by the operator discharging some of their obligations and data protection requirements to reduce the risks to privacy and personal data of the people at the concert. However, the extent to which the footage will be used, whether the operator and the organisers intend on keeping a copy of the footage are not presented in this scenario, but if this is the case, then the risks are increased.

The **privacy issues** associated with this usage of RPAS falls under the following broad categories – a chilling effect, dehumanisation of the surveilled, transparency and visibility, function creep, body privacy, privacy of location and space and privacy of association.

#### Chilling effect (low risk)

The use of RPAS at an outdoor concert when attendees have been notified of there being RPAS in operation, results in a situation whereby individuals are aware that their actions are potentially being captured, although they may not know at what specific moment, they will be captured, or the length of the footage of them will be. Thus, there is a low risk of attendees adjusting their behaviour. This risk may only slightly increase due to attendees not being aware of the exact moments they will be captured or for what duration. Whilst, the operator and the organisers have notified the attendees on their tickets, they could also display signs at the entrance to the concert in the event attendees have not read the terms and conditions of the ticket. This step by the organisers and the operator would ensure that any risk of chilling effect would remain low.

#### Dehumanisation of the surveilled (medium risk)

RPAS operators undertaking filming at the outdoor concert are specifically interested in filming the individuals in attendance, although they may only be interested in showcasing how enjoyable the event is. As such, it seems that in this scenario, the RPAS operator may not completely discount the potential impact of the RPAS operation on these individuals. This is because the operators are focussed solely on images of enjoyment. However, in doing so, there is a medium risk that they may not be sufficiently mindful of other experiences by attendees at the outdoor concert, such as emotional or violent behaviour.

### Transparency and visibility, accountability and voyeurism (low risk)

In this scenario, individuals on the ground are more likely than not to be aware of what the RPAS is doing, what it is recording, who is operating it, etc. This is unlikely to create any significant discomfort on part of the attendees (at least those who have read the terms and conditions on the tickets), and/ or any significant public backlash around the use of RPAS for such operations. However, this risk would be further minimised if the event organisers also posted signs before the entrance to the concert and around the concert grounds to ensure full transparency of the operation. In addition there is some risk that irresponsible operators could engage in voyeurism, given the capabilities of the cameras fitted onto the RPAS, and given that this is a fairly liberal social occasion that presents a number of different image options.

### Function creep (medium risk)

In addition to the issues associated with a generalised proliferation of RPAS, this scenario raises issues related to function creep in relation to secondary use of the footage. Specifically, if such footage was made generally available on the Internet, which is likely if it is used for advertising purposes by the organisers, there is a risk that the footage could be re-used and shared in relation to similar concerts for advertising purposes or otherwise.

### Body privacy (negligible risk)

RPAS being used for such purposes are not collecting biometric or other information that could intrude on bodily privacy.

### Privacy of location and space (low risk)

In this scenario, there is no real risk of intrusion on privacy of location and space in that individuals' are captured in a public space. The only risk that rises in this regard is because the footage could make it possible to link people with the concert venue for on a particular date and time. The operators should mitigate this low risk by keeping the scope of the footage general and at a distance, and by not targeting certain individuals more closely than others or for an extended period of time.

### Privacy of association (medium risk)

RPAS operators are unlikely to be interested in the persons with whom individuals on the footage are meeting and the groups to which they may belong. However, the footage can directly link individuals to their social preferences, such as type of music and the company they keep whilst in attendance, including their relationships and friendships. This represents the potential for an intrusion on privacy of association. This risk may be decreased subject to the specific footage that is recorded, the details of which are not provided in the scenario.

In this scenario, there are some risks to privacy, although for the most part, they are medium or low-level risks. The main risk is to privacy of association, although the attendees are made aware of the intended RPAS operation prior to the concert, so they can elect not to attend. Limiting or minimising the detail of images and the duration of images of individuals could significantly reduce any risks. This may include flying at a higher altitude to ensure less focussed data is collected.

In addition to these privacy risks, there are clear risks associated with the **protection of the personal data** in this scenario. Furthermore, this scenario indicates a situation where *RPAS operators are legally obligated to address the following data protection issues* as they intend to collect and process personal data.

#### Transparency (medium risk)

In this scenario, the organisers have attempted to meet the requirement for transparency by notifying attendees at the concert of the RPAS operation by way of including it on the terms and conditions of the ticket. However, the extent to which the organisers have notified the attendees is not clear, and nor is the level of detail of the operation provided in the terms and conditions. The purpose of the footage is to capture images of individuals enjoying themselves, which might include up close images of individuals smiling and dancing, which would make them clearly identifiable. Thus, it is very important that the event organisers meet their transparency obligation. Further, it is also unlikely that all attendees have read the terms and conditions, or noticed that specific term if it is buried amidst a long list of other terms and conditions. Thus, it could be better practice to also erect signage before entrance to event, as well as throughout the event in an effort to achieve greater transparency. This signage, and the terms and conditions, should also detail the purpose of the operation, the intended use of the footage, the contact details for the RPAS operator etc. Nevertheless, the organisers have taken a sound step towards transparency in this scenario by including the operation in the terms and conditions.

#### Data minimisation (low to medium risk)

This scenario involves the collection of images that display individuals enjoying themselves at the event. There is no additional motivation or purpose for the data collection in this scenario. The scenario does not indicate that any extraneous data will be collected. It is also likely that the concert venue is outside of a residential zone, and as such, footage is unlikely to inadvertently capture images of houses or identifying objects such as car registration numbers etc. However, there is no indication that the footage of individuals would be minimised by blurring images or any other anonymisation techniques would be employed. We are not sure whether the operator of the RPAS will store a copy of the footage, but if they do not, this will assist in meeting the data minimisation principle.

#### Proportionality (medium risk)

In this scenario, the goal of capturing individuals enjoying themselves at the concert could be achieved by using less intrusive and technology and more overt means (e.g., still camera footage from the ground). In that sense, the use of RPAS could be considered disproportionate. Although the still image capture would not give the “bird’s eye view” of the event that RPAS offers, which would be useful for promotional purposes such as advertising. However, this vantage point introduces unnecessary risks to the RPAS operator and concert organisers in terms of liability and obligations, as well as introducing unnecessary risks to people on the ground. However, these risks are reduced due to the fact that the organiser and operator have attempted to notify the attendees of the operation.

#### Purpose limitation (medium to high risk)

As noted above, there is a medium to high risk that the footage will be posted on the Internet for purposes other than the initial purpose of the collection. It is likely that the footage will be

posted online for promotional or advertising purposes, as the object of the footage is to show attendees enjoying the concert. In this age of social media, it is highly likely that the footage will be shared by either attendees at the concert or by others interested in the concert. Irrespective of the organiser notifying the attendees of the RPAS operation, they are still required to consider ways in which they could limit the potential use of the footage, by themselves or others, that do not accord with the initial purpose of collection. For example, organisers could consider how they might discourage subsequent use and sharing of the footage, especially through minimisation.

#### Consent (medium risk)

Individuals in attendance at the concert have been informed about the collection of data by its inclusion as a term and condition of entry to the event. However, this raises the complexities associated the issue of consent. We have very little information pertaining to the scope of the term included on the ticket, or indeed how visible it is. This complexity is compounded by the fact that not all attendees are likely to have read the terms and conditions in detail, and even if they had, they may only object to the data collection by not attending the concert. Further, attendees had likely already paid and committed to attendance prior to be resented with the ticket. Alternatively, the terms and conditions may have been presented to them online before agreeing to purchase the ticket. In that event, consent is still considered a grey area. It is the responsibility of the RPAS operator and the concert organiser to describe what data is likely to be collected and how individuals can opt out of this information collection. This is unlikely to have been met, unless they perhaps detailed this information immediately prior to purchase. As mentioned, one possibility is to have notified the purchasers prior to the transaction of the RPAS operation so that they could make informed decision about going ahead with their purchase. Alternatively, the terms and conditions could provide the option to opt-out or be given a refund should they not wish to attend the concert upon knowledge of the RPAS operation. However, the degree of risk presented here is subject to whether the attendees were notified prior to their purchase or whether first notification occurred after they had purchased the ticket, which would thereby invalidate consent.

#### Accountability (low risk)

There is a low risk that the RPAS operator (or vent organiser) would not meet their accountability requirement. This is because they have purported to notify the individuals attending the concert of the proposed data collection. However, without specific details of the RPAS operator, individuals would have to first contact the event organiser for the contact details f the RPAS operator. Alternatively, the RPAS could display some identifiers such as company logo. Alternatively, the event organisers could include those details on signage at the venue that reads, for example, “footage will be obtained through the use of a RPAS by .....”. Further, accountability and transparency are inextricably linked and thus, the RPAS operator will meet the accountability requirement to the extent that they meet the transparency requirement, thereby enabling third parties to hold the operator accountable for their actions.

#### Data security (low risk)

It is unlikely that the data collected would be accessed by third parties. However, it is important for RPAS operators to store any personal data they collect in a secure manner, and to ensure that it is not stored for excessive lengths of time.

### Third country transfers (medium risk)

It is not certain whether the RPAS operator or the concert organiser, in this scenario, would be transferring personal data outside of the European Union. However, it seems likely that this data could be transferred to other countries, especially if the event organisers are wishing to draw attention to their concert or promote it abroad. If this is the case, they would be restricted from sending footage that included personal data to countries that do not have “adequate” data protection regimes as assessed by the European Commission. However, this requirement can be derogated from by contractual agreements that accord with the contract derogation at Article 26 of the Data Protection Directive or the national or state equivalent law.

### Rights of access, correction and erasure (high risk)

Given the interplay between transparency, consent and accountability, the ability of individuals to exercise their rights of access, correction and erasure also represent a medium to high risk. Personal data will undoubtedly be collected, and it is not certain whether the consent requirement will be fulfilled. The facts of this scenario do not elaborate on what information is included in the terms and conditions that purport to notify the attendees of the RPAS operation. However, it is not practicable for the footage to be accessed by each and every individual in attendance at the concert following the event and before the footage is distributed, especially as this appears to be part of a commercial activity. Attendees with knowledge of their rights under the data protection directive and mirroring national laws may attempt to obtain access to the footage and request that they be deleted, but otherwise, there is no information that this requirement has been met. However, individuals have the contact details of the event organisers, so they have some chance of being able to enforce their rights. Nevertheless, from the facts of the scenario, it appears unlikely that individuals be able to enforce this right. However, adequately addressing the principles of transparency and consent would be a necessary step forward in meeting this obligation.

Therefore, the RPAS operator and concert organisers may potentially breach a number of requirements of the data protection framework by failing to observe a number of the data protection principles. RPAS operators are at a medium or a medium to high risk of compromising the principles of transparency, proportionality, purpose limitation, third country transfers, consent and the rights of access, correction and erasures respectively. There is less risk of a breach of data security and data minimisation presented by this scenario. However, this depends largely upon the extent of transparency, and consent.

In addition to these privacy and data protection issues, **ethical issues** such as safety, public dissatisfaction and discriminatory targeting pose a medium or medium to high risk in this scenario. In general, these risks are increased because the RPAS operation is being conducted at a crowded event, and the operation is specifically focussed on people. The operation in this scenario also contribute to a general proliferation of RPAS, which may be viewed negatively by the public, especially as this is a social event, at which attendees are presumably wishing to feel a sense of freedom to enjoy themselves.

### Safety (medium to high risk)

It is not certain at what altitude the RPAS will fly, which makes it difficult to assess the degrees of risk to safety in terms of actual physical or property damage, or other negative impacts such as noise pollution. In this scenario, it is likely that the RPAS will fly at low

range in order to capture individuals enjoying themselves. If this is the case, the risk to safety is high. In addition to the potential to damage property, such as staging and lighting and other electrical equipment that is positioned a height, attendees may also be disrupted due to noise pollution. On the other hand, if the RPAS operates from a greater height to capture a “bird’s eye view” of the concert, then the risk to safety is reduced. Of course, if the RPAS was to malfunction and drop from the sky, then damage is likely inevitable in the context of a crowded public event.

#### Public dissatisfaction (high risk)

Due to the presence of the RPAS at the concert (and subject to the closeness in proximity of the RPAS to the attendees), there is a significant risk of public dissatisfaction in drone use. The operation could disrupt the attendees’ enjoyment at the concert, and they are likely to consider RPAS use to be a nuisance or cause agitation about the potential violation of privacy rights.

#### Discriminatory targeting (low risk)

This scenario does not specify whether the concert is a regular type of occasion where notable musicians are playing, or whether it is a concert in support of a cause or in the promotion of rights. The risk of discriminatory targeting occurring is subject to those facts. For example, a regular music concert that is open to all is less likely to cause risk of discriminatory targeting. On the other hand, if this is a concert aimed a cause or in relation t raising awareness about marginalised groups or minorities, then there is an increased risk of discriminatory targeting. This is because the latter group may feel more targeted by the RPAS operation and less secure in objecting to the RPAS operation.

Therefore, ethical risks such as safety, public dissatisfaction and discriminatory targeting arise in relation to this situation where the primary aim of the RPAS operation is to capture individuals. However, these risks can be mitigated when the RPAS operator takes steps to reduce any noise or physical disruption caused by the presence of RPAS at the concert.

Overall, the privacy, data protection and ethical risks associated with the use of RPAS in this situation are increased due to the fact that the purpose of the operation is to capture images of individuals, which amounts to personal data under the data protection framework. Although the organiser has taken a valuable step in minimising these risks by purporting to notify attendees of the RPAS operation by including it in the terms and conditions of the tickets, the event organisers and the RPAS operator are required to take additional steps to reduce the threat of privacy and ethical risks and meet their obligations under the data protection framework. Additional steps would be to ensure that attendees are better informed of the intended RPAS operation prior to purchasing the ticket so that they may provide informed consent or assess whether they wish to be captured on the footage. The organiser and RPAS operator could also focus on achieving greater transparency and accountability, as well as minimising other associated risks, by clearly signing the event before the entrance and throughout the grounds. Recommended signage would include detail about the purpose of the collection, the intended use and manner in which the data will be secured, as well as the contact details of the RPAS operator. The attendees must also be given the right to access, correct and erase the personal data collected during this operation. Such steps are significant in reducing the risk to privacy, data protection rights and ethical values.

*A commercial RPAS operator flies high over a historical city taking footage of various landmarks. The footage focuses in on the ruins of a castle, a park and the picturesque marina. Because of the height of the RPAS, the images of the people on film appear to be unidentifiable. The RPAS operator sells the image to a stock image database/catalogue, where it is stored indefinitely and made available for purchase by other entities.*

This scenario results in the collection of data about individuals living, working, or simply being near the castle, and the marina at the time of filming. However, whether it amounts to personal data is disputable on the basis that the individuals captured in the footage are said to be unidentifiable. Nevertheless, once these images are contextualised by particular landmarks or other information, or are capable of being zoomed in, individuals may become identifiable. For example, if there is only one other house located near the castle and only one blonde person that frequents that house, or if there is a particularly notable boat moored at the marina that can be connected to a certain individual. In addition, individuals driving through the city may be identifiable if the footage includes images of their number plates, which can be linked to their personal information. Although these images are likely to be blurry, and said to be unidentifiable, it is still important to consider the potential impacts below.

**The privacy issues** associated with these usages of RPAS fall under the following broad categories – a chilling effect, dehumanisation of the surveilled, transparency and visibility, function creep, body privacy, privacy of location and space and privacy of association.

#### Chilling effect (medium risk)

The use of RPAS for capturing footage of the historical city, the castle ruins and the marina may result in a situation whereby individuals who live near, travel past or encounter these sights are unsure about whether an RPAS is in operation, or are unsure as to what a visible RPAS can see, whether it is recording and the purpose for which it is being used. It is uncertain whether the RPAS is detectable, i.e., whether it can be seen or heard from the ground. If individuals are unsure whether RPAS is in operation, individuals might adjust their behaviour as though they are under surveillance, even when they are not being monitored. These effects could be minimised by a public information campaign that provides information about what the RPAS is doing, when it will be operating and what it may record.

#### Dehumanisation of the surveilled (low risk)

The RPAS operator in this scenario is not interested in the individuals on the ground. However, information about them may be captured inadvertently, and the very fact that the RPAS operator is not interested in these individuals may lead him/her to discount the potential impact of the RPAS operation on such individuals.

#### Transparency and visibility, accountability and voyeurism (medium risk)

While a chilling effect indicates a change in behaviour, issues around transparency and accountability reflect a general discomfort. Thus, as noted above, there is a significant possibility that individuals on the ground may be unaware of what the RPAS is doing, what it is recording, who is operating it, etc. This could create significant discomfort and public backlash around the use of RPAS for such operations. There is also some risk that irresponsible operators could engage in voyeurism, given the capabilities of the cameras fitted onto the RPAS. As mentioned above, these implications could be minimised by a public information campaign.

### Function creep (medium to high risk)

The risks for function creep are indicated as “medium to high” for two reasons. First, the wide-spread use of RPAS for capturing culturally or historically relevant material may “normalise” RPAS and result in a situation where RPAS are more common, are used for more intrusive operations and where individuals stop questioning their precise operators and functions. This could lead to widespread infringements, particularly by irresponsible and/or private users. Second, while the operator of the RPAS is only interested in city structures, the castle ruins and the marina, the fact that that the footage is sold to a stock image database/catalogue, where it is stored indefinitely and made available for purchase by other entities, without any apparent restriction, can have potential effects on individuals captured in the footage.

### Body privacy (negligible risk)

RPAS being used to capture this footage are very unlikely to collect biometric or other information that could intrude on bodily privacy.

### Privacy of location and space (low risk)

As noted above, the RPAS operator in this scenario is not interested in individuals on the ground. Therefore, they are unlikely to use the recording to attempt to identify individuals visible on the footage, what they are doing or who they associate with. However, as the operator, in this instance, is selling the footage to a stock image database/catalogue for further sale, subsequent users of the footage may have an interest in identifying who is on the footage. Nevertheless, this scenario stipulates that individuals are unidentifiable.

### Privacy of association (very low risk)

RPAS operators are very unlikely to be interested in the persons with whom individuals on the footage are meeting and the groups to which they may belong. There is some possibility that individuals or companies who purchase the images from the stock image database/catalogue would be interested in this information, but the chance of this is slim. Further, the quality of the footage in relation to individuals is blurry and unlikely to yield any useful information.

Overall, in this scenario, personal data may be collected inadvertently through the normal operation of the RPAS when scanning the historical city, the castle ruins and the picturesque marina. While individuals captured in this footage are said to be unidentifiable, those familiar with the area and/or familiar with the individuals who may be in the vicinity may be able to identify them, but this is only likely if they are able to zoom in the images. For example, a yacht club at the marina may be able to identify their employees, but only with great effort. Nevertheless, if persons or vehicles are captured on the footage, the data collected by the RPAS operator and stored by the operator and by the owner of the stock image database/catalogue should consider these aspects of the footage to be personal data, that could, however slight a chance, lead, either directly or indirectly, to the identification of those persons. Therefore, in relation to **data protection**, the scenario is associated the following risk levels:

### Transparency (medium to high risk)

In the scenario above it is not clear whether the RPAS operator has alerted individuals on the ground that personal data may be collected. Furthermore, it is not clear whether the RPAS itself has markings on it to identify the data collector. Finally, it is not clear whether individuals would be aware that both the RPAS operator and the communications company would store the collected data. These issues could be mitigated or addressed by alerting people in the vicinity of the castle ruins and the marina that the RPAS operation is taking place, the type of data that will be collected, the purpose of the collection, how the data will be stored, used and/or processed and the right to object to the collection of personal data.

### Data minimisation (medium risk)

The images collected by the RPAS in this scenario, where the RPAS is operated at a great height, renders individuals unidentifiable. However, it is unclear whether the RPAS operator has taken specific steps to minimise the amount of data collected during the operation. A measure that the RPAS operator could take to achieve this minimisation is to review the images to check whether individuals, vehicles or other identifying objects are visible, through zoom or otherwise. If so, the operator could blur the images of individuals.

### Proportionality (medium risk)

There is a medium risk to the proportionality principle because the RPAS is operated from a great height. Although it is arguable that a less intrusive technology could be used to capture the images of the city, the castle ruins and the marina, the RPAS operator may specifically require this type of image that gives a “bird’s eye view” of the city, and depicts a large area in the one photo. However, this scenario does not appear to pose a serious risk to the proportionality principle. To reduce the risk even further, the RPAS operator blurring the images of individuals to the extent that they are guaranteed to be identifiable.

### Purpose limitation (low risk)

As noted above, there is a small risk that purchasers of the footage from the stock image database/ catalogue wish to process the data for purposes that subsequently expand rather than limit the purpose of the original collection. As the purpose of the RPAS operator is to sell this footage, it is arguable that he must meet the purpose limitation requirement, which could be done by employing responsible practices, such as blurring the images.

### Consent (medium risk)

This RPAS is operating in a public space, and the monitoring of visual images in such public spaces is generally acceptable from a data protection perspective, since individuals do not expect a high degree of privacy in public spaces. However, individuals in the vicinity may not be aware that RPAS are in operation, and thus would not have the opportunity to consent to the collection of their personal data, if it were required. Whilst some may argue that the use of RPAS in a public space is analogous to the use of CCTV in public spaces, and should therefore be announced by signage, this is problematic with a mobile technology such as RPAS. This is especially so if the RPAS cannot be detected by individuals on the ground if the RPAS does not have a clear auditory signal that it is approaching. In order to reduce the risk of breaching the consent principle, the RPAS operator could find ways of alerting the public that such information collection is taking place, so that they may give consent, or

alternatively, object to the collection of their personal data. In this situation, where no sensitive data is collected, such consent could be implicitly gained through notifications suggested under transparency.

#### Accountability (medium risk)

Related to issues of transparency and consent is the issue of accountability. RPAS operators who collect personal data must be accountable to individuals who wish to exercise their rights as well as regulators who may wish to enquire about or investigate data. If RPAS operators do not meet their transparency obligations, then it is also difficult for them to meet their accountability obligations. Since, in the scenario above, it was unclear whether the RPAS operator had informed nearby individuals that the filming would be taking place, it would be difficult for third parties to hold the operator accountable for his actions.

#### Data security (medium to high risk)

There is a medium to high risk that the RPAS operator will breach the data security principle. This is because the purpose of collecting the footage is to sell it to third parties. It is also not clear from the scenario whether the RPAS operator will store the footage in a secure manner. This risk is exacerbated by the fact that the RPAS operator will sell the footage to be stored for an indefinite period of time. This action amounts to a breach of the data security principle. Therefore, the RPAS operator must place a condition on the sale of the footage to the stock image database/ catalogue owners that the footage be deleted within a certain period of time. The RPAS operator must not keep the footage for indefinite period of time.

#### Third country transfers (medium to high risk)

There is a medium to high risk that the RPAS operator will transfer the personal data outside of the European Union. Although it is unsure where the stock image database/ catalogue is located, there is a good chance that it is supported by cloud technology, which presents a high risk of the data being moved around to multiple locations. The RPAS operator is restricted from sending footage that included personal data to countries that have “adequate” data protection regimes. To mitigate the risk of a breach of this provision, the RPAS operator must inform themselves of where the personal data will be sent, and potentially arrange for a contractual agreement to accord with the contract derogation at Article 26 of the Data Protection Directive or the national or state equivalent law. The RPAS operator could also make the sale of the footage conditional upon this requirement, although the practical reality of that occurring is slim, especially in the event it jeopardises the RPAS operators commercial potential.

#### Rights of access, correction and erasure (medium to high risk)

Given the interplay between transparency, consent and accountability, the ability of individuals to exercise their rights of access, correction and erasure also represent a medium risk. It is possible that personal information will be collected in this scenario, and individuals have a right to access that material and to request that the data controller delete that material (although this right is not absolute). However, if individuals are not aware who is operating the RPAS, then it is nearly impossible for them to be able to exercise this right. Adequately addressing transparency would be a necessary step forward in meeting this obligation. This risk is however mitigated somewhat if the individuals are truly unidentifiable (either directly or indirectly) as suggested.

The data protection analysis of this scenario indicates that there are some relatively significant risks to data protection when using RPAS to record images of the historical city, the castle ruins and the picturesque marina. This is largely because the RPAS operator, whilst not interested in individuals, has captured individuals. The sale of these images will likely rest on the quality of the images of the city, the castle ruins and the marina. However, the risks that are posed in this scenario can be mitigated by simply meeting the transparency requirement, and anonymising the pictures of the individuals to ensure that they cannot be identified through utilising zoom features.

Finally, in addition to these privacy and data protection issues, **ethical issues** such as safety, public dissatisfaction and discriminatory targeting pose some risk in this scenario. There are various degrees of risk raised by this scenario because the RPAS is operating at a great height, and is not focused on people. However, the operation does contribute to a general proliferation of RPAS, which may be viewed negatively by the public, which presents the highest ethical risk in this scenario.

#### Safety (low risk)

The operation is occurring in a historical city but the RPAS is operated at a great height, and therefore, it is unlikely that the operation poses a significant risk to people or animals, property or other miscellaneous objects such as cars etc. There is no information to indicate that the RPAS operation is noisy, frequent or may negatively impact the area in terms of noise pollution or by disturbing residents or visitors to the city. However, any damage caused by a crash would likely impact the infrastructure being inspected, but the chance of this occurring is slim.

#### Public dissatisfaction (medium to high risk)

The use of RPAS at the location of a historical city that boasts castle ruins and a picturesque marina, may contribute to members of the public feeling “over-run” by RPAS. Transparency and responsible operation can mitigate this potential ethical issue.

#### Discriminatory targeting (very low risk)

The footage is taken of a public space and the RPAS operator has no interest in capturing individuals, and even when they are captured, they are unidentifiable. Thus, there is a very low risk of discriminatory targeting. Even if individuals were identifiable, there is only a small possibility that people in this city may have difficulty voicing their discomfort over the use of RPAS. Further, people of such a historical city may expect footage to be taken of their city from time to time, especially from a perspective of tourism.

The use of RPAS for capturing images of a historical city, castle ruins and a marina, particularly when the individuals inadvertently captured in that footage are unidentifiable due to the height at which the RPAS are operated, is associated with relatively few serious privacy, data protection and ethical risks. These missions are focused on objects, rather than people, and may only collect personal information inadvertently. Nevertheless, great care is still required to ensure that any additional minimisation techniques can be applied to better guarantee that the individuals remain unidentifiable. The transparency requirement can also be met by erecting signage around the city and by notify the managers of the castle ruins so that they can alert visitors to the ruins. Other risks presented by this scenario are related to the sale of the images to the stock image database/ catalogue for what appears to be unrestricted

purchase for an indefinite period of time. This use poses more serious risks. It remains important that RPAS operators educate themselves and members of the public about their use of RPAS and the images they collect, and provide specific information about when RPAS are being used and the purpose for which they are being used. RPAS operators should also consider privacy enhancement and data minimisation practices as mentioned above, such as blurring irrelevant images or limiting their recording to images essential for the mission. These simple activities will assist RPAS operators in meeting privacy expectations, meeting data protection obligations (where they collect personal information) and meeting ethical standards, particularly in combatting public discomfort with RPAS.

### 8.2.3 Novel services

In addition to the services outlined in Chapter 7, the potential missions for that which RPAS may be used are expected to expand. Some of these new services may involve novel payloads and may include the collection of data about people. A typical scenario for such new services is the following:

*An energy company uses a commercial RPAS equipped with a GPS sensor and a thermal camera to film houses and other buildings in several residential areas. Using the information collected from the thermal camera, the energy provider identifies a number of homes and businesses with poor insulation. The energy company then uses the GPS coordinates to match the thermal data with individual customers' addresses. This information is used to send out discount offers on roof insulation under the auspices of meeting national carbon reduction targets.*

The privacy, ethical and data protection issues associated with this scenario are unique in that they are using “sophisticated means” such as thermal imaging cameras to conduct the operation. In the USA, at least, such “sophisticated means” when used by police would likely result in the mission being deemed a “search”, with specific, associated judicial processes and oversight. In Europe, the use of thermal imaging cameras mounted on a drone would likely be qualified by the ECtHR as “hard surveillance” due to the more privacy-intrusive character of such technology. Accordingly, States shall apply the requirements figuring at Article 8§2 of the European Convention of Human Rights more strictly. This may occur through the monitoring being deemed necessary for “economic well being of the country” or through compliance with national carbon reduction targets (i.e., through the protection of health or other national laws).<sup>8</sup> Furthermore, the scenario presents a situation where the non-personal data collected is linked with personal information, and results in RPAS operators possibly having a lot of detailed information about the home and its inhabitants. However, it is worth noting that the operation is not focused on collecting personal information via the thermal images, instead it is focused on the buildings in question. As such, it is only an irresponsible operator that would attempt to review the footage in order to find out information about the specific individuals inside the houses. This section analyses the possible privacy, data protection and ethical risks associated with this particular scenario, with special attention to the thermal imaging and the data linking elements of the mission.

The **privacy issues** associated with this scenario are primarily focused on transparency and function creep as well as the dehumanisation of the surveilled, privacy of location and space

---

<sup>8</sup> Council of Europe, European Convention on Human Rights, Rome, .04.11.1950, Article 8.

and privacy of association. The risks associated with a chilling effect and body privacy are significantly lower.

#### Chilling effect (low risk)

The use of RPAS for such missions represents a very specialised scenario, and the information collected and processed by the company is focused on the buildings in question, rather than the people inside them. Therefore, it is unlikely that individuals would adjust their behaviour, inside their own homes, because they anticipate that an RPAS might be flying overhead with thermal imaging capabilities. However, it is worth noting that the proliferation of RPAS, in general, might lead people to become wary of them. As indicated in relation to the infrastructure-monitoring scenario, these effects could be addressed through greater transparency and awareness raising efforts.

#### Dehumanisation of the surveilled (medium risk)

The energy company undertaking these activities are not necessarily interested in the activities of the individuals in those home, and what the thermal images reveal. However, this operation has the potential to make many people uncomfortable with the thermal images collected. As above, the fact that the energy company is not interested in the individuals per se, may lead him/her to discount the potential impact of the RPAS operation on such individuals. In fact, the survey results in Chapter 6 reveal that the majority of DPA and civil society organisation respondents were likely to view the use of thermal imaging capabilities as representing a high risk to privacy.

#### Transparency and visibility, accountability and voyeurism (high risk)

It is highly unlikely that without some sort of prior notification, that individuals would be aware that an RPAS is collecting thermal images of their homes, and that this information is intended to be linked with their names and addresses. Given that, it is vital that the energy provider, in this case, provides advance information to customers about the operation and allows them the opportunity to opt out of the information collection, the information linking or both.

#### Function creep (high risk)

As indicated above, the risks for function creep will always contain the possibility that the wide-spread use of RPAS for a range of different purposes may normalise their operations, and may discourage individuals from considering what the purposes of the operation may be, leading to significant privacy risks. Specifically, if RPAS are frequently overhead, individuals would find it hard to distinguish between responsible and irresponsible operators. In relation to this scenario specifically, there are also function creep risks associated with the proliferation of thermal imaging operations, and the normalisation of all different types of data linking.

#### Body privacy (low risk)

Although the thermal images collected by the RPAS may contain images of bodies, these are likely to be indistinct and are very unlikely to intrude on bodily privacy. Similarly, the linking of the thermal information associated with the house, and the name and address are unlikely to produce effects related to bodily privacy.

#### Privacy of location and space (medium risk)

Although the energy company is not interested in the individuals within the homes, the images collected by the thermal camera may identify the number of people in the home and could indicate the activities in which they are engaged.

#### Privacy of association (medium risk)

Again, the thermal images collected could indicate the number of people in the home. It could also provide clues as to their relationships, etc. For example, thermal images of two people in one upstairs room, with single individuals in adjacent rooms may indicate a family with two children. Although the energy company may not be interested in this information, there may be some possibility that it could be used in the future for additional marketing projects. Furthermore, the individuals in question may be unwilling to have that information collect about them. Finally, the linking of this information to account names and addresses suggests that a particular individual may be a father or mother (or some other relationship), which infringes upon privacy of association.

In addition to these privacy issues, the use of RPAS fitted with thermal imaging cameras, and the linking of that data to occupiers' names and addresses, also raises significant risks in relation to **data protection** obligations. As above, while the collection of thermal images is not necessarily personal data, the images become personal data once they are linked with the names and addresses. Furthermore, the names and addresses themselves are also personal data. Therefore, the energy company must comply with all of their obligations under the Data Protection Directive.

#### Transparency (high risk)

In the scenario above it is not clear whether the energy company has alerted individuals within the homes and businesses that personal data will be collected, i.e., that thermal images will be attached to their account details. Furthermore, it is not clear whether the RPAS itself has markings on it to identify the data collector. Finally, it is not clear whether individuals would be aware that the energy company would link the images collected by the RPAS to the account details of occupiers. These issues could be mitigated or addressed by alerting people in the filming area that the RPAS operation is taking place, the type of data that will be collected and the purpose of the collection, how the data will be stored, used and/or processed and the right to object to the collection of personal data. The energy company could attach this information to their customers' energy bills or sending a separate notice prior to the intended operation.

#### Data minimisation (medium risk)

Although the images collected by the RPAS during the thermal imaging are not detailed enough to identify individuals, it is not clear whether the energy company has taken specific steps to minimise the amount of data collected during the operation. Specifically, the energy company is presumably focusing on it's own customers and therefore, the images collected of other residences would not be necessary. One potential correction could be to limit the filming to the energy company's existing customers (subject to consent). Another would be to use live images, rather than recorded images, and indicate poorly insulated buildings using a tick on a map or some other mechanism.

### Proportionality (high risk)

It is unclear in this scenario whether the use of RPAS is necessary (and not excessive) to capture the information desired by the energy company, and to achieve successful marketing of their insulation products. As such, the use of RPAS to collect thermal images is likely not the least intrusive technology that could be used to collect the data in question, and that the use of an RPAS for this purpose might be disproportionate. Thus, the energy company would be required to assess the degree of proportionality in this scenario. This could be achieved by undertaking a privacy impact assessment, for example.

### Purpose limitation (low risk)

There is very little risk that the energy company might wish to use the images for some other purpose not originally envisaged in the operation. Furthermore, it is likely that when customers signed up to the energy company, they understood that their details might be used for direct marketing, unless they objected to this practice at that time. Consumers must be given the opportunity to opt out of such direct marketing, and assuming the energy company has respected this, there is little risk that the personal data is being used for additional purposes.

### Consent (high risk)

In the DPA consultation on the 28 Feb 2014, a shortened version of this scenario was presented. Data protection authorities identified consent as the key issue emerging from this scenario. Individuals would have to give specific and informed consent for this operation to take place, especially as this scenario raises issues associated with unsolicited marketing. Such consent could be gained by writing to the customers and offering this service, by indicating to new customers that such operations may be undertaken or by publicising the operation widely and giving customers the opportunity to opt out within a reasonable timeframe prior to the filming taking place.

### Accountability (medium risk)

Related to issues of transparency and consent is the issue of accountability. Companies who collect and process personal data must be accountable to individuals who wish to exercise their rights as well as regulators who may wish to enquire about or investigate data practices. If the energy company does not meet their transparency obligations, then it is also difficult for it to meet its accountability obligations. Since, in the scenario above, it is unclear whether the energy company had informed nearby individuals that the thermal image filming would be taking place, it would be difficult for third parties to hold the company accountable for its actions.

### Data security (low risk)

It is unlikely that third parties could access the data collected. However, it is important for RPAS operators to store any personal data they collect in a secure manner, and to ensure that it is not stored for excessive lengths of time. Deleting unnecessary data (storage limitation) or other data minimisation features could assist the energy company in meeting this obligation.

### Third country transfers (low risk)

It is unlikely that the energy company, in this scenario, would be transferring personal data outside of the European Union. However, if this were the case, the energy would be restricted from sending customers' personal data to countries that have "adequate" data protection regimes. Or through contractual agreements that accord with the contract derogation at Article 26 of the Data Protection Directive.

### Rights of access, correction and erasure (medium risk)

Given the interplay between transparency, consent and accountability, the ability of individuals to exercise their rights of access, correction and erasure also represent a medium risk. If the energy company records the thermal image data and stores it, then individuals will have a right to access that material and to request that the data controller delete that material (although this right is not absolute). This is in addition to their rights to access, correct and delete the personal information already held by the energy company (although this may terminate their relationship). However, if individuals are not aware that the thermal data was collected, then it is nearly impossible for them to be able to exercise this right. Adequately addressing transparency would be a necessary step forward in meeting this obligation.

In this scenario, consent and proportionality emerge as significant data protection risks. The principle of consent is of particular importance as the operation would likely be classed as unsolicited marketing, and prior, informed and explicit consent would be necessary. Furthermore, due to the proportionality principle, a general consent to direct marketing would likely be insufficient to meet the consent obligations. Therefore, the energy company could ensure that it is meeting all of their data protection obligations (including transparency, accountability and data subjects' rights) by writing to customers, informing them of the service being offered, of their rights, and inviting them to opt-in to the thermal imaging data collection.

Finally, in addition to these privacy and data protection impacts, the scenario raises the following **ethical risks**:

### Safety (medium risk)

The operation is occurring in a populated area with many homes and businesses in the vicinity. Therefore, there is a significant risk that if the RPAS were to crash, it would threaten the safety of people and animals or could damage property. However, there is no information to indicate that the RPAS operation is noisy, frequent or may negatively impact the environment in terms of noise pollution or by disturbing wildlife excessively.

### Public dissatisfaction (high risk)

As with any RPAS operation, the use of RPAS in civil air space may contribute to members of the public feeling "over-run" by RPAS. Furthermore, RPAS operations such as these that do collect personal information, and/or link images of people's homes with personal information, may result in significant public backlash, especially if customers were not informed prior to the operation. Transparency, informed consent and data minimisation alongside other responsible operational activities can mitigate this potential ethical issue.

### Discriminatory targeting (medium risk)

There is some likelihood that this operation would target homes in economically deprived areas, as occupiers of homes and businesses in these areas are less likely to be able to afford insulation and other home improvement products and services. As such, these operations could be more common in deprived areas. Furthermore, individuals in these areas may be less likely to understand exactly what data is being collected, and may not feel empowered to exercise their rights, including their rights to complain to the data protection authority about irresponsible practices.<sup>9</sup> As above, using an opt-in mechanism, rather than an opt-out mechanism, would assist in meeting some of these ethical obligations.

Unlike the infrastructure inspection scenario, the fact that this RPAS operation is occurring in populated areas and is focused on people's homes means that the ethical issues are more significant. There is some danger to public safety, given the fact that the RPAS is operating in a populated area. In addition, there are significant risks to public satisfaction with RPAS, given the linking of the RPAS information with personal data. Finally, it is also more likely that disadvantaged areas and populations would be disproportionately impacted by these information collection and linking processes.

This scenario is occurring in areas with a high population density, it is focused on homes and businesses and it is specifically seeking to link the thermal images collected to the personal data of energy customers. As such it raises significant privacy, data protection and ethical risks. Any company wishing to use an RPAS for such purposes should prioritise the assessment of the risks involved in this operation (including the risks to their business via potential public dissatisfaction with the operation). They may also wish to contact their national data protection authority to seek advice about mitigating these risks. However, in this situation the energy company, as the data controller must meet obligations surrounding privacy (in relation to the use of "sophisticated means"), data protection (specifically, transparency, explicit consent, data minimisation and proportionality) and safety issues surrounding the use of RPAS in populated areas.

### **8.3 Law enforcement and government operators**

Unlike commercial users, law enforcement and government users of RPAS are not subject to the Data Protection Directive and the proposed General Data Protection Regulation. Instead, police and law enforcement are partially governed by Framework-Decision 2008/977/JHA and the Proposed Directive regulating data protection in the law enforcement sector. Furthermore, privacy and data protection articles figuring in the Charter of Fundamental Rights of the European Union and the European Convention of Human Rights also apply to governmental authorities including law enforcement. However, under some requirements (if the interference is necessary "in a democratic society in the interests of national security, public safety or the economic well-being of the country"), intrusions by law enforcement authorities in the privacy of individuals could be considered legitimate and not qualify as a violation of privacy. However, despite this legal room to manoeuvre, public sentiment and expectations around their privacy and the protection of their data can have a significant impact on the feasibility of using RPAS for civil law enforcement or government purposes.

---

<sup>9</sup> McCahill, Michael and Rachel L. Finn, *Surveillance, Capital and Resistance: Theorising the surveillance subject*, Routledge, London, 2014.

Furthermore, these organisations have a duty to provide positive and proactive privacy and personal data protections. Therefore, it is important that police and government uses of RPAS seriously consider the impacts of their activities on privacy and data protection, and take steps to minimise these intrusions. This section examines the potential use of RPAS for the surveillance of people, civil protection, search and rescue and regulatory enforcement.

### 8.3.1 Surveillance of people

One of the primary potential uses of RPAS is the replacement of manned helicopters for surveillance activities targeted at people. A typical scenario for such operations is the following:

*A local police force launches a new surveillance mission aiming to identify a group of young offenders committing petty crimes and anti-social activities for the last month. The police station launches two drones fitted with tracking devices (GPS) and multi-function (optical, thermal and infra-red) cameras. The remote pilot flies the RPAS above the social housing estate that has recently been affected by the youth. Although the officers did not locate the youth on the first day, footage from the thermal camera did indicate instances of abnormal hydroponic heat and light usually used for the growth of cannabis plants. The remote pilot shoots some footage of the properties in question and this information is sent to the narcotics team.*

The risks associated with this RPAS scenario are quite significant given that the operation is focused on people, that it is collecting a range of different types of personal data and that it is being carried out by the police. Specifically the operation is looking for a specific type of law-breaker, but it is undertaking blanket surveillance of the area in order to do so. Furthermore this surveillance is not focused on a particular, identified individual (as would be the case in a police chase, for example), instead it is surveying a wide area in order to identify behaviour that suggests illegality. In addition, this scenario indicates that the police are using a range of RPAS functions (optical, thermal and infrared imaging as well as GPS tracking), and as such, are collecting a range of data about the people on the ground. Much of this data is likely to be personal data, as images and location data are classified as personal data.<sup>10</sup> In addition, Data Protection Authorities and civil society organisations identify police use of RPAS as carrying the highest risks to privacy, data protection and ethics. Although police and other government authorities are excused from privacy and data protection obligations in some circumstances, these authorities should strive to attain the highest level of privacy and data protection, given their mandate to uphold existing laws and their interest in maintaining public trust and cooperation. They are also not exempt from using their powers excessively. As such, this analysis examines the privacy, data protection and ethical issues raised by this scenario as though the police were expected to meet all of the obligations required of other actors.

The potential **privacy** impacts associated with this scenario are outlined in detail below:

---

<sup>10</sup> Article 29 Data Protection Working Party, Opinion on the use of location data with a view to providing value-added services, WP 115, Brussels, November 2005. [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp115_en.pdf) and Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, Brussels, 20 June 2007. [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf)

### Chilling effect (high risk)

The use of RPAS for such missions represents the intersection of a lot of different RPAS capabilities and different types of data collected. Furthermore the operation is focused on people, in an area that is already likely to receive a disproportionate amount of surveillance attention from the police.<sup>11</sup> Therefore, it is possible that individuals on the ground would adjust their behaviour or feel discomfort if they were aware that the operation was taking place, even if they were not the targets of the surveillance.

### Dehumanisation of the surveilled (high risk)

As the operation is focused on individuals displaying particular types of behaviours that might indicate illegal activities and that the thermal and infrared images produced will be of indistinct shapes, the police operators of the RPAS are very likely to view the images on the screen as objects rather than people. This may change officers' behaviour when monitoring people on the ground. Furthermore, as noted above, the survey results in Chapter 6 reveal that the majority of DPA and civil society organisation respondents were likely to view the use of thermal imaging capabilities and other advanced technologies as representing a high risk to privacy.

### Transparency and visibility, accountability and voyeurism (high risk)

Unlike police helicopters, which use a clear audio signal to indicate their approach, individuals on the ground may not be aware that an RPAS is in operation, and they are unlikely to be aware that the RPAS in question has thermal imaging, infrared and GPS capabilities. As such, it would be difficult for individuals to react to this surveillance. Police could use an awareness raising campaign to educate individuals about the capabilities of RPAS. They should also explore possible options to indicate that the RPAS is being operated at specific times and in specific places and that the RPAS is being operated by the police.

### Function creep (high risk)

This scenario specifically indicates an example of function creep. The police set out to identify anti-social behaviour, and instead use the RPAS to identify suspected locations of marijuana cultivation. Since the use of RPAS with thermal imaging capabilities would likely be deemed a "search" by the US judicial system and constitutes a "sophisticated means" in the EU, regulators should consider judicial oversight of the use of RPAS for surveillance missions, in order to mitigate the potential for function creep.

### Body privacy (low risk)

The thermal images collected by the RPAS may contain images of bodies, but these are likely to be indistinct and are very unlikely to intrude on bodily privacy.

### Privacy of location and space (high risk)

The ability to collect information about people's whereabouts, the activities within their home and the ability to track their movement through space represents a significant intrusion on privacy of location and space. The police, in this scenario, can interpret the heat signatures

---

<sup>11</sup> Coleman, Roy and Michael McCahill, *Surveillance and crime*, Sage Publications, London, 2010.

emanating from buildings to deduce what is occurring inside, for example, marijuana cultivation. Furthermore, searching for groups of individuals and tracking their activities as they move through the estate may also indicate where they live. Although the collection of this information by the police is lawful, the breach of privacy represented by this scenario should only be used in exceptional circumstances.

#### Privacy of association (high risk)

The thermal images produced by the RPAS and tracking of individuals enabled by the GPS capabilities of the RPAS represent a significant intrusion on privacy of association. These capabilities enable police to identify groups of people gathered together. It also enables them to identify houses or businesses visited by those people, indicating a relationship with those inside.

As indicted by Data Protection Authorities and civil society organisations, the use of these capabilities by police are associated with high-level risks to privacy. Almost all of the privacy issues examined above are associated with a high risk to privacy. Only bodily privacy presents a low risk. However, should the capabilities of RPAS expand to include biometric identification, including soft biometrics like gait recognition, the intrusions to bodily privacy will also be conceptualised as high risk. Furthermore, these additional capabilities are desirable to police. Given this framework, it is clear that the use of RPAS by police for law enforcement raise serious privacy issues.

In relation to the **protection of personal data**, this scenario is also associated with a number of high-risk elements.

#### Transparency (high risk)

As indicated above, law enforcement and other government authorities are not necessarily obligated to meet transparency obligations in relation to their use of RPAS for personal data collection and processing. However, despite this, the police should endeavour to warn people that RPAS surveillance is taking place, that it is the police who are operating the devices and that the RPAS in question has particular capabilities. None of these transparency elements are indicated in the scenario above.

#### Data minimisation (high risk)

Rather than restricting themselves to the collection of data associated with the intended mission, this scenario indicates that the police are not adequately meeting data minimisation principles. First, the police are recording footage rather than monitoring live footage. Second, the police are collecting information about commercial and residential buildings, rather than restricting themselves to information that indicates the presence of the gang of youths for whom they are searching. Finally, it is not clear whether all of the capabilities included in the RPAS in question are necessary for the mission at hand.

#### Proportionality (high risk)

It is unclear in this scenario whether the use of RPAS in general, or the use of the specific range of capabilities of this particular RPAS, is necessary to capture the information desired by the police. Furthermore, the use of RPAS with these particular capabilities is certainly not

the least intrusive technology that could be used to collect the data in question. Therefore, the use of an RPAS for this purpose might be disproportionate.

#### Purpose limitation (high risk)

This scenario presents a specific example of a breach of the principle of purpose limitation. The police have deployed the drone for one purpose (searching for a gang of youths) and have ended up using it to identify suspected locations of marijuana cultivation. As indicated by Data Protection Authorities during the 28 Feb 2014 consultation, such mission changes represent a major risk for the protection of personal data and may be subject to sanction by Data Protection Authorities if undertaken by non-government actors.

#### Consent (high risk)

Even in respect of surveillance in public spaces, some amount of consent is involved, given that individuals may choose not to enter shops, town centres or other locations where surveillance technologies are deployed. Furthermore, most regulations require these surveillance activities to be publicised, even if authorities, such as police, undertake them. However, this consent is tenuous at best, since surveillance technologies are pervasive and since, in many spaces, the opportunities to access essential goods and services are limited to surveilled locations.<sup>12</sup> Despite this, if the police were to find some means to indicate that the mission described above is taking place, individuals could choose to remain indoors or to conceal items or activities that they wish to keep private. Again, the contrast between silent RPAS and audible helicopters provides a useful means to conceptualise the issue.

#### Accountability (medium risk)

Both the police and other government authorities are ultimately accountable to the public who may use elections and other means to indicate their disagreement with particular policies and practices. However, this requires that the public are aware of the exact nature of the operations that are occurring, the types of data that are being collected and the consequences resulting from those operations. As indicated in relation to other scenarios, transparency is a key aspect of accountability obligations.

#### Data security (low risk)

It is unlikely that the data collected could be accessed by third parties. However, it is important for the police to store any personal data they collect in a secure manner, and to ensure that it is not stored for excessive lengths of time. Deleting unnecessary data (storage limitation) or other data minimisation features could assist the police in meeting this obligation.

#### Third country transfers (low risk)

It is unlikely that the police, in this scenario focused on local issues, would be transferring personal data outside of the European Union. However, if this were the case, other legal frameworks, specifically Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters or other bilateral agreements, would apply.

---

<sup>12</sup> Coleman and McCahill, op. cit., 2010.

### Rights of access, correction and erasure (high risk)

Given the interplay between transparency, consent and accountability, it is unlikely that individuals will be aware of the precise nature of the RPAS operation in question. This would present an obstacle for individuals seeking to exercise their rights of access, correction and erasure. Specifically, if individuals are not aware that their data is being collected, then it is nearly impossible for them to be able to exercise these rights. Adequately addressing transparency would be a necessary step forward in meeting this obligation.

This analysis has indicated that the use of RPAS in the scenario outlined above represents specific and significant threats to the protection of personal data. Following from similar assessments of police use of RPAS in Chapter 6, this analysis finds that police, as users of RPAS, are most likely to introduce risks associated with transparency, data minimisation, proportionality, purpose limitation and rights of access, correction and erasure. In this specific scenario, an additional high-level risk includes consent and a medium-level risk includes accountability. However, as above, transparency is a key mechanism through which many of these data protection issues can be minimised. Therefore, police users of RPAS for surveillance activities should consider ways to educate the public without jeopardising their ability to arrest and prosecute those who break the law.

Finally, the police use of RPAS in this scenario also raises **ethical issues** around the use of drones in these locations and for these particular types of data collection.

### Safety (high risk)

The operation is occurring in a populated area with many homes and a few businesses. Therefore, there is a significant risk that if the RPAS were to crash, it would threaten the safety of people and animals or could damage property. However, there is no information to indicate that the RPAS operation may negatively impact the environment.

### Public dissatisfaction (high risk)

Police use of RPAS to fight crime may contribute to members of the public feeling “over-run” by RPAS, especially as civil, commercial uses proliferate. Furthermore, RPAS operations such as the one presented in this scenario where police target specific individuals, collect a lot of information from a relatively large population of individuals and use the RPAS for secondary purposes (e.g., to identify suspected marijuana cultivation), may result in significant public backlash. This is especially true if members of the public are not aware that such data collection practices are possible. Transparency, informed consent and data minimisation alongside other responsible operational activities can mitigate this potential ethical issue.

### Discriminatory targeting (high risk)

It has already been documented that surveillance technologies used for law enforcement purposes, including CCTV and RPAS, focus disproportionately on marginalised populations.<sup>13</sup> Therefore, it is reasonable to assume that this trend will continue and that police use of RPAS for sophisticated surveillance would disproportionately target

---

<sup>13</sup> Finn, Rachel L. and David Wright, “Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications”, *Computer Law & Security Review*, Vol. 28, No. 2, 2012, pp. 184-194.

marginalised populations and neighbourhoods. Furthermore, individuals in these areas may be less likely to understand exactly what data is being collected, and may not feel empowered to exercise their rights, including their rights to complain to the data protection authority about irresponsible practices.<sup>14</sup>

In terms of ethics, police operators are likely to be held to the highest standards, as it is their operations that are most likely to result in public dissatisfaction with the use of RPAS for civil purposes. Although safety is a key ethical issue, especially in situation such as the one depicted here where RPAS are used in populated areas, it is likely that police drones would aspire to the highest safety standards. However, the ethical use of RPAS is also particularly important for police, as their activities are intended to result in arrests and prosecutions, and the large-scale deployment of RPAS could have significant impacts on the life chances of some people, particularly those in deprived neighbourhoods or individuals from already marginalised populations. This has significant potential to generate public dissatisfaction as well as organised back-lash against the use of RPAS by police.

Although the use of RPAS by law enforcement in this scenario generates significant risks to privacy, data protection and ethics, ultimately it is not the RPAS, as such, that introduces many of these risks. Instead, it is the data collection enabled by the payload with which the RPAS is fitted. As such, the primary distinction between the police use of RPAS and other surveillance devices with the same payloads or capabilities is the potential for RPAS to be deployed covertly. Furthermore, RPAS also enable police to survey wide areas and capture data from multiple individuals not connected to the operation in question. As noted above and at length in Chapter 3, the use of RPAS fundamentally changes the nature of surveillance due to RPAS relative silence, potential pervasiveness and ability to survey wide areas almost continuously. As such, law enforcement operators, who already have significant have significant scope for exception from privacy and data protection legislation, must give serious consideration to how their use of RPAS may impact individuals “on the ground” including both “suspects” and innocent potential data subjects. This is particularly the case as unlike commercial operations, the operation of RPAS by police can have significant and long-lasting impacts on individuals’ life chances.

### 8.3.2 Civil protection

In the areas of crisis management, firefighting and search and rescue, RPAS are becoming key tools to protect the lives of members of the public and emergency personnel and respond to incidents as they develop. A typical civil protection scenario includes the following:

*Emergency services deploy an RPAS equipped with thermal imaging, a mobile phone signal sensor and GPS capabilities to search for hikers lost in the woods. The search picks up mobile phone and heat signatures from a number of hikers, generating “false alarms” which must be investigated by matching phone signals to individual mobile phone accounts. The correct lost hikers are found after a few hours, and the data from the “false alarms” is immediately discarded.*

---

<sup>14</sup> McCahill, Michael and Rachel L. Finn, *Surveillance, Capital and Resistance: Theorising the surveillance subject*, Routledge, London, 2014.

This particular scenario is significant for privacy, data protection and ethics as it collects a number of different types of personal data in a situation where the public interest in excusing authorities from privacy and data protection obligations is clear. However, in this scenario the authorities are collecting data in an area where many individuals would expect that they are anonymous, and the personal data that they are collecting is significant and includes thermal images, location information and names and addresses. Furthermore, the information is being collected from ordinary hikers as well as the lost hikers. The following section examines the privacy, data protection and ethical issues specific to this scenario, with particular attention to the collection of identifiable data collected as “false alarms”.

The potential privacy impacts associated with this scenario are outlined in detail below:

#### Chilling effect (low risk)

The use of RPAS for such missions is likely to be very infrequent, and it is unlikely that individuals taking advantage of the woodlands described in this scenario would alter their behaviour. While they may feel discomfort that their mobile phone signal and location is being identified and linked with their names and address, it is unclear how this might impact their behaviour specifically. This is especially true if individuals were aware that the RPAS was undertaking a search and rescue mission, and if they were aware that their information would be discarded upon identification of the correct hikers.

#### Dehumanisation of the surveilled (low risk)

This operation is focused on identifying specific individuals that are in danger. As this is essentially a humanitarian mission focused on rescuing people in danger, it is unlikely that individuals on the ground would be dehumanised.

#### Transparency and visibility, accountability and voyeurism (medium risk)

Although hikers and other outdoor enthusiasts would likely support the mission if they were aware of the purpose of it and the data collection policies and procedures, the operation may raise transparency issues. Specifically, individuals on the ground may not be aware that the RPAS is in operation or that it is collecting their personal data. Even if they notice the RPAS, they are unlikely to be able to identify the operator or the specific mission that is being undertaken. As above, this could be addressed using some sort of markings, information campaign or some sort of live smart phone application that identifies which RPAS are in the air and the location in which they are operating.

#### Function creep (medium risk)

This scenario represents a specialised mission for RPAS that is clearly in the public interest. However, the proliferation of RPAS in general will always “normalise” RPAS and increase the purposes for which they are used. Outside of this general potential for function creep, which may be desirable for many stakeholders, this scenario does not indicate that the authorities may use the thermal, mobile phone or GPS data for any other purpose. This is particularly the case since the data is discarded after the correct hikers are identified.

### Body privacy (low risk)

The thermal images collected by the RPAS may contain images of bodies, but these are likely to be indistinct and are very unlikely to intrude on bodily privacy.

### Privacy of location and space (medium risk)

This scenario represents an ability to collect significant personal information about people using the woodland, including location data and personally identifiable information. In short, after the “sweep” for the lost hikers, the authorities will be able to identify who is in the woods and where precisely they are located. However, this risk is mitigated by the fact that the authorities are only searching for specific persons, and that the data is discarded as soon as those specific individuals are located.

### Privacy of association (medium risk)

The collection of thermal images, the identification of individuals in the woods via their mobile phone information and the location of those individuals using GPS technology will reveal whether individuals are moving through the woodland alone or in groups. As such, authorities will likely be able to infer existing relationships between the individuals identified, and the name and address information may provide some clues to the character of their relationship (spouse, sibling, etc.).

This scenario represents significantly lower risks to privacy than the police surveillance scenario, partly because of the character of the mission (search and rescue) and partly because the data collected by the authorities in this situation are deleted as soon as the lost hikers are found. This represents a significant data minimisation and privacy enhancing practice with clear impacts on the privacy implications for the RPAS mission. However, despite this, the collection of thermal images, mobile phone data and location data does give authorities a clear picture of who is in the woods, where they are in the woods and how they are travelling. As a result, there are some potential impacts for transparency, function creep, privacy of location and space and privacy of association.

The scenario also raises a number of risks to personal data protection, given that personal data is clearly collected in this scenario. This personal data includes the names, addresses and phone numbers linked to the mobile phones identified by the RPAS and the location data associated with those phone signals. As such, the scenario raises the following data protection issues:

### Transparency (medium risk)

As noted above, law enforcement and other government authorities are not necessarily obligated to meet transparency obligations in relation to their use of RPAS for personal data collection and processing. However, despite this, the authorities should, as far as possible, attempt to inform people that RPAS surveillance is taking place and that the RPAS is being operated by authorities in a search and rescue mission. Furthermore, the police should inform individuals that their personal information (including mobile phone information and location information) was collected and then discarded. None of these transparency elements are indicated in the scenario above. However, a news item in the local media, a notice at the woodland’s carpark(s) or some other information campaign could accomplish this.

#### Data minimisation (low risk)

This scenario appears to meet data minimisation requirements via the discarding of information once it is no longer useful. Furthermore, most of the capabilities included in the RPAS in question appear necessary for the mission at hand.

#### Proportionality (low risk)

In this scenario, the use of RPAS and the information collected appears proportionate to the mission at hand. It is necessary to use a flying technology platform to cover a wide area in a short period of time, and to identify the individuals in the woods in a quick and efficient manner. A helicopter may have accomplished this mission in the same manner, however in this situation the use of the RPAS is much more affordable and does not change the nature of surveillance. Furthermore, the relative silence of the RPAS could be mitigated by adequate transparency measures to advertise their use.

#### Purpose limitation (low risk)

In this scenario, the personal information that is collected is restricted to processing for one specific use – to find a particular set of individuals. There is little risk to purpose limitation given this single use. Furthermore, the fact that the data is deleted after the mission limits the possibility for infringing on purpose limitation by using the data for a secondary purpose after the mission.

#### Consent (high risk)

This RPAS is operating in a public space, and the monitoring of visual images in such public spaces is generally acceptable from a data protection perspective, since individuals do not expect a high degree of privacy in public spaces. However, this usage of RPAS does not collect straightforward visual images, nor does it simply monitor without recording. Instead, this RPAS collects significant personal information, and does so in a setting where people would not expect to be monitored by authorities. As such, the idea that people could simply choose not to use this particular space if they wanted to excuse themselves from potential personal information collection does not apply here. Furthermore, the authorities cannot predict when such a use of RPAS might be needed, so it is difficult to inform individuals before the RPAS is launched. Despite this, improving transparency in general will enable individuals to decide whether to enter the woodland and potentially subject themselves to information collection.

#### Accountability (low risk)

Authorities are ultimately accountable to the public who may use elections and other means to indicate their disagreement with particular policies and practices. However, the public are likely to find this use of RPAS, and the associated information collection practices, acceptable, as long as the authorities treat their data carefully. Improving transparency will assist in this.

#### Data security (low risk)

Since the data is deleted when it is no longer necessary, data security is a low-risk issue in this scenario. Furthermore, it is highly unlikely that someone wishing to “hack” the RPAS would

be concealing themselves in the woods waiting for a lost hiker search in order to intercept the personal data of ordinary hikers. However, as noted above, it is important that the authorities treat the personal data that is collected respectfully and with the highest level of security. The data minimisation feature of this scenario is an important safeguard in relation to data security.

#### Third country transfers (negligible risk)

It is highly unlikely that the authorities in this scenario would be transferring personal data outside of the European Union.

#### Rights of access, correction and erasure (low risk)

Given the interplay between transparency, consent and accountability, it is unlikely that individuals will be aware of the precise nature of the RPAS operation in question. This would present an obstacle for individuals seeking to exercise their rights of access, correction and erasure. Specifically, if individuals are not aware that their data is being collected, then it is nearly impossible for them to be able to exercise these rights. However, in this scenario, the data is not stored, so there would be no information for individuals to access, correct or erase.

Unlike many of the scenarios already examined where the risks to personal data protection were deemed to be relatively high, this collection of personal data raises significantly lower risks to personal data protection. The data minimisation element of this scenario is a significant factor in lowering risks associated with proportionality, purpose limitation, data security and data subjects' rights. However, the scenario still represents some data protection risks, particularly around transparency and consent. Although the data collected is minimised, individuals still have rights to be informed that their personal data is being collected and be given an opportunity to either consent to that data collection or access the information collected about them (if it is stored). As such, the data protection risks associated with this scenario could be significantly reduced using an information campaign or some other mechanism to alert people that an RPAS may be in operation and that their data may be collected in special circumstances.

As indicated in relation to data protection, this ethical issues raised by this scenario are reduced in comparison to other scenarios examined in this chapter.

#### Safety (low risk)

The operation is occurring in an unpopulated area, however there may be some risk to animals or the environment if an RPAS were to crash. There is no information to indicate that the RPAS might damage the environment in any other way.

#### Public dissatisfaction (low risk)

The use of RPAS for these sorts of missions are unlikely to generate public backlash, especially if the authorities can put forward a “good news story” in terms of finding the lost hikers and if they adequately address transparency obligations.

#### Discriminatory targeting (negligible risk)

This operation is targeted at specific individuals for a clear public safety purpose. As such, it is not discriminating against any particular groups of people.

Unlike previous scenarios, especially the other scenario involving police authorities presented above, this scenario raises substantially less considerable ethical issues. Although some risks to safety and public dissatisfaction remain, these are substantially reduced compared with other scenarios given the rural location and the fact that members of the public would likely support the use of RPAS for such missions. Furthermore, as the mission is focused on specific, known individuals, there is little likelihood that particular categories of people are more likely to be impacted than others.

Despite the fact that this scenario collects personal data, including data which identifies individuals by name, provides their phone number and likely provides their address, the privacy, data protection and ethical risk are relatively low when compared with other scenarios. The scenario is being carried out for a purpose that is clearly within the public interest, is occurring in an unpopulated area and is only collecting data for one particular purpose for a set period of time. All of these factors, but especially the privacy enhancing, data minimisation feature, contribute to these reduced risks. However, it is important to note that considerable risks remain, with particular reference to transparency, function creep and consent. As in all of the other scenarios examined here, RPAS operators have an essential obligation to notify individuals that an RPAS is in operation, the purpose for which it is being used and the identify of the operator. These transparency elements are important to assist individuals in exercising their rights, but they are also an important aspect of combatting public dissatisfaction. Again, devising some sort of information campaign would significantly reduce the risks associated with this particular RPAS mission.

### 8.3.3 Regulatory enforcement

RPAS may also be used by authorities for less traditional enforcement activities that may fall outside the remit of the police, as such. For example, RPAS could be used by environmental authorities to monitor for illegal logging, fishing or trespassing in protected areas. A typical scenario examining such regulatory enforcement includes the following:

*The Environmental Protection Agency hires a commercial RPAS operator to undertake a range of surveillance necessary to enforce restrictions against logging and monitor for forest fires and air pollution in a nature reserve. The RPAS is fitted with high definition video surveillance, thermal imagery and environmental sensors. It patrols a specific area and takes regular photos and readings. These photos and readings are transmitted back to the forest rangers' office. Occasionally hikers, campers and other nature enthusiasts are captured in the images, and authorities occasionally follow up on suspicious images or readings by visiting campsites or seeking out groups of people. No arrests have been made.*

There are a number of data collection practices being undertaken in this scenario. The first type of data collection, the environmental sensing, is not focused on people and will not include personal data. As such, the privacy, data protection and ethical risks are negligible in relation this type of data collection (with the exception of safety as it relates to noise pollution, etc.). The high-definition video surveillance and thermal imagery do raise some privacy, data protection and ethical risks, primarily because the footage is recorded rather than live feed being monitored. As such, the images, especially represent personal data. However, the fact that the RPAS takes photos at regular intervals (rather than continuous recording) is a significant data minimisation feature. The particular risks associated with this scenario are examined in detail below.

The potential privacy impacts associated with this scenario are relatively low, especially when compared to other scenarios that involve the collection of personal data.

#### Chilling effect (medium risk)

The use of RPAS for such missions is focused on detecting illegal behaviour, rather than continuous monitoring. Furthermore, it is unlikely that individuals taking advantage of the woodlands described in this scenario would alter their behaviour. While they may feel discomfort if they notice a drone flying overhead, it is unclear how this might impact their behaviour specifically. However, this level of discomfort might be increased if hikers, campers and other individuals noticed the RPAS had a camera, noticed that the RPAS was flying near to them or connected a visit by the park rangers to the RPAS footage.

#### Dehumanisation of the surveilled (low risk)

While the fact that the RPAS takes regular patrol images represents an important data minimisation feature, images can be taken out of context, especially if the purpose of the mission is to identify “suspicious behaviour”.<sup>15</sup> However, any suspicious behaviour is followed up by a human investigator, which mitigates much of the potential for dehumanisation.

#### Transparency and visibility, accountability and voyeurism (medium risk)

Hikers, campers and outdoor enthusiasts would likely support the environmental protection elements of the RPAS mission. However, this scenario does not provide any information about whether these individuals were made aware of the mission, including who was operating the RPAS and the purpose for which it is being used. As such, the operation may raise transparency issues. As discussed in relation to many of the scenarios above, there are some strategic actions that could assist authorities in making individuals aware that information about them may be collected.

#### Function creep (medium risk)

The expansion of the missions for which RPAS are utilised serve to “normalise” RPAS and further expand the purposes for which they are used. Outside of this general potential for function creep, which may be desirable for many stakeholders, this scenario does not indicate that the authorities may use the data collected by the RPAS for any other purpose.

#### Body privacy (low risk)

The optical and thermal images collected by the RPAS may contain images of bodies, but these are unlikely to intrude on bodily privacy.

#### Privacy of location and space (low risk)

Although the RPAS in this scenario is taking images of individuals in particular places and at particular times, there is no “systematic” recording of their behaviour that would indicate tracking of the individuals in question. Furthermore, the individuals themselves are not

---

<sup>15</sup> Norris, Clive and Gary Armstrong, *The Maximum Surveillance Society*, Berg Publishers, Oxford, 1999.

identified by the images, as such. The authorities in this scenario have to physically seek out the individuals and make further enquiries. As a result, the risks for privacy of location and space are relatively low.

#### Privacy of association (low risk)

Although the collection of optical and thermal images will reveal whether individuals are moving through the woodland alone or in groups, the fact that the individuals in question are not identified means that the authorities are not able to automatically collect information about who those individuals are. As such, it would also be difficult for them to identify relationships between individuals aside from broad categories such as family, group of friends, etc. In consequence, the risks to privacy of association are relatively low.

Because images of individuals are collected, this scenario does raise some privacy related-risks. However, these are primarily generalised risks related to a function creep, transparency and a chilling effect, rather than specific risks like bodily privacy, privacy of location or privacy of association. Furthermore, although these risks do exist, they are tempered by the fact that the images are not accompanied by or linked with any other data (names, addresses, etc.) and thus, it is unlikely that individuals could be identified via the data collected. They are also tempered by the fact that the RPAS collects images at regular intervals, rather than “systematic” recording. Nevertheless, these tempering mechanisms are not complete, particularly because rural, woodland locations are areas where people are unlikely to expect to be under “surveillance”.

The scenario also raises a number of data protection issues worthy of consideration, particularly because image data is personal data.

#### Transparency (high risk)

As noted above, people are unlikely to expect to be under surveillance in woodlands, and so the authorities should, as far as possible, attempt to inform people that RPAS surveillance is taking place and the purpose for which it is being used. The scenario above, set in a similar location provides some suggestions as to how this mission could be better publicised to assist in meeting transparency obligations.

#### Data minimisation (low risk)

This scenario appears to address data minimisation requirements, as the information collected is restricted to regular intervals rather than continuous collection. Furthermore, it appears that all of the capabilities used by the RPAS are relevant to the mission described. However, the scenario does not offer any information about whether the image data related to persons is stored, by whom and for how long. RPAS operators should consider each of these when addressing data minimisation obligations.

#### Proportionality (low risk)

In this scenario, the use of RPAS and the information collected appears proportionate to the mission at hand. It is acceptable to use an RPAS to cover a wide area of difficult terrain in a short period of time, and to get a “bird’s eye” view of the landscape. The collection of personal data is restricted to image data that is not linked with any other personal information, and which is followed up by a human investigator if more information is required.

Furthermore, the relative silence of the RPAS could be mitigated by adequate transparency measures to advertise their use.

#### Purpose limitation (low risk)

In this scenario, the personal information that is collected is restricted to image data that is not automatically linked with any additional personal information. There is little use for these images after they are collected, except to potentially identify known individuals or compare images to previous incidents. Yet, each of these purposes is compatible with the original regulatory enforcement purpose. Furthermore, there is no information to indicate that the images or the RPAS in general could be used for additional purposes other than regulatory enforcement.

#### Consent (high risk)

Although this RPAS is operating in a public space, the case law indicates that the primary reasoning behind the distinction between public and private space is around the expectation of privacy. While woodland is technically public space, there is an expectation of privacy due to the fact that it is an unpopulated area. As such RPAS operators need to meet transparency requirements given that the RPAS is used regularly, that it records images of individuals and that individuals may choose not to enter the woodland if they are aware that their image data may be collected. In this situation, the authorities must give individuals the opportunity to consent to the data collection, even if this consent is implicit and based on the authorities having publicised the use of RPAS for this purpose.

#### Accountability (low risk)

In this scenario, it is likely to be relatively obvious who is operating the RPAS, and as such individuals should be aware of whom they should approach to comment on the use of RPAS and the collection of personal information. Furthermore, while the public are likely to find this use of RPAS, and the associated information collection practices, acceptable, improving transparency will assist in this.

#### Data security (low risk)

Since the personal data collected is not connected with names, addresses or other specific information that would lead to the identification, either directly or indirectly, of the individuals on screen, data security is a relatively low-risk issue in this scenario. Furthermore, it is unlikely that the personal information collected will be of interest to anyone outside of the police or other authorities. However, as noted above, it is important that the authorities treat the personal data that is collected respectfully and with the highest level of security, including methods of secure erasure.

#### Third country transfers (negligible risk)

It is highly unlikely that the authorities in this scenario would be transferring personal data outside of the European Union.

#### Rights of access, correction and erasure (medium risk)

Although the personal data collected by the RPAS is relatively minimal and difficult to link with other data about the individual, people may have difficulty exercising their rights if they

were unaware that their data was being collected. Consequently, it is nearly impossible for them to be able to exercise these rights. If transparency obligations were robustly addressed, this would result in a significantly lowered risk.

Although the risks to personal data protection in this scenario are significant, they are reduced in comparison with other scenarios presented here. This is primarily because the data collected is restricted to still images taken at regular intervals and the image data is not linked to any other personal data. This responsible data collection practice means that risks to data minimisation, purpose limitation, proportionality and data security are relatively low. However, as indicated in relation to many of the other RPAS missions described above, the interplay between transparency and consent results in significant risks in these areas. Although authorities are not subject to the Data Protection Directive in many circumstances, they should always aim to meet these requirements as far as possible in order to reduce public dissatisfaction with RPAS usage and to foster public trust in such authorities.

Finally, the ethical risks associated with this RPAS scenario are also relatively low, primarily due to the context in which the RPAS is operating and the mission for which it is being deployed.

#### Safety (low risk)

The operation is occurring in an unpopulated area, however there may be some risk to animals or the environment if an RPAS were to crash. There is no information to indicate that the RPAS might damage the environment in any other way.

#### Public dissatisfaction (low risk)

The use of RPAS for these sorts of missions are unlikely to generate public backlash, especially if the authorities highlight that the RPAS is assisting them in protecting the environment, if people using the woodland do not feel harassed by the RPAS or any subsequent investigation and if authorities adequately address transparency obligations.

#### Discriminatory targeting (medium risk)

Although it is highly unlikely, this operation may raise some issues in relation to discrimination. Some users of the woodland might be viewed by authorities as “legitimate users”, e.g., families, fishermen, etc., while the presence of other types of people, e.g., groups of young people, might be deemed suspicious. Without the surveillance by the RPAS and the regular image data collected, park rangers would not have as much information about who was using the woodland and the characteristics of people or groups would not be cause for further investigation.

In this scenario, the ethical risks are not as considerable as the risks associated with police surveillance of youth or commercial information collection. This is primarily because the operation is occurring in an unpopulated area, and is being used for a mission that is primarily focused on protecting the environment. However, the fact that the RPAS collects visual images, and that these visual images are the sole basis for launching further investigation, means that many of the social biases potentially held by park rangers would be implicated in their decision about whether to launch an investigation. As such, there is a possibility that particular categories of individuals would be more likely to be investigated than others, with discriminatory undertones.

This scenario represents a reduced set of risks to privacy, data protection and ethics. The fact that the RPAS is collecting occasional visual images, rather than systematically recording, is a key aspect of these reduced risks. In addition, the existing risks would be further reduced if it was clear that the park rangers were meeting transparency obligations by informing members of the public that such information collection via RPAS was taking place and by providing information about how the rangers could be contacted if people had specific questions or concerns. If this were the case, the existing risks to transparency, a chilling effect, consent and rights to access, correction and erasure would drop substantially.

## 8.4 Journalists and filmmakers

In the chapters above, journalists and artists, such as filmmakers, have emerged as another key stakeholder group in relation to RPAS operations. However, like police, these operators may fall outside of some of the specific provisions of privacy and data protection legislation. As noted in Chapter 3, Article 9 of the 1995 Data Protection Directive foresees exemptions to several provisions when “processing [that] is carried out solely for purposes of journalism or the purposes of literary or artistic expression”. However, journalists and filmmakers are likely to target members of the public as their subject material, and thus, their use of RPAS may raise privacy, data protection and ethical risks. This sub-section examines two scenarios, separately, that represent typical uses of RPAS for filmmaking and journalism.

### 8.4.1 Filmmaking

Filmmaking may include fictional filmmaking, which is unlikely to result in the collection of personal data or raise privacy or ethical issues, and documentary or promotional filmmaking, which may raise such issues. The following scenario was presented in Chapter 7 in relation to promotional filmmaking:

*A local council decides to encourage tourism by commissioning a collection of videos and still photos of village life, as captured by an RPAS. The RPAS zipped through the streets, capturing images of people shopping, sunbathing and relaxing in the local gardens. Residents were not informed of the filming, although some saw the RPAS and its operator and assumed it was a toy. A few residents complained when images of them and their families were released via the Internet, but the council has argued that videoing in public places is just like CCTV.*

This scenario represents the use of an RPAS for filmmaking purposes, a practice that can take advantage of some derogation from privacy and data protection legislation through claims to artistic expression. Nevertheless, the use of RPAS in this scenario, specifically the fact that residents’ images were captured without consent, and that the council has compared this to CCTV, raise significant issues related to the privacy, data protection and ethics. First, while the filmmaker himself might be able to claim artistic expression, it is not clear whether the council can take advantage of such claims. Second, the filming by the RPAS differs from CCTV in that residents were not notified of the data collection, that the RPAS is moving around rather than static, and that the footage is recorded, stored and then released publicly.

As such, the filming of town residents in this scenario raises a number of privacy issues.

#### Chilling effect (medium risk)

Although the use of RPAS for this mission was clearly an event that would occur only once, the fact that residents were not informed of the filming may lead them to be concerned that every incident of filming they notice, and every RPAS that they notice may result in publicly released footage. This means that every filming as well as every sighted RPAS may encourage individuals to alter their behaviour as though their images were going to be released to the general public.

#### Dehumanisation of the surveilled (high risk)

This scenario represents a clear example of dehumanisation of the individuals whose images were captured. The RPAS operator and the council did not consider the perceptions and preferences of residents, and as such the human consequences of the RPAS operation were not taken seriously. A meeting with residents would have assisted both the Council and the RPAS filmmaker in addressing these concerns.

#### Transparency and visibility, accountability and voyeurism (high risk)

Although the RPAS in this scenario was visible to village residents as it was filming, the residents were not given prior information about the filming, nor were they aware of the purpose for which it was being used. As such, this mission significantly compromised transparency and accountability. Furthermore, as filmmakers have some derogation from privacy laws, there is a possibility that some residents could feel that the filming of people in the park sunbathing included a voyeuristic element.

#### Function creep (low risk)

The use of RPAS in this situation represents a small risk to function creep in that publicising the images displays the capabilities of RPAS and may encourage their use for other purposes. However, this aspect of function creep is desirable for many stakeholders. In terms of the images being used for another purpose, there is very little information to indicate that this is a significant risk.

#### Body privacy (low risk)

The images collected by the RPAS contain images of bodies, including of people sunbathing, but these are unlikely to intrude on the integrity of the body.

#### Privacy of location and space (medium risk)

The RPAS in this scenario is taking images of recognisable individuals in particular places and at particular times. This would enable these recognisable individuals to be “placed” in particular locations, which they may wish to conceal. Furthermore, the fact that such an RPAS would be relatively undetectable means that individuals could not necessarily react to the RPAS filming by ducking indoors to remove themselves from the images collected.

#### Privacy of association (medium risk)

As the images collected by the RPAS in this scenario are specific to a particular village, consist of recognisable individuals and are released publicly, this scenario raises an issue in relation to privacy of association. Specifically, the RPAS recorded images of particular

individuals moving around town, shopping or relaxing in the park. If people were to review these publicly available images, they would reveal who their neighbours are socialising with and who their children are associating with as well as other social connections. As individuals have a right to keep their personal relationships private, the recording and subsequent release of this information could have potential impacts that rights to privacy are meant to prevent.

The privacy impacts raised by this scenario are primarily related to the recording and the disclosure of images of identifiable individuals in a small village, the lack of transparency in that villagers were not informed of the filming and the subsequent release of those images publically. As a result, there are significant potential impacts related to a chilling effect, dehumanisation of the people captured by the footage, transparency, privacy of location and space and privacy of association.

In addition to these privacy impacts, the scenario also raises a number of potential impacts related to the protection of personal data. Artistic expression is not necessarily covered by the Data Protection Directive, the Council, especially, and the RPAS community, in general, should strive to meet the highest data protection standards in order to encourage the public to support the use of RPAS for civil operations.

#### Transparency (high risk)

As noted above, many residents were unaware that an RPAS was in operation, that their images were being recorded, and that the image data would be released on the Internet. Each of these elements represents a potential non-compliance with the transparency principle, and thereby infringes applicable data protection laws. Members of the public need to be informed that their data is being collected and the purpose for which it is being used. Furthermore, they must be given an opportunity to consent to that data being released to the general public.

#### Data minimisation (high risk)

This scenario does not indicate that any obligations to minimise the amount of data collected about individuals were considered. The RPAS operator could have flown the RPAS higher above the ground, focused on buildings and/or blurred the images of people to ensure that they were not identifiable. Furthermore the local Council could also have suggested each of these data minimisation practices during the filming and before the film was released on the Internet.

#### Proportionality (high risk)

In this scenario, the use of RPAS is proportionate to the mission, but the collection of personal information during that mission is not. Individuals captured by the footage could have been given the opportunity to consent to their image being revealed, or as suggested above, fixes like blurring could have been used to ensure that no personal information was collected or released.

#### Purpose limitation (low risk)

Although the collection of personal data in this scenario is widespread and disproportionate, there is little indication that the footage would be used for a purpose other than that which was originally envisaged. As such, the risks to purpose limitation in this scenario are relatively low.

### Consent (high risk)

Although this RPAS was operating in a public space, images were being recorded and were publicly released. As such, the residents had a right to be given the opportunity to consent to being filmed, or consent to their image being released. This could have been accomplished via implicit consent through notifying villagers via local advertisements, signs or other mechanism that the filming would be occurring at a specific day and time, thus gaining implicit consent from those who chose to use the square at that time. Consent could have also been obtained by showcasing the film to villagers (in private) and asking them to explicitly consent to their images being released. Alternatively, the Council would not be required to obtain consent if they anonymised the images.

### Accountability (high risk)

In this scenario, it was unclear to the residents who was operating the RPAS and the purpose for which it was being used. Nor were the residents consulted before the images collected by the RPAS were publicly released. Finally, the filmmaker may be exempt from the relevant legal framework, although this is not certain, and the council refuse to accept liability for the incident on the basis that they draw an analogy between their activity and the use of CCTV. Given each of these points, the residents' only recourse may be judicial.

### Data security (medium risk)

As the personal data is publicly available, there is little risk to the security of data. However, the release of the data publicly considerably undermines the principle of data security, in general.

### Third country transfers (high risk)

Posting the video containing personal information that leads to the identification of those shown in the film is effectively transferring personal data outside of the European Union. Furthermore, some journalists may sell the data to news agencies, many of which may be based in third countries.

### Rights of access, correction and erasure (high risk)

In this scenario, the risks to rights of access, correction and erasure are particularly high. In relation to privacy concerns about outsiders gathering information about residents, this could have been mitigated in a relatively straightforward fashion by inviting residents to view the film before it was released. But, this would not mitigate risks associated with revealing to other villagers what their friends, neighbours and families were involved in during the time of the filming. As such, these rights need to be addressed both before the filming through transparency and consent, as well as after the filming through the rights examined here.

This scenario was discussed at length at the informal workshop with Data Protection Authorities on the 28<sup>th</sup> February, but the scenario was presented as a commercial operation rather than a filmmaking operation. In that discussion, the DPAs were significantly concerned about the legality of the described operation, given the significant data protection risks raised by the scenario. Similarly, in another DPA presentation at the 28<sup>th</sup> May workshop, Dr. Peter

Kimpian noted a number of important breaches of data protection law in a similar scenario presented via YouTube.<sup>16</sup> As described above, although the RPAS operator may have some protection from any legal breaches of the DPD, the Council may not enjoy such protection. These data protection issues should be given serious consideration before the launch of such relatively common missions.

Finally, the ethical risks associated with this RPAS scenario are primarily related to safety and public dissatisfaction rather than discriminatory targeting.

#### Safety (medium risk)

The operation is occurring in a populated area, and there may be some risk to people, animals or buildings if the RPAS were to crash. However, having the RPAS operating in the pilots' line of sight does mitigate some of these potential safety impacts.

#### Public dissatisfaction (high risk)

This scenario describes a situation where residents were upset about the use and release of their image data without forewarning and without their consent. This has a significant potential to have a negative impact on people's perceptions of RPAS in general, when used for civil applications. This could have a knock-on effect on the RPAS industry, which could be prevented with better consideration of transparency and consent obligations.

#### Discriminatory targeting (low risk)

This scenario represents few risks to discriminatory targeting as the whole centre of the village during a busy afternoon was the subject of the video. As such, a range of different types of people would have been captured on the film.

The most significant ethical risks associated with this scenario are related to the public satisfaction elements of the use of RPAS. Although safety represents a broad area of concern across different RPAS missions, it is not specific to this mission. Instead, the risks to public dissatisfaction have to be considered by specifically attending to the privacy and data protection issues raised in this scenario. Ensuring that individuals' personal data is treated respectfully will increase public tolerance of RPAS for a range of different uses.

This scenario raises serious and significant risks for privacy, data protection and ethics as individuals were not aware that they were being filmed, and that the footage was released on the Internet without the consent of individuals who appeared on film. This first aspect of these risks arises in relation to the filming. Whilst, individuals would have recognised a traditional television-style camera as the filmmaker moved around the village, the use of an RPAS meant that some people mistook the filming device for a toy and were unaware of the purpose for which it was being used. Thus, they did not have an opportunity to consent to being filmed in the same way as they would have had a more traditional, recognisable filming device been used. While there may be some ways in which the RPAS operator, and possibly the Council, may be excused from their obligations under the Data Protection Directive as a result of

---

<sup>16</sup> Kimpian, Peter, "The use of RPAS in Hungary and its data protection implications", The civil use of drones: a challenge to privacy?", DG ENTR Workshop, 28 May 2014.  
[http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item\\_id=7496&lang=en&title=Workshop-on-%22The-civil-use-of-drones%2C-a-challenge-to-privacy%3F%22](http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=7496&lang=en&title=Workshop-on-%22The-civil-use-of-drones%2C-a-challenge-to-privacy%3F%22)

artistic freedom, these infringements may need to be considered by a court to determine the precise line between data protection breach and artistic freedom for such scenarios.

#### 8.4.2 Sensationalist journalism

The following scenario presents a different take on the use of RPAS for journalism or filmmaking and focuses on sensationalist journalism. Such sensationalist, semi-professional and citizen journalists may impact privacy, data protection and ethics without the stringent ethical protocols used by reputable, professional journalists in major news organisations. The following scenario illustrates these risks:

*An enormous car accident occurs on a main highway and the first reports from the scene are from a car driver describing events on the local radio. A photographer who specialises in breaking news drives directly to the scene and parks close to the accident site. He launches his RPAS equipped with a high-definition video camera directly connected to his computer, which streams live feed to his personal website. Flying above the highway he spots a car overturned in a field along the road and approaches with his RPAS. He begins streaming the footage to his website and captures and transmits images of two dead bodies just over two meters from the stricken vehicle.*

The vast majority of professional journalists abide by strict ethical controls that also serve to protect the privacy and personal data of citizens, particularly those who are not being targeted by a particular investigation or who are peripheral to a particular news story. Such protections may include anonymisation, blurring of images or the protection of sources. However, citizen journalists or journalists who may be under pressure to produce sensationalist material (e.g., paparazzi) may not be as protective of the privacy and personal data associated with targets and bystanders. This scenario represents one such scenario, with clear impacts for privacy, data protection and ethics that are a direct result of the use of RPAS rather than traditional camera equipment. Specifically, the RPAS allows the semi-professional journalist to breach the accident scene and record and transmit images that contain personal data.

The privacy impacts associated with this scenario include the following:

##### Chilling effect (low risk)

This RPAS mission is specifically targeted at the scene of an accident, and it is unlikely that it would change individuals' behaviour during or outside the accident site because they were concerned that an RPAS could be in operation. However, outside of this specific scenario, the use of drones by journalists could encourage a chilling effect among some types of individuals (e.g., celebrities).

##### Dehumanisation of the surveilled (high risk)

This scenario represents a clear example of dehumanisation of the individuals whose images were captured. The journalist operating the RPAS is not considering the impacts of his filming for the individuals on the ground or their families or acquaintances. Furthermore, the fact that privacy laws give journalists wide scope for breaching privacy expectations may contribute to this specific risk with RPAS, especially in situations where RPAS are able to infiltrate locations that are often inaccessible to human camera operators.

### Transparency and visibility, accountability and voyeurism (high risk)

As mentioned many times in this chapter, the primary difference between RPAS filming and traditional filming is the mobility and visibility of RPAS devices. As such, the fact that the RPAS can infiltrate crime scenes and the fact that it may do so undetected significantly raises the risks to transparency and visibility. Furthermore this scenario also indicates a situation where risks associated with voyeurism are particularly immediate, and the viewing of the remains of individuals caught up in the crash (as well as the viewing of celebrities in being secretly filmed) contains a clear voyeuristic element.

### Function creep (high risk)

In relation to RPAS journalism, there is specific scope for function creep, both in general and in relation to specific missions. First, in general, the use of RPAS for covert filming during serious, professional investigative journalism in high profile cases will encourage other types of journalists (including citizen journalists) to consider RPAS a legitimate journalistic tool, which could lead to significant privacy, data protection and ethical breaches. Second, while RPAS operators may be intending to use their footage for one, particular purpose (e.g., monitoring a festival or a protest), they may be interested in doing a more sweeping investigation using the captured footage (via the high-definition optical camera) to gather information peripheral to their original purpose.

### Body privacy (medium risk)

The use of optical filming, in general, carries very few risks to bodily privacy. However, in this scenario, the body becomes objectified as something about which information can and should be gathered. In consequence, the body itself become dehumanised.

### Privacy of location and space (medium risk)

The RPAS in this scenario is taking images of recognisable individuals in particular places and at particular times. This enables these individuals to be linked with particular places at particular times. Furthermore, the fact that such an RPAS may be relatively undetectable, especially in a situation such as a large-scale accident, means that individuals could not necessarily react to having their images collected.

### Privacy of association (low risk)

This scenario raises few risks to privacy of association in that it is likely filming a set of vehicles and individuals with no relationship to one another, aside from being in a particular place at a particular time. Although some relationships could be inferred from individuals who are co-passengers, this remains a relatively low risk aspect of privacy.

The information outlined above demonstrates the serious potential impacts that the use of RPAS in this scenario could introduce. It is one of the few scenarios that raise risks associated with body privacy, and it also raises high risks in relation to transparency, dehumanisation and function creep. The risks to function creep are particularly worthy of further consideration, given their potential consequences when used by less professional journalists. However, the targeting of a specific scene in this scenario also means that there are low risks associated with a chilling effect and privacy of association, given the specialised scenario

presented. This demonstrates that high-risks to privacy are not “across the board” and must be considered creatively and individually to arrive at a full assessment.

The scenario also raises the following risks to the protection of personal data. Although Article 9 of the Data Protection Directive provides an exemption for journalism and freedom of expression, that exemption is unlikely to support a scenario where journalists display blatant disregard for data protection principles. This is because that exemption is not a blanket exemption. Any compromise of the below data protection principles would be tolerated to the extent that the journalistic endeavour achieves a fair balance between privacy and freedom of expression.

#### Transparency (high risk)

One of the key advantages of using RPAS for journalism is the potential to use the device for covert filming. As noted above, the vast majority of professional journalists will use these devices responsibly for targeted investigations that are in the public interest. Nevertheless, these uses as well as their use by sensationalist, semi-professional or citizen journalists raise significant transparency issues. The subjects of the investigation and visual or audio recording may not realise that the individual operating the RPAS is a journalist, that the RPAS is recording visual or audio information or the purpose for which the visual or audio information may be used. Although there are reasons why journalists are not required to conform to transparency requirements, this scenario, nevertheless, represents a breach of those obligations.

#### Data minimisation (high risk)

This scenario represents a significant risk to data minimisation. There is no information to suggest that the journalist in question has blurred the footage that he is taking of the vehicles (which may be identifiable via number plates), the individuals filmed or the background footage. Furthermore, his mission does not seem to be restricted to taking anonymous footage of the scene, instead he is panning the whole scene, hoping to find something newsworthy or sensational. As such, journalists in such scenarios would likely seek to collect as much information as possible, in case it is useful later. This is a clear breach of the principle of data minimisation as the collection is likely to be considered excessive.

#### Proportionality (medium risk)

There is a long history of journalists taking photographs, audio recordings, and attempting to capture and transmit graphic images in order to communicate important information about particular scenes, incidents and events. The primary risk to proportionality in this scenario is the use of potentially undetectable RPAS that can breach police cordons and other barriers. While the ability to breach such barriers in order to capture footage from protests or other events is certainly an advantage and may represent an important public service, in relation to this specific scenario (i.e., a serious car accident) that is not likely to be the case. Thus, there is some risk to the proportionality principle here in terms of excessive footage, footage of dead bodies and other gruesome details. Proportionality would be met by providing an image of the wreckage that can be taken at a distance.

### Purpose limitation (medium risk)

There is some risk to purpose limitation in relation to journalism using RPAS in general, because while some reputable journalists may use them for specific purposes and adhere to professional ethical standards, less respectable professional journalists and amateur journalists may not use them in the same way. As such, there is some risk that the use of RPAS may expand from serious and investigative journalism to sensationalist or voyeuristic journalism. This specific scenario appears to be an example of such voyeuristic journalism. Yet, the further use of the data recorded for additional purposes does not appear to be a significant risk in this scenario.

### Consent (high risk)

The use of RPAS for journalism raise serious risks to consent whether they are used for investigative journalism, sensationalist journalism or amateur, citizen journalism. This is because RPAS differ from traditional news cameras, which are recognisable to average citizens. As such, if they saw a traditional camera, most individuals would be aware that they were being filmed, and journalists would be able to claim implicit consent through their continued presence at the “scene”. While the potentially covert nature of RPAS is certainly useful and appropriate in a variety of situations, their widespread use could create a generalised consent problem for individuals who, as in this scenario, are not necessarily aware that they are being filmed.

### Accountability (medium risk)

The risks associated with accountability are judged to be “medium” in this scenario. Although it would be difficult to identify the journalist and hold him accountable at the point of filming, he would be identified at the point of broadcast thereby making it easier to effect accountability. As such, the collection of information raises significant accountability risks, while the broadcast of the information makes it clear who might be contacted with complaints, questions and other issues.

### Data security (medium risk)

The risks to data security in this, and other journalistic scenarios, are complex. First, the purpose of collecting the information is often to broadcast it. As such, the data are intended to be released publicly, not protected under lock and key. However, the information collected and not broadcast may be sensitive, and may be of interest to other stakeholders. In consequence, this could represent an attractive store of information for hackers or other individuals who may be able to intercept the transfer of data from the RPAS to the base station, creating some risk to data security.

### Third country transfers (low risk)

The personal information broadcast via the media carries an obvious potential to be transferred outside of the EU. However, it is unlikely that unused information would be transferred.

### Rights of access, correction and erasure (high risk)

As is always the case with information collected via journalistic pursuits, it is difficult for individuals to correct or erase information once it has been broadcast. The use of RPAS by sensationalist or amateur journalists who may not adhere to the same codes of conduct as professional, reputable journalists could significantly impact the well-being and reputation of the person about whom information is collected.

This specific scenario, as well as the use of RPAS by sensationalist journalists or amateur journalists in general, raises concerns where data protection rules apply. In particular, it introduces risks to transparency, data minimisation, consent, rights of access, correction and erasure as well as proportionality, purpose limitation, accountability and data security. Some of these risks are related to risks associated with journalistic filming in general (which RPAS journalists must also consider) while others are specifically related to the ability of RPAS to operate covertly or to film in locations not easily accessible to traditional cameramen. Finally, some of the risks arise in relation to the more covert nature of RPAS in contrast to more traditional news camera equipment. While journalists can claim a number of derogations from data protection legislation, meeting as many data protection obligations as possible would enhance the reputations of RPAS journalists and encourage the public to support their use in appropriate circumstances. Journalistic exemptions are also not intended to support a disregard for social values such as privacy and ethics.

This specific scenario raises a number of ethical issues related to the use of RPAS for journalistic purposes.

### Safety (medium risk)

Journalists operating RPAS in populated areas, or around people in general, may introduce risks to the safety of the people being filmed, as well as any animals or environmental features that are being filmed. This generalised safety risk is not specific to journalism, except that RPAS may be able to access areas that are difficult for traditional camera platforms operated by hand to access.

### Public dissatisfaction (medium risk)

Members of the general public are unlikely to be impacted by the use of RPAS for journalistic purposes. Furthermore, in some cases, members of the public might be interested in viewing sensationalist images captured by RPAS, especially celebrity images. However, in some specific situations, such as the one depicted in this scenario, members of the public might not support the use of RPAS to infringe upon the privacy of victims of the accident and their families. Specifically, the transmission of images of identifiable bodies might cause some public backlash.

### Discriminatory targeting (low risk)

This scenario represents very few risks in relation to discrimination in that it is a collection of individuals that happened to be in a particular place at a particular time who are being captured on film. Yet, the use of RPAS for sensationalist journalism may disproportionately impact celebrities or other specific categories of people.

The ethical risks in this scenario are relatively low, especially given that public dissatisfaction may not be a significant problem in relation to the use of RPAS for journalism, and sensationalist journalism in particular. Furthermore, the risks associated with discrimination are quite low in this scenario, as well as in relation to RPAS journalism in general. Specifically, it is the wealthy and powerful who are more likely to be targets of RPAS journalism, than people who are unable to exercise their rights, either because of a lack of knowledge, resources or confidence.

This scenario specifically sought to outline a likely scenario for RPAS journalism that did not focus on “paparazzi drones”<sup>17</sup>. And, the scenario outlined here does pose considerable risks both to privacy and data protection, especially because of the fact that people caught up in the accident are unlikely to be aware that they are being filmed, because the RPAS can “breach” the scene of the accident in a way that a human camera operator would find difficult and because the eventual footage included identifiable images of bodies. However, the use of RPAS for journalism cannot ignore the potential use of RPAS by sensationalist journalists or amateur journalists that may not adhere to the same ethical and professional codes of conduct that more professional or reputable journalists take as a given. As such, some controls ought to be considered in order to address these concerns associated with the use of RPAS for journalistic purposes, in general.

## 8.5 Telecommunication providers

While government authorities, law enforcement authorities, journalists and artists are exempted from some privacy and data protection regulations, telecommunication providers must adhere to a different sub-set of regulations, many of which are relevant to privacy and data protection. Furthermore, the protection of communications from intrusion has always been high on the agendas of governments and lawmakers. This sub-section examines a realistic scenario for the use of RPAS to provide telecommunication services.

*A national telecommunications provider launches a new service intended to provide high-bandwidth, mobile broadband to under-served rural areas. The RPAS routes local mobile signals to the company’s communications satellite, and no data is stored by the RPAS. However, a local teenager has found a way to hack into the wireless signal and can view information about her neighbours’ communications and whereabouts.*

In this scenario, the RPAS is not implicated in the collection, processing or storage of data; instead, it is simply being used as a relay device. No data, including personal data, are being collected by the telecommunications company that would not be collected as a result of normal operations. As such, the only change to normal telecommunication operation represented by the RPAS is the relay of signals wirelessly to a local device. The chief privacy, data protection and ethical issues here are related to the potential insecurity of data as it passes through the RPAS wirelessly. The scenario presented here represents an illegal interception of this data, which is facilitated by the use of an RPAS, rather than a wired device. Given the illegal nature of this data collection, and the obvious privacy, data protection and ethical issues associated with any illegal information collection, this sub-section does not analyse this scenario in detail. However, it is the responsibility of the telecommunications provider and/or

---

<sup>17</sup> Villasenor, op. cit., 2013,

the RPAS manufacturer (in some circumstances) to ensure that the data that passes through the RPAS is appropriately secured.

## 8.6 Private individuals

Finally, as noted in previous chapters, the use of RPAS by private individuals for personal uses is of most concern to almost all RPAS stakeholders, including Data Protection Authorities and other regulators. Furthermore, these stakeholders are almost un-regulated as a result of the “household exemption” in the Data Protection Directive and the proposed General Data Protection Regulation. A typical scenario for the use of RPAS by private individuals includes the following:

*A local aircraft enthusiast purchases a drone to curb anti-social behaviour in his neighbourhood. He films teenagers’ hanging out in his neighbour’s front garden, and sometimes uses the drone to follow young people home and identify where they live. The drone is small and very quiet, and the teens are often unaware that they are being filmed.*

The collection of personal data by private individuals for “household use” represents a grey area in relation to privacy and data protection. In relation to privacy, it is difficult to identify when privacy is being breached, even though the consequences may be obvious. Furthermore, while private individuals are technically liable for privacy breaches, privacy is notoriously difficult to define, and breaches can be difficult to identify in a strictly “legal” sense. In addition, private individuals can claim derogation from data protection legislation via the household exemption. As such, it is difficult to prosecute individuals for privacy or data protection breaches in both circumstances. Nevertheless, the implications for privacy, data protection and ethics are one of the most pervasive when RPAS are used by private individuals, given the potential they have to stoke dystopic imagery and public dissatisfaction in relation to RPAS use. In chapter 6, professional RPAS users, Data Protection Authorities, Civil Aviation Authorities and civil society organisations all identified private individuals as the category of RPAS user that generated the most significant risks to privacy, data protection and ethics.

The privacy impacts associated with this scenario include the following:

### Chilling effect (high risk)

This RPAS mission has significant potential impacts on the use of public space in the neighbourhood in question, as residents, visitors and other knowledgeable individuals may be concerned that their neighbour is monitoring their activities. This could encourage them to adjust their behaviour at all times when they are outdoors, because they are not sure whether or not they are being monitored. Although individuals do not have a legal right to privacy when they are in public space as such, they are protected against the systematic recording of their activities.

### Dehumanisation of the surveilled (medium risk)

In this scenario, the neighbour operating the RPAS does not appear to be separated from the human consequences of his actions on the ground. However, he is objectifying the young people to some extent, by not respecting their rights to privacy through his systematic recording of their activities.

### Transparency and visibility, accountability and voyeurism (high risk)

There is a considerable risk to transparency, visibility and voyeurism associated with this scenario. The young people do not seem to be aware that they are being filmed, and as such, there is no indication that the RAS operator has made his activities transparent. Furthermore, it is possible that the young people have not even noticed the RPAS and are unaware that it is equipped with optical imaging and recording capabilities. The monitoring and recording appears to be related to one specific purpose (i.e., identifying anti-social behaviour), but there is significant scope that the monitoring could become voyeuristic.

### Function creep (high risk)

The neighbour in question may restrict his activities to monitoring the activities of this particular group of young people. Or, he may move on to other targets for other purposes. As such, the possibilities for function creep in relation to this particular scenario are considerable. Additionally, in general, once private individuals start using RPAS for a small set of purposes, these purposes will likely expand alongside the expected expansion of RPAS usage in other civil areas.

### Body privacy (low risk)

The use of optical filming, in general, carries very few risks to bodily privacy.

### Privacy of location and space (high risk)

Like the scenario associated with the police use of thermal imaging, this scenario represents significant risks to privacy of location and space. The RPAS operator has a record of individuals who are gathered at a particular place and at a series of specific times. He also records the movements of the young people, including which houses they enter, which appears to be an attempt to gather additional personal information about those individuals, such as their names and addresses.

### Privacy of association (high risk)

The filming of young people gathered in front of his neighbour's yard is also a considerable breach of privacy of association, as the gathering of young people together at a particular home indicates a relationship among those young people and with the occupier of the house. Furthermore, following young people as they move about the neighbourhood and enter particular homes also indicates a relationship with those living inside.

In this scenario, the risks to privacy are judged to be "high" across the board (with the exception of risks to bodily privacy and dehumanisation of the surveilled). The risks associated with a "chilling" effect, transparency, privacy of location and space and privacy of association are particularly significant and worthy of further consideration. These infringements may prevent residents from using their neighbourhoods in the ways in which they wish, and may make them feel as though they are "under surveillance" every time they leave their homes. This feeling of being "under surveillance" may be further intensified if RPAS are used by private individuals to peer into back gardens, or even inside the homes, of friends and neighbours. These issues are also intensified given the transparency issues associated with RPAS, in that they may operate almost undetectably. If individuals are not

sure whether they are under surveillance, this can cause stress, paranoia and other negative effects.

As noted above, private individuals may claim exemption from the Data Protection Directive in relation to the processing of information for household use, and as such are not subject to data protection obligations. However, the risks associated with data protection are so intense in this scenario, that they are worthy of consideration.

#### Transparency (high risk)

In this scenario, there is no indication that the young people are aware that they are being filmed, or that the RPAS operator took any steps to inform the young people that they are being filmed. As such, the filming of these individuals using and RPAS, and the subsequent recording of those images is completely non-transparent. The young people do not appear to have any ability to take steps to avoid being captured on film.

#### Data minimisation (high risk)

In this scenario there is no indication that any steps are being taken to minimise the amount of data collected by young people. In contrast, by undertaking a systematic recording of young peoples' activities and also following them as they move around the neighbourhood, this RPAS operator appears to be attempting to collect the maximum amount of information possible using the RPAS.

#### Proportionality (high risk)

The use of a potentially undetectable RPAS is certainly not the least intrusive technology possible to capture the desired information about the young peoples' anti-social activities. The RPAS operator could keep a journal of the young peoples' activities, make frequent reports to the police or use some other, less intrusive method to strengthen his complaint to authorities.

#### Purpose limitation (medium risk)

As discussed in relation to function creep, there is a possibility that the neighbour may move on to other recording projects once the young people have grown out of this particular phase. There is no way to prevent this particular RPAS operator, as a private individual, from undertaking additional recordings, or from using the data recorded for additional purposes not related to the young people's anti-social behaviour.

#### Consent (high risk)

In this scenario, it appears that the young people are unaware that they are being filmed outside the neighbour's house, and that they are occasionally being followed. As such, they have not been given any opportunity to consent to the collection of their images as personal information, nor have they been given an opportunity to alter their behaviour to prevent the recording of undesirable activities, either by moving indoors or choosing not to participate in those activities. Individuals have a right to ensure that images of them are not recorded without their consent, and this use of RPAS represents a clear breach of that right.

### Accountability (high risk)

As noted in other scenarios, when risks to transparency and consent are high, the risks associated with accountability and rights to access, correction and erasure are also elevated, given the interaction and interdependency between these elements of personal data protection. If individuals are not aware that they are being filmed, and are not given the opportunity to consent to that filming then it is difficult for those individuals to hold the person or organisation that is conducting the filming to account. In this scenario, this issue is further exacerbated by the fact that the collection of data by a private individual is not subject to the obligations outlined in the Data Protection Directive, nor will they be subject to the Proposed General Data Protection regulation.

### Data security (high risk)

There is some risk to data security in that the RPAS operator in this scenario does not appear to be taking any measures to protect the integrity of the data flow between the RPAS and his operating station, nor are any protective measures mentioned in terms of data security once the footage is stored. Furthermore, he may also broadcast it at a later stage as by posting it to YouTube or some other site where it might be publicly accessible.

### Third country transfers (low risk)

It is unlikely that the information would be transferred to a third country.

### Rights of access, correction and erasure (high risk)

This scenario also represents another manifestation of the interacting risks between transparency, consent and accountability. If individuals are unaware that their data is being collected, have not been given the opportunity to consent to that collection and the data collector is not being held accountable for that collection, then individuals have almost no opportunity to exercise their rights to access the data, correct it or erase it. This leaves individuals in a precarious position in relation to other private persons, which they are not subject to in relation to commercial RPAS operators and some government operators.

As identified by all of the groups of RPAS stakeholders consulted in the course of the research, private users of RPAS pose the greatest risks to data protection, which is compounded by the fact that they are not subject to the 1995 Data Protection Directive. Additionally, private users will also not be subject to the Proposed General Data Protection legislation. This leaves an important gap, where individuals may experience significant impacts related to consent, proportionality, a chilling effect and the exercise of their rights to access correction and erasure. However, excluding the ability of RPAS to operate almost invisibly and to access spaces that are difficult for human camera operators to reach, the data protection risks associated with RPAS are not that different from mobile phone cameras, which are beginning to be seriously addressed.

Alongside these privacy and data protection risks, the scenario introduces the following ethical risks:

### Safety (medium risk)

Any RPAS operating in populated areas will pose risks to people's safety, as well as risks to personal property. This is particularly the case when RPAS are used by amateurs and enthusiasts rather than trained professionals.

### Public dissatisfaction (high risk)

The possible use of RPAS for the purpose of neighbours "spying" on neighbours carries considerable potential for public backlash. The risks outlined above related to voyeurism and a "chilling" effect are likely to negatively impact people's use of neighbourhood spaces and private spaces (such as back gardens). The stakes are also raised when young people are involved and are perceived to be targets of adult individual's monitoring and recording. All of these issues could contribute to a generalised public dissatisfaction with RPAS, which could have a negative impact on the proliferation of RPAS for a range of civil applications.

### Discriminatory targeting (high risk)

When private individuals utilise RPAS, there is an increased likelihood that the missions for which they are used will disproportionately impact young people and women. In this particular scenario, young people are the target of the RPAS operator's mission, due to perceived anti-social behaviour. However, these groups are also the least likely to exercise their rights or pursue illegal uses of RPAS.

Although this analysis has revealed that individuals are under the highest threat in relation to data protection from private individuals' use of RPAS, they are least protected from these operators. This leaves people more vulnerable vis-à-vis their peers than other actors such as government authorities and commercial organisations. While the risks associated with government or commercial operations clearly have high potential impacts on individuals' life chances, their unfettered use of public space, and semi-private space (e.g., neighbourhood greens, front gardens, etc.), is certainly at risk in this scenario. In addition, the risks to public dissatisfaction and discriminatory targeting have the potential to undermine the wider rollout of RPAS for a range of civil applications. The lack of meaningful regulatory oversight of amateur, private RPAS users may represent a stumbling block to the industry in general. As such, we recommend that RPAS manufacturers encourage private users to educate themselves about or consider privacy issues when operating these devices. This could take the form of an instruction leaflet, or information boxes when purchasing RPAS online. At the European level, this could be managed and imposed through an aviation safety regulation and subsequent CE marking of the product to indicate conformity with European legislation. However, this would require the cooperation of European and Member State bodies in charge of aviation and market regulation.

## **8.7 Summary**

This analysis has identified a number of privacy, data protection and ethical impacts associated with typical and/or realistic scenarios for commercial, law enforcement, journalistic or artistic and private RPAS operators. These potential impacts range from negligible to high risks, and are largely depending on two factors. First are characteristics specifically associated with RPAS, including the ability to fly and collect information almost undetectably and the ability to access spaces that are difficult for humans or traditional

technologies to access. Second are characteristics associated with the payload and type of data collected by the RPAS, including visual images, thermal images, sounds, location data and others.

Given the two factors identified above, and the associated heterogeneity of RPAS capabilities and applications, the potential risks associated with RPAS are difficult to pin down and categorise in a comprehensive way. These impacts vary depending on the purpose for which the RPAS is being used, the types of data collected and the operators' focus. Furthermore, as RPAS capabilities and applications proliferate, future risks are difficult to predict.

Furthermore, law enforcement authorities, journalists and filmmakers, telecommunications providers and private individuals are not subject to the same privacy and data protection regimes as commercial organisations using RPAS for the missions described above. However, they do have other legal frameworks within which they must operate, and they ought to consider the importance of adhering to as many privacy and data protection conventions as possible in order to ensure that the public become or remain supportive of their use of RPAS in general. This is particularly important as many of these missions involve the potential collection of personal data, as well as storage and subsequent use.

The following chapters, but especially Chapter 13, will outline some specific policy recommendations to assist RPAS operators, especially commercial operators, in meeting data protection obligations and addressing potential privacy and ethical issues. This analysis has, however, indicated some initial directions. First, all RPAS operators should offer members of the public clear and detailed information about the operation of RPAS in their area, the purposes for which it is being used and the identity of the operator. This transparency activity will assist RPAS operators in meeting and addressing many of the potential risks associated with RPAS, including transparency, a chilling effect, function creep, consent, accountability and enabling members of the public to exercise their rights. RPAS operators should also involve members of the public in discussions about acceptable and unacceptable uses of RPAS. This will decrease public dissatisfaction and build consensus that will offer more firm support for the RPAS industry in general.

## 9 THE ADEQUACY OF CURRENT EU REGULATORY FRAMEWORKS

### 9.1 Introduction and overview

In Chapter 4 of this report, we examined the relevant European existing privacy and data protection laws that may apply to civil drones. Furthermore, in Chapters 7 and 8 of this report, we identified the risks posed by the different civil RPAS applications. The present assesses the adequacy of this European privacy and data protection legal framework. In order to do so, we will firstly examine whether all categories of RPAS operators/applications we have identified are covered by the regime (*Section 9.2*). As a reminder, Chapters 4 and 5 demonstrated that there are five types of drone operators: Commercial operators including corporations and professionals, journalists, state agencies, telecommunication and Internet providers and private individuals including hobbyists and private users. Secondly, we will examine if, for the operators covered by the European legislation, the rules adequately address all risks these operators can pose by using drones in their activities. In this regard, we will particularly examine if the current European legislation encompasses sufficient high-level protection standards to mitigate the issues posed by the commercial operators using RPAS (*Section 9.3*). Finally, we describe the problems that lie at the enforcement level. In this context, we will study, in-depth, each difficulty that commercial operators encountered processing personal data through the means of drones to implement the data protection requirements and individuals' rights. In addition, we will also see that data subjects might have certain difficulties in exercising their rights. Finally, we will discuss the enforcement concerns faced by the data protection authorities (*Section 9.4*).

### 9.2 Current and emerging RPAS applications not covered by the current European privacy framework

In this present section, we will analyse whether certain RPAS applications are covered by the current privacy and data protection framework. Above all, we emphasise that the current Directive 95/46/EC applies to all personal data processing, collection, storage and disclosure for commercial purposes. As such, commercial operators are well covered by the European data protection legislation. Furthermore, commercial operators will be still covered by the European framework based on information contained in the draft of the GDPR, once it is adopted.

#### ***Problem 1. All operators – RPAS used in public places: no privacy regulations***

In the first part of this research project, we argued that RPAS technology poses privacy as well as data protection concerns. A drone that does not process data might cause privacy issues. Furthermore, if it is used for processing personal data, it will not only engender privacy concerns but also data protection risks. However, we also found that although the rights to privacy and data protection are both recognised at by the European Convention of Human Rights as well as the European Union Charter (primary sources), only data protection law is regulated by secondary sources (Convention 108, DPD, DPF, etc.). Regarding the right to privacy, there exist no regulations at the European level and no obligations and principles to ensure this right, unlike in the data protection law. However, Article 8 ECHR and the case-law of the Strasbourg Court have given a bit of substantive content to this right by issuing certain obligations that privacy intruders have to respect. Article 8(1) ECHR requires that organisations, public authorities and individuals do not interfere in the

enjoyment of the private sphere of another individual, except if this interference is in accordance with the law, pursued a legitimate aim and is necessary in a democratic society (Article 8(2) ECHR).<sup>1</sup>

Applied to the context of the RPAS technology, this means that RPAS operators cannot fly their drones in the private sphere of individuals unless they can justify the interference according to the sub-mentioned conditions. For instance, a farmer which uses his drone for crop dusting purposes cannot pass above the backyards of his neighbours as, in principle, he will not be able to justify such interference. In the same vision, a company which uses drones for delivering pizzas cannot, a priori, pass above a schoolyard where children are playing. Nevertheless, a State agency that uses a drone for monitoring the property of a man suspect of murder can easily justify this interference in the private sphere of this man. So in the private sphere, privacy risks are mitigated by the prohibition to interfere with the private sphere and chilling effect, mission creep and other privacy issues are addressed.

However, in public places, individuals expect less privacy, therefore Article 8 ECHR will, a priori, not apply. Therefore, in public places where a chilling effect can be also felt when a drone is flying above someone's head, nothing prevents such usage and certain privacy concerns will remain.

### ***Problem 2. State agencies - RPAS processing personal data in a purely domestic context***

Like for private individuals, we have discussed in the previous chapters that State agencies will use RPAS technology in their activities. Being the primary actor of surveillance, law enforcement authorities mostly use and will use RPAS technology for monitoring people and objects in surveillance operations.<sup>2</sup> However, we also recognised that State drones might also be used in other applications like regulatory enforcement and civil protection.

Furthermore, we found in our analysis of risks and our surveys that the use of RPAS by such State bodies may have great impacts on individuals especially from a privacy, ethics and data protection perspective. As a reminder, we had particularly pointed out privacy, data protection and ethical risks related to chilling effect, function creep, dehumanization of surveilled into the hands of surveillants, accountability, transparency, privacy of location and space, privacy of association, transparency, data minimisation, proportionality, purpose limitation, consent, individual rights, safety, public dissatisfaction and discriminatory targeting. We also observed that in comparison to the other type of drones' operators, law enforcement authorities raise higher risks and are often described by watchdog reports and the public as the most controversial users of civil drones. This is explained by the fact that contrary to other operators (private, commercial), the police are legally permitted to operate covert and overt surveillance operations on people and things which necessarily lead to more risks of abuse and violation. Additionally, the cost of new technologies declining and deployment of new security technologies increasing, police will soon have access to very intrusive payloads like "smart surveillance technology" including abnormal behaviour recognition, ANPR systems, technologies which will be unlikely to be commercialised to other kind of operators. Therefore, as explained by scholars Paul de Hert and Vagelis Papakonstantinou the

---

<sup>1</sup> Council of Europe, European Convention on Human Rights, Rome, 04.11.1950, Article 8.

<sup>2</sup> Physical surveillance (visual surveillance and aural surveillance), location surveillance, communications surveillance, dataveillance, assemblages, personal and mass surveillance.

particularity of the sector requires higher level privacy standards, “the police have a broader task, ranging from criminal investigation, crowd control or politic policing, a series of functions often exercised without transparency, making control and data protection more vital”.<sup>3</sup>

However, despite the importance to set up high-level protective data protection rules in the context of law enforcement processing, the Data Protection Directive 95/46/EC, excludes explicitly its application to data processing activities in security and criminal matters “*This Directive shall not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law*”. This exclusion comes from the fact that in the pre-Lisbon era, data processing carried out by police and criminal justice authorities were part of the former “third pillar”, a pillar of shared competences between the European Community and the Member States. Therefore, whilst the economic sector and the public administration were regulated by the DPD, data processing by the security and criminal sector were left unregulated. However, recently the European Decision-Framework 2008/977/JAI was adopted, although this act only covers police and judicial data exchanged among Member States, EU authorities and associated systems. In the context of RPAS, this scope limitation means that only the data processed through the means of a State RPAS which are exchanged between law enforcement authorities in a European or International contexts fall under the application of the DPDF. So personal data processed by a governmental drone for national law enforcement or judiciary cooperation are not regulated at the European level.

However, it is noteworthy that although no European subsidiary legislation covers these processing, the CoE Data Protection text (Convention 108), Article 8 ECHR and Article 8 of the European Charter which provide some data protection principles apply.

### ***Problem 3- Private individuals and hobbyists - RPAS processing personal data for purely domestic purposes***

In the previous chapters, we have firstly emphasised the increasing use of drones’ by individuals and demonstrate that private operators using RPAS for photography, mapping, monitoring people, etc. for personal purposes raise a wide range of privacy and data protection risks: chilling effect, voyeurism, transparency, visibility, accountability, function creep, privacy of location and space, privacy of association, data minimization, proportionality, consent, accountability, data security individual rights. Secondly, we have considered whether the current European data protection framework apply to RPAS technology and address those risks. However, in our study we observed that RPAS operators processing personal data for recreational and personal purposes are exempted from the application of the Data Protection Directive 95/46/EC.<sup>4</sup> Although this exemption seems

---

<sup>3</sup> De Hert, Paul, and Vagelis Papakonstantinou, “The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for”, *computer law & security review*, Vol. 25, 2009, pp. 403–414.

<sup>4</sup> “2. *This Directive shall not apply to the processing of personal data: - by a natural person in the course of a purely personal or household activity*”; European Parliament and the Council, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to

justified when it concerns the database of names and addresses or relatives and friends that an individual kept on his/her PC, this exemption is well more controversial in the two following examples:

**Example 1.**

A husband has some doubts on the fidelity of his wife and suspects that she is leading a double life. Having recently bought an RPAS fitted with a camera, he decides to launch his new tool in the park where her wife usually goes during her lunchtime and starts to film individuals walking into and out of the park.

**Example 2.**

A father buys a mini-drone equipped with a camera to monitor his son walking to the bus stop every morning. By monitoring his son, he is also monitoring and recording other children waiting at the bus stop.

These scenarios raise a number of critical questions. Who would guests call to report the capture of image without authorization? What happens if the drone which has processed massive amount of data is hacked by the drone of a neighbor? What occurs if an image is re-used years later for commercial purposes? Who deals with eventual abuses? Currently, these questions remain unanswered by the privacy and data protection legal framework.

### **9.3 Legal gaps in the current and proposed regulatory framework**

We have previously found that RPAS operators using drones for processing personal data for commercial purposes are covered by the current European data protection regime, more particularly by the Data Protection Directive 95/46/EC. Nonetheless, the present section will show that although commercial applications are covered, several legal gaps remain to adequately address all risks raised by the usage of drones in such contexts.

#### ***Problem 1. Commercial operators - Lack of preventive and remedial security data protection measures***

##### *The Data Protection Directive 95/46/EC*

In our analysis of the risks inherent to the RPAS technology, we have emphasised that thanks to their multitude of payloads and aerial ability, RPAS operators may (unintentionally, although indiscriminately) process and collect a significant amount of personal information. Furthermore, RPAS collectors have acknowledged that through the means of RPAS, they accidentally process personal information not necessary for the purpose of the flight. Consequently, this study of the RPAS characteristics and risks enable us to realise that there is a real need for preventive security measures to mitigate this security processing risks inherent to RPAS technology. Furthermore, we also pointed out that many newspapers and IT researchers have publicised that the content of a drone can be easily hacked by the operator of another RPAS. Thus, such hackers can then access to personal information collected by the

---

the processing of personal data and on the free movement of such data OJ L 281, 23.11.1995, (“Directive 95/46/EC”), Article 3.

initial drone. To avoid the risks related to such accidental disclosure, remedial security measures are also needed.

In this respect, we have to analyse whether the current data protection framework provides **sufficient preventive and remedial safeguards** to avoid these risks.

In our study of the Data Protection Directive 95/46/EC, we observed the security of processing requirement at Article 17:

*“1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.*

*Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected”<sup>5</sup>.*

By using the words “*against accidental destruction or loss*” in its first alinea, the DPD only requires data collectors to adopt security measures to avoid breaches after the collection of personal data, at the stage of the disclosure.

It is only at the second alinea that the DPDP requires the adoption of security measures to address “*the risks represented by the processing itself*”. Furthermore, the notion of “appropriate technical and organizational measures” is vague and there is no further guidance information about which kind of measures commercial operators should adopt. Furthermore, this obligation to undertake preventive security measures to address eventual processing risks depends on two considerations “*the state of the art and the cost of their implementation*” and once again, neither “the concept of the state of art”, nor “the cost of implementation notion” are defined.

Therefore, although such provision entails that RPAS operators adopt security measures to avoid unauthorised disclosure like content hacking, it does seem to systematically require that RPAS operators adopt preventive security measures to address the risks related to the processing (the inadvertent data processing and the indiscriminate collection of massive amount of data). Furthermore, it does not give any indications on how and which kind of measures should be adopted. Finally, the Directive does not contain a duty to notify the DPA or the data subject when a data breach occurs. Therefore, in cases where personal information processed by RPAS are accidentally disclosed, no action must be taken by the commercial operator to mitigate the effects such data breach may provoke on the individuals’ life. Such lack of clear preventive and remedial measures addressing the security risks raised by commercial RPAS makes clear that it remains several legal gaps within the European data protection law.

The data protection being under reform, we can expect that the future European regime will bring some changes. Although the General Data Protection Regulation is still under the

---

<sup>5</sup> Directive 95/46/EC, Article 17.

decision-making process, we can already examine if the provisions of the draft issued by the Parliament the 12<sup>th</sup> March 2014 improves the *status quo*.

### *The Proposed General Data Protection Regulation*

In January 2012, the European Commission delivered the General Data Protection Regulation proposal aiming to replace the current DPD. This draft is still currently under review but it has already been amended by the European Parliament. In our examination of the future data protection framework, we found that, in general, the text proposed brings higher-level data protection safeguards and a more adapted text to the development of new technologies.

Regarding to the above mentioned risks, in relation to data processed by commercial RPAS, and the need of preventive and remedial security measures to address such risks, the GDPR seems to bring relevant new elements. Indeed, we found that the Regulation firstly makes a clear recognition of the data minimization principle. Secondly, it expressly includes two new preventive security instruments, the Data Protection Impact Assessment (DPIA) and the Data Protection by Design measures. Finally, we remark the introduction of a duty for collectors to notify the DPA and the data subject in case of data breach.

The **data minimization principle** figures at Article 5 of the GDPR which encompasses the core of the data protection principles. This provision stipulates “*Personal data shall be: (c) 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 (data minimisation). e) kept in a form which permits direct or indirect identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research or for archive purposes in accordance with the rules and conditions of Articles 83 and 83a and if a periodic review is carried out to assess the necessity to continue the storage, and if appropriate technical and organizational measures are put in place to limit access to the data only for these purposes (storage minimisation)*”<sup>6</sup>.

In reality, this data minimisation already exists in the current DPD as it stems from the necessity, purposes limitation and proportionality principles. However, the GDPR clarifies and expressly enshrined this principle. In practice, for RPAS collector, this data minimisation implies that they must process, collect and store the “only personal data which is necessary to obtain certain specified and legitimate goals”. Second, it further requires that the personal data should be destroyed as soon as it is no longer relevant to the achievement of these goals. So this principle expressly prohibits that RPAS collectors process a massive amount of personal data in an indiscriminate way as well as the inadvertent collection of personal information.

In addition, the GDPR brings a new element to the security data processing requirement, **the Data-Protection-by-Design approach**. Whereas we have seen that this principle in the DPD requires from the collectors to undertake security measures to avoid processing and disclosure

---

<sup>6</sup> European Parliament, The legislative resolution of 12 March 2014 on the 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)0011 – C7-0025/2012 – 2012/0011(COD)), Article 5.

risks, the GDPR goes a lot further as it incorporates the obligation to implement “*appropriate technical and organisational measures are taken, both at the time of the design of the processing and at the time of the processing itself to ensure that the requirements of this Regulation are met*”.<sup>7</sup> So by incorporating this Data-Protection-by-Design approach, the GDPR requires that the RPAS collectors already embody the data protection principles including among other the data minimization principle in the design of the RPAS. By requiring that data collectors use such type of RPAS, obviously the GDPR will in reality implicitly obligates manufacturers to build and design drones respecting data protection principles.

Furthermore, Article 33 provides that data collectors must carry out a **Data Protection Impact Assessment** prior processing when such processing operations are likely to present the following risks:

“(a) *processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;*

(b) *processing of special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large scale filing systems;*

(c) *profiling on which measures are based that produce legal effects concerning the individual or similarly significantly affect the individual;*

(d) *processing of personal data for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;*

(e) *automated monitoring of publicly accessible areas on a large scale;*

(f) *other processing operations for which the consultation of the data protection officer or supervisory authority is required pursuant to point (b) of Article 34(2)*”<sup>8</sup>.

In the context of RPAS, this DPIA requirement implies that RPAS collectors should assess the eventual risks related to the processing, collection, storage and disclosure of personal data. After this analysis of risks, if their processing operations are likely to present the above mentioned risk, they will have to adopt additional safeguards to mitigate those risks.

Finally, Article 31 of the GDPR deals with a notification requirement in circumstances of personal data breaches. RPAS controller must “*without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority*”<sup>9</sup>. Additionally, Article 32 prescribes the communication of a personal data breach to the data subject. It states: “*1. When the personal data breach is likely to adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay. The communication to the data subject shall be comprehensive and use clear and plain language. It shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of Article 31(3) and information about the rights of the data subject, including redress*”<sup>10</sup>.

---

<sup>7</sup> European Parliament, The legislative resolution of 12 March 2014 on the General Data Protection Regulation, Article 23.

<sup>8</sup> European Parliament, The legislative resolution of 12 March 2014 on the General Data Protection Regulation, Article 33.

<sup>9</sup> Ibid., Article 31.

<sup>10</sup> Ibid., Article 32.

Consequently, with the adoption of the GPDR, RPAS operators will have to use a RPAS which is designed to respect, among others, the data minimization principle. Furthermore, commercial operators will have to conduct a DPIA before operating processing activities when they are likely to present specific risks. Finally, they will also be required to notify the DPA and the data subject in case of accidental disclosure. It is clear that the GDPR, by incorporating such pro-active and remedial requirements, will better address the security risks that commercial operators may pose by using drones for processing personal information.

*Scenario on landmarks images.*

Such considerations can be related to the scenario studied in the Chapter 8 on landmarks. As a reminder, we had seen in this scenario that a commercial operator flying high over a historical city taking footage of various landmarks capturing images of tourists initially not identifiable can become easily identifiable with the use of specific software. In this regard, we had emphasised the risks surrounding the disclosure of images become identified data.

Under the current Directive, data collectors are only required to adopt “technological and organisational measures” to prevent such risks. Which kind of measure? At which stage? The Directive remains silent on the issues.

Under the proposed GDPR, the company collecting data will be required to adopt a RPAS which integrate the data minimization by design like a drone mounted with a camera which blurs faces. Furthermore, being likely to pose some risks, the collector will have to conduct a PIA before the flight. Finally, in case of images of tourists would be still identifiable and that these footages would be accidentally disclosed, the company would be in charge to inform such data breach to the DPA and the tourists concerned.

***Problem 2. Journalists – The exemption “for journalistic purposes”***

As mentioned in the previous chapters, by being light, remotely, small and cheap, RPAS are by nature the perfect kit accessible to every journalist. This has even been confirmed by the Reuters Institute for the Study of Journalism at the University of Oxford which states “drones have already been used by journalists, from the Australian television channel that took aerial images of a controversial immigrant detention centre to paparazzi using the technology to photograph heiress Paris Hilton on holiday”.<sup>11</sup> Although it is apparent that the usage of drones in the journalism field may be very useful, we also found that due to the atypical features of RPAS, journalists are likely to present risks related to privacy, data protection and ethics as they can easily undertake covert surveillance on individuals, especially public figures<sup>12</sup>, feed the scandal press and perform voyeurism activities.

In our analysis of the provisions of the Data Protection Directive, we observed that this instrument encompasses an exemption to certain provisions, including data protection principles and data subject rights, in the interests of freedom of expression. More precisely, Article 9 provides that such derogation shall apply to “*the processing of personal data*

---

<sup>11</sup> *The Telegraph*, “The brave new world of 'drone journalism’”, 19 June 2013.

<http://www.telegraph.co.uk/technology/news/10129485/The-brave-new-world-of-drone-journalism.html>

<sup>12</sup> The Queen of Cambridge, the Belgian King and many other public figures have already been subject of illegal covert surveillance by Medias with a drone.

carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right of privacy with the rules governing freedom of expression”.<sup>13</sup> If such derogation clause is understandable as it attempts to balance the right to private life and the freedom of expression, the notion “for journalistic purposes” is unclear and the Directive gives neither a legal definition nor insights to know who should be considered as “journalist” under the exemption. Furthermore, this legal vacuum surrounding the notion of journalism poses real concerns since the function of journalism has evolved. As explained by the scholar Vineet Kaul, “the high tech revolution has significantly altered the way the public obtains its news and information, and has deprived the mass media of its traditional monopoly”.<sup>14</sup> Therefore, besides the traditional media we have seen emerging new type of “media”, today called bloggers, Youtubers, paparazzi, “citizens-journalists”<sup>15</sup> and “new communication formats, often called ‘social media’—such as blogs, Twitter, Facebook and YouTube—to distribute information and express opinions about an range of matters public and private”<sup>16</sup>. However, contrary to traditional journalists, these “new media” journalists do not always follow professional rules of journalism including the privacy, moral and ethical norms of the profession. So it is quite unfortunate that by using drones in their activities, these new media may greatly increase already present data protection risks related to the use of this atypical technology. Therefore, if this potential exemption clause applies also to them, such risks will not be addressed.

#### *Scenario Journalist. Organisers of a concert event*

As a reminder, we have seen in the concert scenario that organisers (collectors) of a concert have contracted a drone operator (processor) to taking footage of people in the crowd enjoying themselves. Attendees of the event were informed of the filming via a short notification in the terms and conditions statement when they bought their tickets online. These footages and film are used for making a video which is released on Youtube for promoting the concert of next year. Against this background, we had studied privacy, data protection and ethical high risks related to transparency and visibility, accountability and voyeurism, function creep, proportionality, discrimination, etc.

Given the lack of definition of the exemption “processing for journalistic purposes” in the directive, we can wonder *in casu* whether the organisers of the concert should be considered journalist for the scope of the exemption.

This lack of a clear definition poses also a harmonisation issue among the Member States. Indeed, we will examine further that this provision is interpreted quite differently in the Member States. In the context of RPAS, this issue of non-harmonisation is a particular concern as many drone operators process data in different Member States. Therefore, a drone operator that does not fall under the exemption of Article 9 in his or her Member States, but who knows that he or she will fall under this derogation and so escape at the application of the majority of the DPDP obligations in another Member State, will be tempted to establish in

---

<sup>13</sup> Directive 95/46/EC Article 9.

<sup>14</sup> Kaul, Vineet, “Journalism in the Age of Digital Technology”, *Online Journal of Communication and Media Technologies*, Vol. 3 – Issue: 1, India, 2013.

<sup>15</sup> Flanagan, Anne, “Defining ‘journalism’ in the age of evolving social media: a questionable EU legal test”, *International Journal of Law and Information Technology*, Vol. 21, No. 1, 2012, pp. 1–30

<sup>16</sup> *Ibid.*

this second Member States.<sup>17</sup> So this lack of definition will likely lead to a forum shopping for the law of the Member States encompassing the largest interpretation of the notion “journalistic purposes” and then, a lower protection for individuals. Furthermore, there is also a legal vacuum surrounding the scope of the “necessary” requirement. Although it makes clear that the Directive does not give an automatic blanket exemption in every case, it is less evident to know when we are in the circumstances where it is necessary to strike a fair balance.

In 2008, the ECJ has issued a decision in which it interprets how this concept of “journalistic purposes” should be understood and in a close future the DPD will be replaced by the Proposed General Data Protection Regulation (GDPR). We should, therefore, examine whether the case-law and the Draft GPRD put an end to the current legal vacuum.

#### *The sensu lato interpretation given by the ECJ*

In the common sense, journalistic activities cover a wide range of tasks and, then, do not only refer to the profession of journalist in a strict sense. This broad interpretation seems also to be the approach that the European Court of Justice has adopted in the ruling of the *Satamedia Case* where the CJEU had to answer a question preliminarily referred by the Finnish Supreme Administrative Court regarding the interpretation of the “journalistic purposes” exemption provided by Article 9 of the Data Protection Directive. In this latter; the ECJ holds that the importance of freedom of expression in all democratic societies required broad interpretation of its related notions, including journalism<sup>18</sup>: the concept of journalistic activities “encompasses all activities whose object is the disclosure to the public of information, opinions or ideas, irrespective of who is carrying on such activities (not necessarily a media undertaking), of the medium which is used to transmit the processed data (a traditional medium such as paper or radio waves or an electronic medium such as the internet) and of the nature (profit-making or not) of those activities”<sup>19</sup>. By analogy, this entails that the exemption of Article 9 in the context of RPAS applies to any entity using a civil drone capturing personal data aiming to be disclosed to the public. So the derogation seems not only concern media organisations but also every person engaged in journalism including paparazzi, Youtubers, citizens-reporters as long as the purpose of the data processed was initially to disclose the information to the public. Although this *sensu lato* interpretation of the concept of “journalism” makes the DPD a living instrument evolving with its time, it will also allow to many entities and persons to put aside fundamental requirements of the DPD such as individuals’ rights.

#### *Scenario Journalist. Organisers of a concert event*

If we apply this ECJ case-law to our scenario, organisers of the concert (Youtubers) will be considered as journalists as the object of the drone use was to disclose the video to the public.

---

<sup>17</sup> “National law applicable - 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State”, European Parliament and the Council, 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 OJ L 281, 23.11.1995, (“Directive 95/46/EC”), Article 4.

<sup>18</sup> Flanagan, Anne, op. cit., 2012, pp. 1–30.

<sup>19</sup> ECtHR, *Tietosuoja- ja valtuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, application no. C-73/07, judgment of 16 December 2008.

Therefore, they fall under the exemption. Does it mean that any company using a drone for making a video that it makes public for promoting its services or activities should also fall under the notion of journalists? If a priori the “necessary” requirement will prevent that such “journalists” apply the exemption to their data collection, there is a risk to consider such companies as “media falling under the scope of the exemption”.

#### *The Proposed General Data Protection Regulation (GDPR)*

The Commission proposal under the basis of Article 81 restates the expression for “journalistic purposes”. However, the Recital 121 clarifies this expression *“In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly. Therefore, Member States should classify activities as “journalistic” for the purpose of the exemptions and derogations to be laid down under this Regulation if the object of these activities is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes”*.<sup>20</sup> In this new Recital, the Commission has incorporated the meaning given by the ECJ in *Satamedia case*. Therefore, although this clarification will put an end to the uncertainty of the current legal vacuum, the adoption of a broad meaning of “journalism”, as stated above, will allow a large number of RPAS operators to claim the exemption, at the expense of data subjects.

Regarding the amendments proposed by the Parliament to the Commission’s proposal, we observe a same *latu sensu* interpretation: *“In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom broadly to cover all activities which aim at the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them, also taking into account technological development. They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes*. However, in a difference with the Commission’s proposal, the Parliament has included that technological development should be taking into account.<sup>21</sup> We can, therefore, expect a margin of manoeuvre for Member States to adopt stricter rules when the technology used for the collection is too ubiquitous and intrusive into the privacy of individuals.

#### *Concluding remarks regarding to this broad notion of “journalism”*

Although we understand the decision making powers and the ECJ for having chosen a broad and modern interpretation of the notion of “journalism”, we think that certain technologies like RPAS in the hands of paparazzi will strongly increase privacy and data protection risks to individuals as they are not subject to such rules. Therefore, if moreover they are exempted from the application of the DPD, such “journalists” will be free to operate in ways which might increase these risks. In US, the risks related to the use of drones by paparazzi have also been highlighted and some States have even already adopted anti-paparazzi laws.<sup>22</sup> Therefore, we encourage Member States to adopt a stricter notion of “journalistic purposes” and then,

---

<sup>20</sup> European Parliament, The legislative resolution of 12 March 2014 on the General Data Protection Regulation, Recital 121.

<sup>21</sup> ECtHR, *Tietosuoja- ja valtuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, application no. C-73/07, judgment of 16 December 2008.

<sup>22</sup> Hawai, California.

narrow the exemption when personal information is processed through the means of intrusive technology like civil RPAS.

***Problem 3. State agencies - Lack of high-level standards applying to processing data for law enforcement purposes in a cross border context***

Earlier we have found that despite the high risks related to the use of RPAS by law enforcement authorities, the European data protection framework, more particularly the Framework-Decision 2008/977/JAI (hereafter, the DPFJ), does not cover the domestic data processing performed through the means of RPAS for law enforcement purposes by states agencies.<sup>23</sup> We will specifically see in the next Chapter the extent to which such absence of harmonisation at the European level may raise concerns when personal data are domestically processed.

On contrary, the DPFJ covers the processing operations by such RPAS operators taking place in a cross-border context. However, having been adopted in a security context and at a lower common denominator, this text does not provide an adequate protection to face with the risks that law enforcement drones applications may pose. Indeed, the ‘basic data protection principles’ have been greatly compromised in the text of the DPFJ. This has been done either by exempting clauses or by use of the broad notion of ‘further processing’.<sup>24</sup> Rights and safeguards are less protective than in the framework of the Data Protection Directive, despite the fact that the law enforcement sector is legally empowered with surveillance functions that pose higher risks. Therefore, even when intrusive technology like governmental drones are used by a national state agency to capture data aiming to be transmitted to another national law enforcement authority, there are no high-level data protection standards that apply. The study of two core principles gives us an example.

a) Purpose limitation

In the scenarios examined where state agencies use drones for law enforcement purposes, we have specifically highlighted that RPAS are likely to be launched for one purpose but in reality the personal data captured will be used for another criminal conviction. For example, an RPAS initially launched for monitoring an evening marathon could be finally used to capture thermal images proving the existence of a marijuana field in a residence close to the running.

Risks related to multiple usage of personal information are very common when personal data are processed, this is the reason why the ordinary data protection law encompass in its core principles the purposes limitation principle prohibiting such misuses. However, in police and criminal justice processing, the DPFJ applies and whereas this latter encompasses the purposes limitation requirement, it also provides three derogations:

*“Further processing for another purpose shall be permitted in so far as:*

*(a) it is not incompatible with the purposes for which the data were collected;*

---

<sup>23</sup> Council of the European Union, Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 27.11.2008, Article 1.

<sup>24</sup> de Hert and Papakonstantinou, op. cit., 2009.

*(b) the competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions; and*

*(c) processing is necessary and proportionate to that other purpose”<sup>25</sup>.*

Such derogation renders the principle of purpose limitation null as “personal data shall always be collected for police processing purposes and processing under the DPFJ shall thus never be ‘incompatible with the purposes for which the data were collected’”.

b) Information of the data subject (transparency principle)

Earlier we emphasised that the invisible feature of data collection operated by State RPAS technology will likely cause chilling effect and particularly transparency concerns as most of the time, RPAS operators will process data whether or not an individual is aware of the presence of the drone or without the individual being aware that data is being collected. Therefore, “the right of the data subject to be informed about which of his or her data is processed by whom is fundamental to the protection of personal data. Without this knowledge, the data subject is virtually unable to exercise any of his or her other rights”.<sup>26</sup>

However, a clear obligation to provide the data subject with information is not found in the Framework Decision. Recital 26 FDPJ mentions that “... *it may be necessary to inform data subjects regarding the processing of their data ...*”<sup>27</sup> and it further details that “Member States shall ensure that the data subject is informed regarding the collection or processing of personal data by their competent authorities, in accordance with national law”<sup>28</sup>. As the European Data Protection Supervisor notes, the wording of the provisions relating to notification of the data subject suggests it is a possibility rather than an obligation.<sup>29</sup> In consequence, in the framework of police and judicial processing, Member States themselves decide about the introduction of the notification duty. Therefore, under the current DPFJ, State agencies which have captured personal information through the means of drones are not all subject to notify individuals. Consequently, it is clear that this lack of transparency obligation and harmonisation does not provide an adequate framework to address the inherent transparency concerns posed by the RPAS technology. Furthermore, it is noteworthy that there are no accountability principle, no profiling restrictions, no clear preventive security measures and many exemptions to the obligation to ensure individuals’ rights; concerns which have been specifically highlighted in the context of drones applications.

All these considerations and examples have led to a conclusion that the current European data protection legal framework applying to the data processing carried out by police and criminal judicial authorities is not adequate to address the privacy and data protection issues raised by usages of drones. The lack of a subsidiary law applying to internal processing in the law enforcement sector and the low-level of data protection standards of the DPFJ has already

---

<sup>25</sup> Council of the European Union, Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 27.11.2008, Article 3.

<sup>26</sup> Paul de Hert, Vagelis Papakonstantinou, op. cit., 2009, pp. 403–414.

<sup>27</sup> Council of the European Union, Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 27.11.2008, Recital 26.

<sup>28</sup> Ibid., Article 16.

<sup>29</sup> EDPS, Opinion of the European Data Protection Supervisor on the Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, [2007] OJ C 139/1, 27.11.2008., para 37.

been subject to lively criticisms. With the deployment of RPAS technology able to perform all types of surveillance on an unprecedented scale and collect massive amount of data, we can expect more privacy abuses and an increase of risks previously studied. Therefore, there is a legal need to adopt high level data protection standards, adapted to the functions and the security nature of this sector which apply to intra-Member States processing as well as to processing in cross-border context. This vision seems to be also the one of the Commission which has recognised that the Decision Framework is in need of review and has already proposed in the reform context a draft of a Data Protection Directive dealing with police and judicial cooperation in criminal matter. Does this Draft Directive encompass better data protection standards? Will it be able to mitigate the risks posed by RPAS technology? These questions are deeply examined in the next section.

### **The new proposal for a Police and Criminal Data Protection Directive: Towards a better protection?**

In the framework of the reform, the Commission has proposed to replace the DPFDP by a Data Protection Directive. This latter has been welcomed by data protection specialists in many points. This section aims to examine if among these new provisions some of them could bring a better data protection to processing operations carried out by State drones than the current DPFDP.

Firstly, the most important change to mention is that the Proposed Directive would apply to all national authorities competent for the prevention detection and investigation of criminal offences or the execution of criminal penalties. This extension of scope to domestic processing will therefore close the gap produced by the Framework Decision 2008/977<sup>30</sup> and the “EU data protection law would be more effectively harmonised than ever before”<sup>31</sup>. However, such authorities are still excluded from the scope the data processing in national security matters (processing generally processed by domestic and foreign intelligence agencies) and by EU institutions, bodies, offices and agencies.<sup>32</sup> National security matters being a national competence, it falls outside the scope of EU law while data processing regarding EU institutions, bodies, offices and agencies is subject to Regulation 45/2001 and of sector-specific legislation.<sup>33</sup> Consequently, if the proposal is adopted, State agencies capturing personal data via RPAS will have to apply the proposed changes regardless if the processing takes place in a purely national or a cross-border context, except if it concerns national security matters, such as terrorism.

Secondly, the proposed Directive includes a new element that makes “reference to the transparency principle, to the data minimization principle and to the obligation to process only of non-personal data, as far as possible, as well as to the comprehensive responsibility and

---

<sup>30</sup> European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25.01.2012., Article 2.

<sup>31</sup> Boehm, Frederika and Paul De Hert, “Notification, an important safeguard against the improper use of surveillance - finally recognized in case law and EU law”, *European Journal of Law and Technology*, Vol. 3, No. 3, 2012.

<sup>32</sup> European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25.01.2012., Article 2 (3)(b).

<sup>33</sup> Explanatory Memorandum , PDPJP COM (2012) 10 final, p. 7, para 3.4.1.

liability of the controller, responding to the debate on a 'principle of accountability'".<sup>34</sup> Such clear recognition of the core data protection principles in the criminal area will necessarily reduce all data protection risks and data breaches inherent to such RPAS application. Furthermore, regarding to the transparency principle, we observe a significant turnaround. Article 11 of the proposed Directive introduces an obligation for the Member States to set up a duty to inform individuals concerned when personal data about them have been overtly or secretly collected.<sup>35</sup> It introduces a high-level standard similar to what we see with the Data Protection Directive.<sup>36</sup> Nevertheless, it is noteworthy that "to recognize the specifics in police and judicial related data processing", the proposed Directive provides several exemptions. It is clear that "a notification might impair the investigation in some way"<sup>37</sup>, therefore Article 11(4) provide some exemptions. These clauses are at a first glance, "relatively far reaching exemptions and Member States have the possibility to establish categories of data processing which may wholly or partly fall under the exemptions"<sup>38</sup>. However, Article 11(4) also mitigates these exceptions by requiring that any restriction on the duty to notify must be necessary and proportionate.

Given these considerations, it is clear that the planned revision explicitly foresees provisions providing for more protection of the processing activities carried in police and judicial work. Therefore, this will inevitably reduce the risks of processing related to State drones. Nevertheless, certain broad exemption clauses enshrined in the Draft will still leave considerable discretion to Member States. In particular, we think to the right to be informed is significant, which in context of drones processing is already weakened by the invisibility characteristic of RPAS technology and the non-identification of drones' operator. We would like to draw attention to the fact that in case of secret surveillance operations, the exemption should apply on case-by-case basis and individuals whose personal data have been processed shall be notified after the secret processing operation. In this respect, we should recall that if the data protection law provides broad exemption to the right to be informed, the right to privacy and its ECtHR case law require that individuals are notified after a surveillance measure has been undertaken.<sup>39</sup> Finally, since the ECJ has issued a decision in which it declares the Retention Directive invalid, we recommend to the European Union and Member States to adopt complemented procedural safeguards when police officers access to data that have not been processed or collected for criminal justice purposes such as the obligation to obtain a warrant.

---

<sup>34</sup> De Hert, Paul and Vagelis, Papakonstantinou, "The Police and Criminal Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, Vol. 22 Issue 6, 2012.

<sup>35</sup> Bäcker, Matthias and Gerrit Hornung, "Data processing by police and criminal justice authorities in Europe - The influence of the Commission's draft on the national police laws and laws of criminal procedure", *Computer Law & Security Review*, Vol. 28, 2012, p. 632.

<sup>36</sup> European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25.01.2012., Article 11 and Boehm, F, de Hert, P 'Notification, an important safeguard against the improper use of surveillance - finally recognized in case law and EU law', *European Journal of Law and Technology*, Vol. 3, No. 3, 2012.

<sup>37</sup> Bäcker and Hornung, op. cit., 2012, p. 632.

<sup>38</sup> Boehm, F, de Hert, P 'Notification, an important safeguard against the improper use of surveillance - finally recognized in case law and EU law', *European Journal of Law and Technology*, Vol. 3, No. 3, 2012.

<sup>39</sup> De Hert, Paul and Franziska, Boehm, "The rights for Notification after Surveillance is over: Ready for recognition?", *Digital Enlightenment Yearbook*, 2012.

## 9.4 Implementation and enforcement difficulties of the current Data Protection Directive 95/46/EC

We have above examined that the current remaining gaps should be mitigated with the adoption of the new data protection framework. However, the present section will show that the implementation of the Data Protection Directive by commercial operators is likely to face some difficulties. Certain difficulties come first, from the fact that the data protection law is technologically neutral, but this also makes it abstract and difficult to operationalise in practice. Second, certain additional difficulties result from the characteristics inherent to the RPAS technology.

### *Problem 1 - Difficulties for collectors to comply with several data protection concepts and principles*

In the previous chapters, we observe that the European data protection law subjects each data controller to several obligations and rights. Amongst these obligations, we find the main data protection principles, the individual rights and some additional obligations that the data collector and data processor have to fulfil jointly. So, the data controllers and processors that process personal data through the means of a civil RPAS must comply with obligations and rights during three distinct phases: before the processing, during the processing and after the processing.

Before the execution of the processing, the data collector has to determine the purpose of the processing. This must be legitimate and explicit. Furthermore, he or she must notify the data protection authority or data subjects that he or she is going to operate data processing activities for one or multiple specified purposes (purpose limitation and transparency principle).

During processing activities, the data collector has to process the data fairly and lawfully<sup>40</sup>, in accordance with the legitimate purposes previously determined and collect only adequate, relevant and not excessive data in relation to the purpose pursued (lawfulness principle, data quality principle, proportionality and data minimisation principles).

Once the processing has been executed, the data collector has to verify that the data are accurate and if necessary update the data.<sup>41</sup> He or she also has to take all the necessary measures to correct or delete the eventual data inaccurate or incomplete. In addition, he can only store the data under a form that allows data subjects to be identified for a specified period, which cannot be longer than is necessary for the purposes pursued. He or she must, moreover, ensure the confidentiality of the data and the security of the data by undertaking organisational (limit the number of person accessing the data, using passwords, etc.) and technical measures. Besides these obligations, the data collector must also ensure the individual rights of the data subject. In that respect, he or she must inform the data subject by giving him or her some information about the data processing (type of data collected,

---

<sup>40</sup> To process lawfully the data collector has to obtain the consent of the subject or must be necessary for the execution of a contract or to comply with a law or to protect the vital interest of the data subject or be necessary to carry out a mission of public interest or be necessary to carry out a legitimate interest.

<sup>41</sup> Fossoul, Virginie, "RFID et biométrie: Etat des lieux", in Docquier, B A. Puttemans (Eds.), *Actualités du droit de la vie privée*, Bruylant, Brussels, 2008, p. 149-150.

purposes, his/her identity, etc.) and provide him or her a right to access to the provenance of the data.<sup>42</sup>

After having recalled what type of obligations and rights and at which moment of the execution the responsible for processing data has to ensure them, we will see that some of them are difficult to be ensured or easy to be ignored by the RPAS collectors. However, before analysing such principles more deeply, we will examine that even certain basic concepts like personal data and data collector/processor are not so easy to understand in the context of RPAS.

*The concept of personal data: Are all information collected by drones personal data?*

The definition of personal data is central to the Data Protection law as it determines the activities that fall within its scope. Previously, we have seen that unlike other technologies, civil RPAS may be mounted with wide range of equipment designed for processing data: videos, images, sounds, IR and UV images, geolocation data (location and traffic data), communications, biometric data, etc.

However, in Chapter 6 we found that the majority of the respondents to our survey reported that they do not collect personal data and then do not raise any issues regarding the data protection. This is despite the fact that 55% stated that their systems do capture or may capture images of members of the public. Moreover, 97% of the respondents indicated data was recorded and 76% indicated that the data recorded is also stored. Nevertheless, although many RPAS stakeholders think that they do not collect personal data, the survey results demonstrate that in reality RPAS operators may frequently process personal data.

a) Current legal definition – Directive 95/46/EC

First of all, it must be recalled that the data protection directive defines the “personal data” as *“any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”*.<sup>43</sup> This broad definition is refined in recital 26: *“to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person”*.<sup>44</sup>

However, being vague and, then opened to different interpretation in Member States, the Court firstly and then, the Article 29 Working Party have expressed their views on this matter.

b) Jurisprudential definition – *Lindqvist Case C-101/01*

The European Court of Justice has given its first interpretation in the case law *Bodil Lindqvist*, where it had to consider if information about individuals placed on a website was personal data. The ECJ stated that *“referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or*

---

<sup>42</sup> Ibid.

<sup>43</sup> Directive 95/46/EC, Article 2.

<sup>44</sup> Directive 95/46/EC, Recital 26.

information regarding their working conditions and hobbies, constitutes the processing of personal data".<sup>45</sup>

This jurisprudential interpretation points out that “a relatively broad interpretation ought to be taken and clarifies that certain types of information, such as telephone numbers, should be categorised in this manner”.<sup>46</sup> However, the doctrine has even expanded the approach by given a broad interpretation to all criteria of the notion.

c) Doctrinal definition - Article 29 Working Party’s Opinion 4/2007<sup>47</sup>

The leading guidance on the approach to personal data is the Opinion 4/2007 issued by the Article 29 Working Party. In an objective of harmonisation, it gives some insights on how personal data should be interpreted, given the four criteria laid down in the legal definition: (i) any information (ii) relating (iii) to an identified or identifiable (iv) natural person. Therefore, collectors shall follow this guidance to determine which data captured by their civil RPAS must be qualified as “personal data”.

(i) *First criterion: “Any information”*

This first element must be interpreted in its widest sense. The nature of the personal data may cover objective as well as subjective information. The Article 29 Working Party explains that the concept of any information includes “any sort of statement about a person”, the information does not even need to be correct. In terms of content, it does not matter that the information concerns family life, professional life or social life of the person.<sup>48</sup> Regarding the format on which the data is stored, the Article 29 Working Party stated that “the concept of personal data includes information available in whatever form” such as numerical, alphabetical, graphical, or acoustic, kept on a paper, on a computer memory, or videotapes etc.<sup>49</sup>

(ii) *Second criterion: “relating” to someone*<sup>50</sup>

Information relates to an individual when the information is “about” that person and “relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated”.<sup>51</sup> The Article 29 Working Party has clarified that “for information to ‘relate’ to a person, a ‘content’ element, a ‘purpose’ element or a ‘result’ element should be present”.<sup>52</sup> The “content” element means that the information has to be about a particular person. The “purpose” element may also be sufficient to treat information as information relating to a person. If the data are used or are going to be used for the purpose of evaluating or

---

<sup>45</sup> ECJ, *Bodil Lindqvist*, judgement of the 6 November 2003, application no. Case C-101/01.

<sup>46</sup> Linklaters, “What is personal data?”, no date.  
<http://www.linklaters.com/Publications/Publication1403Newsletter/PublicationIssue20081001/Pages/PublicationIssueItem3513.aspx>

<sup>47</sup> Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20.06.2007.

<sup>48</sup> Fossoul, Virginie, op. cit., 2008, p.166

<sup>49</sup> Article 29 Data Protection Working Party, op. cit., 2007

<sup>50</sup> Ibid.

<sup>51</sup> Ibid.

<sup>52</sup> Kindt, Els J., *Privacy and Data Protection Issues of Biometric Applications. A comparative Legal Analysis, Law, Governance and Technology Series*, Volume 12, Dordrecht Heidelberg New York London, Springer, 2013 pp. 108-109.

influencing a person, such data relate to that person. A “result” element is present if the information is likely to have an impact on a person.<sup>53</sup>

Meeting this criterion may seem evident in some RPAS processing activities. For instance, when the information captured by the drone is a biometric data like a facial recognition image, the data relates by nature to someone and identifies necessarily an individual. The same criterion is also obviously met when the data consists of an image of a person filmed by a video-camera fitted on an RPAS.

However, in some other cases, the relationship between the person and the information is not so easy to establish. What happens when the information concerns an object, such as a vehicle? In several cases, this object may belong to someone, or may be subject to particular influence by or upon individuals or may maintain some sort of physical or geographical vicinity with individuals or with other objects. Therefore, this object may indirectly “relate to” someone. Is it the case with RPAS processing?

Example 1.

In the scenario presented in Chapters 7 and 8, an energy company using a commercial RPAS equipped with a GPS sensor and a thermal camera films the roofs of several residential areas. Thanks to the information collected from the GPS and the thermal camera, the energy provider matches the information to customers’ addresses and offers them discounted roof insulation. In addition, consider that he might also decide to sell these data to insurance companies determined to increase their insurance prices for badly isolated houses.

Example 2<sup>54</sup>.

A Society for the Prevention of Cruelty to Animals launches a new campaign aiming to spy on the treatment of farm animals in a bid to find evidence of abuse. For that purpose, they bought RPAS equipped of a GPS sensor and a surveillance camera and launched the drone filming the living conditions of the animals. While the geo-localisation data and images do not directly concern someone, they can have an impact on the farmers if these data are disclosed or used as evidences in front courts.

In these examples, although the information as such are not relate to a person, they can create consequences for persons and thus concern persons.<sup>55</sup> However, although it is clear that the pieces of information relate to an individual, to be “a personal data” the information must also serve another criterion, it has to relate to an identified or identifiable person.

---

<sup>53</sup> Article 29 Data Protection Working Party, op. cit., 2007 and Kindt, Els J., op. cit., 2013 pp. 108-109.

<sup>54</sup> Topnotizie.info, Drones contre la cruauté sur les fermes, <http://topnotizie.info/fr/2014/06/droni-contro-la-crudelta-negli-allevamenti/>; AU news, « Drone targets farm animal abuse », <https://au.news.yahoo.com/a/16486185/drone-targets-farm-animal-abuse/> and Smh, « I spy with my little fly-Animal cruelty », 31 March 2013. <http://www.smh.com.au/technology/sci-tech/i-spy-with-my-little-fly--animal-cruelty-20130331-2h02s.html>

<sup>55</sup> Fossoul, Virginie, op. cit., 2008, p.166 and Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20.06.2007

(iii) *Third criterion: “to an identified or identifiable (natural person)”*<sup>56</sup>

The third criterion “identified” or “identifiable” has been subject to different considerations by the Working Party.

Firstly, it clarified that a person is “identified” when she or he can be distinguish among a group of person while the person is “identifiable” when the individual has not been identified yet but it is “*possible to do it by all the reasonable means likely to be used by the collector or any other person*”.<sup>57</sup> However, the mere hypothetical possibility to identify the individual is not sufficient to consider the person “identifiable”. The Working Party has given in its Opinion different factors to assess this criterion “*all the reasonable means likely to be used*”. Firstly, it points out that “*where the purpose of the processing implies the identification of individuals, it can be assumed that the controller or any other person involved have or will have the means “likely reasonably to be used” to identify the data subject*”.<sup>58</sup>

Example 1.

This first insight is very relevant in RPAS technology as this implies that when the collector places on his/her drone a payload destined to identify persons such as a video surveillance camera, “the whole application as such has to be considered as processing data about identifiable persons, even if some persons recorded are not identifiable in practice”.<sup>59</sup>

As a second factor for assessing the “*reasonable means likely to be used*”, Art.29 WP states that we should consider “*the state of the art in technology at the time of the processing and the possibilities for development (also the possibilities of future technologies) during the period for which the data will be processed*”.<sup>60</sup> In other words, this means that if the identification is not possible today but will be possible in the future thanks to technological advances, these information must be consider as personal data. This interpretation given by the Working Party is particularly relevant in RPAS technology as it evolves every day and new emerging capabilities will come.

Secondly, the Article 29 Working Party also explained in its Opinion that the “identification” of the person must be understood in general terms as this individual may be “directly” or “indirectly” identified or identifiable. Usually, a person “directly” identified or identifiable implies that such person has been identified by his or her name. On contrary, a person is “indirectly” identified or identifiable when the identification of the person is allowed thanks to the combination of the data hold and other information.

Example 2.

A paparazzi focused on the Belgian Royalty decides to buy a Quadcopter RPAS equipped with a high-tech camera. Aware that the Prince and his family are on holiday in the South of France and pass their day to sunbathing on the beach, he flies his drone above the coast and takes footage of the people lying on the beach. Amongst the tourists we can easily identify the Prince accompanied of his wife and their three children. As their faces are famous and people

---

<sup>56</sup> Ibid.

<sup>57</sup> Article 29 Data Protection Working Party, op. cit., 2007.

<sup>58</sup> Article 29 Data Protection Working Party, op. cit., 2007 and Fossoul, Virginie, op. cit., 2008, p.166

<sup>59</sup> Article 29 Data Protection Working Party, op. cit., 2007.

<sup>60</sup> Ibid.

are able to associate them with their names, these footages allow identifying directly persons targeted, and are therefore personal data.

(iv) *Fourth criterion: “a natural person”*<sup>61</sup>

By using the terms “natural person”, it means that it only applies to the data related to physical person by opposition to those of legal persons (civil society, commercial society, not-profit association). It should also be noted that personal data concerns only data relating to identified and identifiable “living persons”.

d) Future legal definition – Draft General Data Protection Regulation

In the present draft, the wording remains the same: “*‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person*”<sup>62</sup>. However, particular reference is made to certain type of data (location data, IP addresses, RFID are “examples of identifiable individuals despite the lack of an apparent connection”).<sup>63</sup> Whereas such guidance intends to offer more protection to the data subjects, in reality, it only reminds us the extensive approach adopted by the Article 29 WP in its Opinion.<sup>64</sup>

e) The concept of personal data: an adequate concept?

After having analysed in detail the necessary criteria that RPAS collectors have to check to determine if the information processed is personal data, we can now draw certain conclusions regarding the appropriateness of the concept of personal data.

As first observation, we remark that the broadness of the concept has the benefit of making the data protection law applicable to a wide range of information processed by a multitude of technologies. However, in return, such broadness makes impossible to set up an exhaustive list of the information that could be collected by RPAS that are personal data. Furthermore, the analysis of criteria makes clear that it is more the circumstances surrounding the processing, than the kind of data, which determines whether a data is personal. Consequently, such a concept implies that RPAS collectors cannot always easily determine if the information collected is a personal data and requires that they attentively examine whether the data collected falls under the above-mentioned criteria. This may be result in a costly administrative burden.

Secondly, we remarked that whereas Art.29WP has issued some guidance, in practice several criteria may be subject to diverse interpretations. For instance, a RPAS collector which

---

<sup>61</sup> Article 29 Data Protection Working Party, op. cit., 2007.

<sup>62</sup> European Parliament, European Parliament Legislative Resolution on the 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)0011 – C7-0025/2012 – 2012/0011(COD)), Article 4§1.

<sup>63</sup> De Hert, Paul and Vagelis, Papakonstantinou, “The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals”, *Computer Law & Security Review*, Vol. 28, 2012, p. 134.

<sup>64</sup> Ibid.

discovers on his footages the fuzzy and distorted image of a person will a priori determine that it is not a personal data as the person is not “easily identifiable through the use of reasonable means” as he does not have access to a cutting-edge technology allowing him to make the image of the person identifiable. However, another collector, a specialist in web design, in the same situation may easily make the image identifiable through the use of a specialist software package. Another example would be the visual capture of the tops of people’s heads by an RPAS. Privacy scholars will promote “that the footage taken by a drone showing only the overhead of a person does not allow to identify the person through reasonable means. Therefore, it is not a personal data”. However, among those who collect information via RPAS, the notion of “reasonable means” itself will not have the same meaning.

A third observation regards the implementation of the data protection definition in Member States. Despite of the insights issued by the Art. 29WP, studies show that although most States’ definitions of personal data are consistent with the Directive and the Art. 29WP s’ Opinion, there are some variations in practices. For example, images and sounds are recognised by Belgium, Germany, France, Italy, Denmark and the United Kingdom as a personal data while Sweden makes for them another category.<sup>65</sup> In the context of RPAS applications, such variations of interpretation are particularly critical as RPAS data controllers are more likely to “operate in multiple jurisdictions and then are likely to take a cautious approach and adopt a wide interpretation (forum shopping)”.<sup>66</sup>

To sum up these considerations, we can say that if the legal definition of the “personal data” concept is defined through broad and vague criteria, the Opinion of the Article 29 Working Party gives a comprehensive guidance to data collectors. However, in practice, an RPAS operator will have to take in account different elements to determine whether a data is personal or not and this may be a costly administrative burden for the RPAS industry.

f) Are data processed inadvertently personal data?

Whether the data have been conscientiously, voluntarily or inadvertently processed, once they meet the four criteria discussed above, they are recognised as personal data and shall be collected, stored and used according to the data protection law.<sup>67</sup> In general, RPAS operators who inadvertently collect and process personal data do not need such information. Therefore, in conformity with the data minimization, proportionality and data retention principles, the personal data should be deleted or at least must be made anonymous. For RPAS operators using civil drones in activities that are likely to process personal data inadvertently, the data minimization should be read in combination with the security of processing principle and the Data Protection by Design approach. According to these, RPAS operators must adopt technologies and security measures that prevent the processing of personal data not necessary for the scope of the flight. We think particularly about mapping companies and real estate agencies which take footages of residential areas through the use of drones. These latter should opt for a blurred technology or taking pictures at a certain flying height to avoid the identification of person on their footages.

---

<sup>65</sup> Linklaters, op. cit., no date.

<sup>66</sup> Ibid.

<sup>67</sup> Article 29 Data Protection Working Party, op. cit, 2007.

g) Are data collected by RPAS sensitive data?

As previously explained, some data are more sensitive than others and for that reason they are prohibited to be processed, collected or stored, except under certain legal conditions. The data concerned and qualified as such are “data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and those concerning health or sex life”.<sup>68</sup> Additionally, judicial data “data relating to offences, criminal convictions or security measures”<sup>69</sup> are also qualified as sensitive data.

Although this concept of “sensitive personal data” is not really pragmatic and varies among the Member States<sup>70</sup>, some technologies are more likely to process sensitive data than others. It is particularly the case for biometric recognition systems. Imagine a law enforcement entity which launches a RPAS equipped with a facial recognition payload for monitoring and profiling criminals. Biometric technologies are closely linked to certain characteristics of an individual and some of them are able to scan all type of information from age to gender to “ethnicity” to “skin colour” to height and weight; in other words, discriminatory data. Therefore, biometric data are generally considered as sensitive personal data and then, may only be processed under the respect of strict conditions and the adoption of safeguards. Nonetheless, the Working Party reminds data processors that in the assessment of the sensitivity of data processed by a biometric system, the context of the processing should also be taken into account.<sup>71</sup>

Regarding “judicial data”, it is obvious that RPAS used for law enforcement purposes will use drones for collecting some evidence of offences, i.e., data that may qualify as “judicial data”. It is already the case as in the Netherlands some police officers have deployed drones for identifying and condemning thefts on railways. However, according to the Data Protection Directive, the rule is the prohibition of processing such type of data. Nevertheless, judicial data processing may exceptionally occur “under the control of official authority, or if suitable specific safeguards are provided under national law”.<sup>72</sup> Another issue related to judicial data collected by drones concerns their admissibility of such data in front a court. Could the footage of a man in a street and the metadata of the photography taken by a mapping company serve in front a court to claim his innocence in the murder of his wife? Are thermal images of a cannabis field taken by a law enforcement authority admissible in front a Criminal Court?

Although such question is particularly relevant in the context of civil RPAS as they are likely to process images from everywhere even inadvertently, this question falls under the national competence and will be further examined in the next chapter related to the analysis of the national regime of Member States.

*Data controller and data processor: How do these two legal roles map onto the role of the operator of the RPAS?*

---

<sup>68</sup> Directive 95/46/EC, Article 8 and Article 29 Data Protection Working Party, op. cit., 2007.

<sup>69</sup> Ibid.

<sup>70</sup> Linklaters, op. cit., no date.

<sup>71</sup> Article 29 Data Protection Working Party, Advice paper on special categories of data (“sensitive data”) Ref. Ares (2011)444105, 20.04.2011.

<sup>72</sup> Directive 95/46/EC, Article 8§5.

a) Current situation – Directive 95/46/EC

The determination of the “controller” is crucial in data protection matters as it defines “who shall be responsible for compliance with data protection rules, how data subjects can exercise their rights, which is the applicable national law and how effective Data Protection Authorities can operate”.<sup>73</sup> Article 2(d) of the Data Protection Directive characterises the data controller by three main elements: (a) the personal aspect (“the natural or legal person, public authority, agency or any other body”); (b) the possibility of pluralistic control (“which alone or jointly with others”); and (c) the essential elements to distinguish the controller from other actors (“determines the purposes and the means of the processing of personal data”).<sup>74</sup> In other words, the data controller exercises overall control over the ‘why’ and the ‘how’ of a data processing activities, he/she supports all obligations and responsibilities stemming from the Directive.

Besides the role of the controller, there exists also the role of the “processor”. In the current DPD, this latter has a role limited to the confidentiality and security of the processing.<sup>75</sup> For the processor, it is stated that “*the legal or natural person must be legally separated from the collector and processing personal data on his behalf*”.<sup>76</sup> So the existence of a processor depends “on a decision taken by the controller, who can decide either to process data within his organization, or to delegate all or part of the processing activities to an external organization, i.e. by a legally separate person acting on his behalf”.<sup>77</sup>

In 2010, the Article 29 Working Party has issued an Opinion 1/2010 on the concepts of “controller” and “processor”. Through this guidance it interprets each criterion stemming from the legal definition and makes clear the distinction between processor and controller. The controller is distinct from the processor by the fact that “he/she determines the purposes and the means of the processing” (third element). This capacity may find its origin in a legal source (e.g., an explicit legal competence) or in factual circumstances (e.g., contractual relations, a traditional and visible control from a party). However, in some situations, the processor himself/herself determines the finalities and means of the data processing. In these cases, the processor is also the controller and all obligations rely on the same “person”. On contrary, “in complex environments”, explains the Art. 29WP, “many scenarios can be foreseen involving controllers and processors, alone or jointly, with different degrees of autonomy and responsibility”.<sup>78</sup>

After having explained both theoretical concepts, we should see in practice how these roles fit with the civil drone applications. Who determine the finalities and means in a RPAS context? Is it the operator of drones or the client that requires the processing of data?

---

<sup>73</sup> Article 29 Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, 16.02.2010.

<sup>74</sup> Ibid.

<sup>75</sup> Directive 95/46/EC, Article 16 establishes “*Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law*”. Furthermore, and 17 (security of processing) states “*a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures*”.

<sup>76</sup> Directive 95/46/EC Article 2.

<sup>77</sup> Article 29 Working Party, op. cit., 2010.

<sup>78</sup> Article 29 Working Party, op. cit., 2010.

In the context of personal data captured by civil drones, different types of entities can be data controllers, for example corporate actors, professionals such as journalists, law enforcement authorities, etc. Regarding to the criteria exposed, it is clear that the drones' operator will not necessarily be the data controller as drone operators do not always decide the purposes and the means of the processing but acts on behalf of his company or client. As with the determination of a personal data, it will depend on the circumstances of the case.

**Example 1.**

The State owns old pipelines which need to be monitored. Public authorities decide to hire the services of an Energy company specialised in the monitoring of such materials. The Energy company rents specific drones mounted with thermal and high-tech cameras and hire a free-lance consultant owning a drone licence. This operator launches the drone and tests it by scanning the landscape and taking a few close-up images of the base of the tower. Satisfied that the images are of sufficient quality for later analysis and can be enhanced to provide close-up footage of cracks or damage, the operator begins his inspection. As the RPAS ascends into the air, the operator circles the mast, moving steadily upwards. The video footage is focused on the mast, but the landscape behind the mast is visible in the shot as he makes his way around the mast and higher into the air. Although the operator and the Energy company are not interested in the farms or vehicles in the background, these images are captured and included in the footage provided to the public authorities and saved in the RPAS operator's and Energy company archives. In the case that such footages will allow to identify someone and so give birth to personal data, the collector of data shall be determined in order to trigger the application of the data protection law. In that case, we can wonder if the data controller is the drone operator (the free-lance consultant), the Energy company or the public authority?

It is noteworthy that in the Telecom sector where civil drones will be used as proxy-satellites for offering Internet and Communications services, another legal guidance needs to be mentioned. In this sector, the Recital 47 of the Data Protection Directive 95/46 has clarified the role of collector: *"where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; (...) nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service"*.<sup>79</sup> This statement makes clear that in principle, the Telecom provider of telecommunications services which uses civil RPAS for transmitting communications should be considered data controller only for traffic and location data related to the communications while the subscriber will be responsible for personal data transmitted in the communication itself.

From these considerations, two main elements must be pointed out. First, the definitions of "data controller" and "data processor" can be difficult to translate in the context of data processing by drones. The deployment of the RPAS technology leads to create new jobs in the public and private sector, new roles and responsibilities and it is not always clear from a scenario to another "who determines the purposes and the means of the processing". Sometimes we can even remark shifts of responsibilities. The Article 29 Working Party seems sharing the same vision when it states "The Working Party recognizes the difficulties in

---

<sup>79</sup> Directive 95/46/EC, Recital 47.

applying the definitions of the Directive in a complex environment, where many scenarios can be foreseen involving controllers and processors, alone or jointly, with different degrees of autonomy and responsibility<sup>80</sup>. However, it is very important to ensure that the responsibility for data processing is clearly defined and can be applied effectively. Therefore, **when various entities are involved we stress the importance “to establish the degree of independence of each party and their roles and responsibilities at an early stage**, particularly before the processing commences. This will help to ensure that there are no gaps in organisations’ responsibilities, such gaps could result in subject access request going unanswered, for example<sup>81</sup>. We also recall **the role of the DPAs to help the organizations using drones in their activities to determine the data controller and data processor roles by enacting guidelines for instance**.

Second, it is clear that the DPD assigns all responsibilities on the controllers as they exercise control over the processing and carry data protection liability for it while processors co-jointly with the collector have only few obligations. Having no responsibility, no action can be taken under the DPD against a data processor itself (no liability)<sup>82</sup>; even in case of data breach, only the collector has to shoulder the responsibility. Therefore, even the Data Protection Authorities “cannot even take action directly against a processor who is entirely responsible for a data breach, for example by failing to deliver the security standards the controller has required it to put into place”.<sup>83</sup> In the context of RPAS, this may pose certain issues as generally when there is a data processor, he/she is the RPAS operator (the pilot) that owns the full control of the drone. It means that the operator-processor that uses a drone is under the responsibility of the controller which may be at another place at the moment of the processing. This may lead to certain risks principally when a drone equipped with a camera transmitting without recording the images on a screen online hold by the processor. In this case the processor will be able to use the drone to spy individuals without any possible a posteriori control by the controller.

- b) Will the future data protection regime bring any changes to the current framework? –  
The Draft General Data Protection Regulation

In its Regulation the European legislator did not touch to the “*data controller*” and “*data processor*” definitions enshrined in the Directive. Therefore, it seems that we will experience the same abovementioned concern about their distinction in the future. Furthermore, we found the same obligation for controllers and processors to specify the obligations of each other in a written contract. However, the draft Regulation goes beyond the Directive as it stipulates what the terms of any contract between the controller and processor must be. Moreover, it has explicitly included the notion of *joint controllers*: “if a processor processes data other than as instructed by the controller, the processor will be considered a joint controller of those data”.<sup>84</sup>

---

<sup>80</sup> Article 29 Working Party, op. cit., 2010.

<sup>81</sup> ICO, “Data controllers and data processors: what the difference is and what the governance implications are”, 2014,  
[http://ico.org.uk/for\\_organisations/data\\_protection/the\\_guide/~/\\_media/documents/library/Data\\_Protection/Detailed\\_specialist\\_guides/data-controllers-and-data-processors-dp-guidance.pdf](http://ico.org.uk/for_organisations/data_protection/the_guide/~/_media/documents/library/Data_Protection/Detailed_specialist_guides/data-controllers-and-data-processors-dp-guidance.pdf)

<sup>82</sup> Ibid.

<sup>83</sup> ICO, op. cit., 2014 and Article 29 Working Party, op. cit., 2010.

<sup>84</sup> European Parliament, Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of

In terms of responsibility and liability, the changes are more significant. The Draft places on the data processors additional obligations and responsibilities. Among new obligations, we observed: “maintain documentation relating to their processing operations in compliance with the detailed requirements of Article 28(2); to co-operate with the supervisory authority as required by Article 29; to implement appropriate technical and organisational measures as required by Article 30; to designate a Data Protection Officer if one of the conditions described in Article 35 is met; to inform the controller immediately after the establishment of a personal data breach.”<sup>85</sup> Consequently, the liability regime has also been adapted. Processors are, henceforth, liable for damages. Being those who act on behalf of controllers and highly involved in the processing, such regime seems more than justified.<sup>86</sup> Furthermore, the Draft prescribes that “*Where more than one controller or processor is involved in the processing, each of those controllers or processors shall be jointly and severally liable for the entire amount of the damage, unless they have an appropriate written agreement determining the responsibilities*”.<sup>87</sup> This co-responsibility in case of violation of the data protection law will allow to put an end to issues occurring in scenarios where multiple actors are involved and will “remove from the shoulders of data subject the burden to prove whose fault it is”.<sup>88</sup>

In the context of RPAS where in many cases multiple actors are involved in the processing and where operators-processors hold the full control of the tool, such substantial changes brought by the Draft GDPR will simplify the business relationships and improve the protection of individuals.

*The core data protection principles: does the RPAS collector respect them?*

a) Consent and other grounds: lawfulness principle

As examined earlier, for processing data the data collector must have a lawful ground. Consent of the data subject is the first ground of lawfulness presented by Article 7 of the Directive. Although “the order in which the legal grounds are cited under Article 7 is relevant” states Article 29WP, “consent is not always the most appropriate ground to legitimize the processing of personal data”. Article 7 provides also that processing activities may be based on a legal basis, a contractual basis or even for balancing interests. Unlike consent, these five other grounds must pass the “necessity test” which “strictly limits the context in which they can apply”.<sup>89</sup>

In the context of RPAS technology, this principle means that RPAS operators must either have the consent of the data subject concerned or have another lawful ground for launching its drone and capture personal data. The respect of this principle may be seen as a costly administrative burden for private companies which through the means of drones process data

---

personal data and on the free movement of such data (General Data Protection Regulation)(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Article 26 (4).

<sup>85</sup> Ibid. and Burnett, Emma, Julia, Graham and Cameron, McKenna, “The draft Data Protection Regulation— a new era for data processors?”, *Privacy & Data Protection Journals*, Vol. 12, Issue 5.

<sup>86</sup> Costa, Luiz and Yves, Poulet, “Privacy and the regulation of 2012”, *Computer Law & Security Review*, Vol. 28, 2012, p. 259.

<sup>87</sup> European Parliament, Draft European Parliament Legislative Resolution on the 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)0011 – C7-0025/2012 – 2012/0011(COD)), Article 77.

<sup>88</sup> Costa, Luiz and Yves, Poulet, op. cit., 2012, p. 259.

<sup>89</sup> Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 13.07.2011.

for marketing or profiling purposes. In general, these companies seek to process data information about groups of people, which define trends, as it ultimately helps companies market products more accurately and allow them to gain big benefits. Therefore, most of the time they collect personal data to build profiles with a view to creating contractual obligations with customers (not at their request). For example, we have recently seen mayors which post a video filmed by a drone of his city and events for promoting tourism. However, such video does not respect the lawfulness principle even if the citizens have been kept informed that drones are filming due to a lack of legal ground. Same issues will be particularly encountered in events like concert and festivals, the simple fact to notify people that they are filmed is not sufficient as it does not constitute a legal ground unless conditions were stipulated in the purchase agreement of the concert ticket.

b) Purpose limitation principle

As a reminder, the purpose limitation principle figures at the Article 6(1)(b) of Directive 95/46/EC and stipulates “*that personal data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'*”. Last year, the Article 29 Working Party published an Opinion on the ‘purpose limitation’ principle in which it analyses each component of the principle and gives some concrete example of its good implementation.<sup>90</sup> In this, it explains that this principle is composed of two obligations. On one hand, RPAS controllers must only collect data for specified, explicit and legitimate purposes and on the other hand, once data are collected, they must not be further processed in a way incompatible with those purposes. In other words, the collector must undertake a compatibility assessment where personal data are collected for one purpose and a data controller wishes to utilise those data for another purpose.<sup>91</sup>

The purpose limitation is a cornerstone of data protection as it prohibits “mission creep”, which could otherwise “give rise to the usage of the available personal data beyond the purposes for which they were initially collected”.<sup>92</sup> However, in the context of civil drones, the purpose limitation principle risks to pose some concerns of implementation. To ensure the respect of this principle, RPAS collectors must determine, prior to collection, the specific purpose of their collection and cannot re-sell data which will be used for another purpose. However, in a society where data worth money for private as well as public entities, some collectors will prefer to ignore the principle than respect it.

Example 1. (Private entity)

A home insulation company uses a commercial RPAS equipped with a GPS and a thermal camera to film the roofs of several residential areas. Thanks to the information collected from the GPS and the thermal camera, the operator has set up a marketing strategy allowing him to focus on houses with sub-standard roof insulation. An insurance company willing to tighten the home insurance conditions of its client proposes to the insulation company to buy its personal data collected.

---

<sup>90</sup> Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 02.04.2013.

<sup>91</sup> Treacy, Bridget and Bapat, Anita, “Purpose limitation— clarity at last?”, *Privacy and Data Protection Journals*, Vol. 13, Issue 6.

<sup>92</sup> Article 29 Data Protection Working Party, op. cit., 2013.

Example 2. (Public authority)

A real estate uses a drone for taking footages of residential areas for promoting luxury houses among clients. A municipality seeking to impose higher taxes on owners holding swimming pool ask to buy the data.

Example 4. (Journalists)

A journalist launches a drone to film an outdoor concert and during the event he notices a pickpocket that is stealing from people in the crowd. The journalist cannot then sell these footages to the police.

Example 3. (State agencies)

A State drone passes above residential areas for monitoring a marathon which discovers marijuana fields. In principle, according to the purposes limitation principles, law enforcement authorities cannot use the footages to launch a home raid.

These examples make clear that in many drone applications it is easier for drones' operators not to comply with the purpose limitation principle than respect it. This is particularly true when personal data are processed by drones as once in the air they often capture more data than those necessary for the specified purpose. Furthermore, being often undetectable or at least difficult to identify the operator and thus the collector, there is less deterrent effect for drones' operator to obey the rule.

c) Necessity, proportionality and data minimization principles

The legitimate purpose and purpose limitation principles taught us that not all finality are acceptable and that data can only be processed for a determined purpose(s) and re-used for purposes compatible with the initial ones. However, even when faced with a specified and legitimate purpose, not all data can be collected. Data collected by a drone must also be "adequate, relevant and not excessive in relation to the purposes pursue", this implies "a strict assessment of the necessity and proportionality of the processed data and if the intended purpose could be achieved in a less intrusive way"<sup>93</sup>, says Art.29WP. Actually, this statement refers to three other fundamental data protection principles: the necessity, the proportionality and the data minimization principles.

To assess the proportionality and data minimization principles of a RPAS technology, four requirements must be checked. A *prior requirement* is whether the RPAS technology is necessary to carry out the purpose identified.<sup>94</sup> A *second factor* to take into consideration is whether the RPAS use is likely to be effective in meeting that need by having regard to the specific characteristics of the RPAS technology planned to be used.<sup>95</sup> A *third aspect* to weigh is whether the resulting loss of privacy is proportional to any anticipated benefit (balance

---

<sup>93</sup> Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, 27.04.2012.

<sup>94</sup> Ibid.

<sup>95</sup> "Necessity" has not been interpreted by the courts as meaning strictly necessary in the sense that there was possible alternative. The Court of Justice of the European Union has held that "necessity" extends beyond necessity for the application of the legislation and includes choosing an option which allows the relevant legislation to be more effectively applied. It may not be possible to change the wording of the 1998 Act itself, but it is worth considering how to make clear to data protection practitioners that "necessity" in this context does not carry its ordinary and natural meaning. Its meaning is autonomous and may not be the same as that in other contexts, such as "necessary in a democratic society" under the European Convention on Human Rights.

between the interest of the data collector and the data subject concerned).<sup>96</sup> If the benefit is relatively minor, such as an increase in convenience or a slight cost saving, then the loss of privacy is not appropriate. *The fourth aspect* in assessing the adequacy of a RPAS is to consider whether a less privacy intrusive means could achieve the desired end.<sup>97</sup> According to these conditions, these both principles are, therefore, directly related and dependent on the finality for which the data controller executes the processing.

Example. Necessity, proportionality, data minimization

Pursuant the proportionality principle, drones equipped with different data processor systems (camera, GPS, altimeter) shall only collect information necessary and proportionate to the realisation of the purposes pursued. In this regard, a camera mounted on a drone aiming to take aerial photographs should not process personal data as the processing of personal data for such purpose is not necessary. In case some personal data could be inadvertently taken, this loss of privacy shall be weighed and be proportional to the benefit of the data collector. In that respect, if faces and other personal data have been shot because the collector of data did not add a blur technology on his camera (devoted to blur certain types of images, e.g., individuals) for economical purpose, the collection of data could be qualify disproportionate and so, as being in non-compliance with the European data protection law. Pursuant the minimization principle, RPAS technology shall not be used for data processing activities whether the purpose of this collection can be carry out through the use of a less-intrusive technology. RPAS technology being able to be equipped with different type of sensor, this principle also implies for such technology that a payload less-intrusive shall be preferred to a more intrusive sensor. Therefore, in the example of a drone launched for taking aerial photographs, if any other less-intrusive technology is able to collect such kind of data, the drone shall be equipped with the less intrusive sensor, for example a optical camera specific to aerial footages shall be used and not a camera with an extra optical zoom susceptible to spot faces.

Regarding to the proportionality principle, it is evident that in some circumstances RPAS technology will even not pass the prior-requirement, the “necessity test”. In some applications, using a drone for processing personal is more a question of fun than necessity. Such issue is particularly well demonstrated in the *scenario on new services* where an energy company decides to use a drone equipped with a thermal camera for collecting houses insulation images combined with names of individual customer’s addresses (= personal data) for offering roof insulation discount. Furthermore, collectors will be tempted to purchase the most efficient and cheapest drones and sensors which are not necessarily the least privacy intrusive and ubiquitous.

Example 1. Necessity and proportionality

A shop of luxurious products is always at the cutting-edge of the technology for its customers. The marketing director decides to buy drones equipped with a RFID system and a facial recognition system in order to propose the best services to his customer and increase the sales. These drones recognise the customers directly thanks to the facial recognition system and suggest them products according to the profile of the customer. For running such a system, footage of each customer is taken at its first entry in the shop and store in the facial biometric

---

<sup>96</sup> Article 29 Data Protection Working Party, op. cit., 2012.

<sup>97</sup> Ibid.

system. Moreover, mounted with a RFID system they are also able to give information on a specific product at the request of the customer and create the profile of the customer. Besides the fact that the data subject is maybe not aware of such use of his/her biometric data, the RPAS technology mixed with biometric and RFID systems seem to be disproportionate in relation to the need to increase sales and providing funny, high tech and good “salesman” to their customers. Collecting biometric data is also unnecessary, too intrusive and exposes data subjects concerned to too high risks for the purpose pursued.

Concerning the data minimization principle, specific difficulties may also arise as RPAS technology has a large breadth of view and is able to be mounted with several sensors. Therefore, they can monitor on a large scale and collect massive amount of data. So it is tempting and even sometimes less costly for data collectors to grab all information available provided than only the required specific data.

#### Example 2. Minimization

The organiser of a festival bought a drone equipped with an optical camera for taking footages of musicians and concert stages during the event for advertising the next festival. The drone is launched and starts filming and taking footages of the concerts. Amongst the footages taken some of them show men and women enjoying the music. Personal data have therefore been processed, collected and stored while the purpose was only shooting musicians during the show. The data minimization principle is then not respected as not only it processing personal data was not necessary but also the organiser would have avoid such intrusion in the privacy of the public members if he would have hired a photographer.

#### d) Transparency principle

By way of reminder, the transparency principle encompasses two main obligations stipulated by the directive on controllers: the obligations to inform the data subject<sup>98</sup> and to notify the data protection authority<sup>99</sup> prior carrying out the data processing operations. As already mentioned, being silent, in high altitude and small, drones may be invisible while RPAS operators, being remote pilots, they are not-identifiable. Therefore, it is very easy for collectors to undertake processing activities without informing and registering their activities. The risk that drones operators benefit from these invisibility and non-identifiable characteristics is certainly the most serious concern surrounding drones as once operators decide to process covertly, they can put aside the whole application of the data protection law at the expense of individuals. Moreover, when we know that individuals “could make €700, or £560, per year if they were paid ... for their personal data”<sup>100</sup>, we also understand that personal information is worth big money for business. So it is clear that unscrupulous money-

---

<sup>98</sup> **Directive 95/46/EC**, Article 10.

<sup>99</sup> **Directive 95/46/EC**, Article 18.

<sup>100</sup> Google and the University of Trento in Italy performed a study on participants in a lab as well as real world users. Luke Edwards (Pocket lint), “Guess how much money your personal data is worth? A study has finally found out”, <http://www.pocket-lint.com/news/129811-guess-how-much-money-your-personal-data-is-worth-a-study-has-finally-found-out>

grabbers which see data protection law as a costly administrative and economic burden will not hesitate to operate illegal covert processing data.<sup>101</sup>

Furthermore, the Belgian DPA explains that “Even if the processing proceeded by a drone is notified to the Commission, that does not make the identification of the collector easy as the database of the Commission does not allow to make a research by addresses. Nevertheless, the identification of the collector has all its importance as the individual concerned can only exercise its right to access, opposition, rectification and deletion from the collector”<sup>102</sup>. Finally, if the notification is not respected and the finalities are not identified by the person concerned, the risks to divert the data collected from its primary finality are multiplied.

#### Example. Transparency

A local council decides to encourage tourism by capturing photos of “the village life”, via a RPAS. The RPAS zipped through the streets, capturing images of people shopping, sunbathing and relaxing in the local gardens. Residents are not informed of the filming, although some see the RPAS and its operator and assumed it was a toy, while others were concerned by the intrusion in their private life but nothing allowed the drone operator to be identifiable. Some residents were complaining to the DPA but it was not able to identify the collector of data.

### *Problem 2. Difficulties for data subjects to exercise their rights*

Besides the obligations on controllers, we also examined that the DPD provide a multitude of rights to individuals: the right to be informed, the right to access (including the right to obtain from the controller the information about the type of data collected, the origins of the data and the purpose of such collection), the right to rectification, the right to erasure, the right to object, the right not to be subject to an automated individual decision.<sup>103</sup> The Directive also provides judicial remedies as well as the right to receive compensation for damage suffered. As explained under the transparency principle, individuals are often neither aware nor in control of what happens to their personal data and therefore fail to exercise their rights effectively. How exercise your right to access if you even do not know that your personal data have been processed or if you cannot even determine who the collector is?

#### *Scenario. New services*

As a reminder, we have seen in this scenario that a roof insulation company collected personal information through the means of drones for direct marketing purposes. It was emphasised that most of the residents were not aware of such collection because of the character undetectable of the drones (small drone flying above roofs). Furthermore, for those which had seen the drone passing above their houses, they were unable to identify the operator, this latter being remote kilometers away from the residential area. Consequently, individuals who did not receive any discount offer as their roofs are well insulated will never be able to exercise their rights to access, correction and erasure.

---

<sup>101</sup> Commission Vie Privée, « FAQ sur les drones », <http://www.privacycommission.be/fr/faq-themas/drones>

<sup>102</sup> Ibid.

<sup>103</sup> Ibid.

### ***Problem 3. Difficulties for DPA to enforce the data protection law***

This enforcement concern naturally stems from the implementation difficulties mentioned above. Specifically, how can Data Protection Authorities control and enforce the data protection rules if they are even not aware that personal data have been captured? Enforcement depends on the will of the data collector to notify the DPA or individuals on the ground of these processing activities. Furthermore, given their privacy intrusive nature, it is clear that processing activities operated through the means of drones should be considered through prior checking. However, once again if they are not notified, DPAs cannot evaluate the future processing activities. Additionally, although the prior checking would be a relevant mechanism to reduce the data protection issues related to drones, the determination of the processing activities subject to such prior-checking is left to the Member States. As we will see in the next chapter, this absence of European harmonisation is, in itself, already an implementation concern in the Member States.

### **Solutions. How to mitigate these implementation concerns? Will the future data protection framework bring some solutions?**

We will have the opportunity to deeply examine what are the solutions to improve the compliance of the data protection law and the respect of the individuals' rights in the, devoted to the study of soft law measures. Nevertheless, we can already say that the Draft of the General Data Protection Regulation introduces new principles, new monitoring mechanisms and new rights which will certainly ensure a better protection of the data subject rights when data are processed through the means of drones. Here are the following principles, tools and data subject rights incorporated in the GDPR that we will further study Chapter 12.

- Accountability principle
- The data minimization principle
- The Data Protection Impact Assessment
- The Data Protection by Design and Data Protection by Default approaches
- The Code of Conducts
- The right to be forgotten
- The right to object to data processing for profiling activities

## **9.5 Concluding observations**

The present chapter set out to determine whether the European privacy and data protection framework is adequate to address the risks posed by civil drones' applications, particularly commercial ones. Firstly, we have seen that commercial operators using RPAS for processing personal information in the course of their business are well covered by the current European data protection framework even if certain legal gaps remain within the European data protection Directive 95/46/EC. As legal gaps, we have studied the lack of preventive and remedial security measures. However, such gaps would be addressed by the adoption of the Parliamentary proposal for a General Data Protection Regulation. Indeed, this document includes elements like the data minimisation principle, Privacy Impact Assessment, Data Protection by Design and an obligation to notify DPA and data subject after a data breach. If these are implemented, it should result in a reduction of security processing issues in the context of data processing through the means of civil drones. Nevertheless, it is noteworthy that the current European privacy regime does not address the privacy and ethical risks posed

by RPAS applications when they are used in public places. A chilling effect, discrimination targeting, mission creep are remaining risks in commercial activities as well as in any other drones' applications.

Finally, implementation concerns have been analysed in the context of this study. Commercial collectors observe certain difficulties to comply with the requirements of the Directive when they collect data through the means of drones. Consequently we remarked also several issues about the exercise of rights by the individuals whose data have been processed and enforcement gap for the DPAs. Nevertheless, we will see in the next chapters that such implementation and enforcement concerns might be easily mitigated with the adoption of the new GDPR provisions and several complementary measures based on the soft-law.

## **10 THE ADEQUACY OF CURRENT MEMBER STATE REGULATORY FRAMEWORKS**

### **10.1 Introduction and overview**

In the first part of the project we focused on presenting a comprehensive analysis of privacy and data protection risks arising from the current and emerging use of RPAS (Chapters 7 and 8) and a legal analysis of the current Member States legal frameworks applicable to these RPAS uses (Chapter 5). In this legal analysis, we examined national privacy laws (including the right to privacy, the data protection law and laws governing the telecommunication and network services sectors) and surveillance regulations (including CCTV systems regulations and surveillance regulations governing the law enforcement sector) of seven Member States. On one hand, we examined six Member States having already implemented safety regulations for RPAS uses and on the other hand, we focused on one Member States currently preparing or drafting proposals for RPAS-specific regulations.

We shall now turn to the question of whether the current national legal frameworks examined afford an adequate protection to address the potential privacy risks arising from the use of RPAS in civil contexts. In this regard, this chapter is devoted to examining if current and emerging RPAS applications are all adequately covered by the national privacy and surveillance regimes in each Member States. Therefore, we will assess the shortcomings in current national privacy and surveillance regimes like we have analysed in the previous chapter with European law. Additionally, we will also discuss whether certain national regulatory mechanisms are working well and the elements of good practice that Member States have adopted.

As all Member States have implemented the Data Protection Directive 95/46/EC in their national regimes, national data protection laws entail the same implementation problems than the Directive itself. Having been examined in the previous chapter and to avoid duplication, we will only focus here on the specific legal gaps that national regimes carry. As in Chapter 5, we will firstly examine the adequacy of the national regimes of Members States already using civil RPAS: UK, Germany, France, Italy, Sweden and Denmark. Secondly, we will scrutinize the national regime of a Member State currently preparing RPAS regulations, Belgium.

### **10.2 Member States already using civil RPAS**

#### *10.2.1 The United Kingdom*

*Current and emerging RPAS applications not adequately covered by existing and proposed national legislation*

#### ***Problem 1. Commercial operators and public authorities - No prior-checking by the UK DPA: a lack of preventive security measure***

We have seen in our study of the Data Protection Directive 95/46/EC (hereafter, the DPD) that Article 20 of the Directive requires, on one hand, for the Member States to determine the processing operations likely to present specific risks to the rights and freedoms of data

subjects and, on the other hand, for the Data Protection Authority to check that these processing operations are examined prior to the start thereof.<sup>1</sup> Following this prior checking, the Data Protection Authority may, according to its national law, give an opinion, an authorisation or require the data collectors to adopt several safeguards mitigating the risks related to the processing. Regarding to the type of processing which should fall under the application of prior checking, the EDPS has explicitly stated that “*in some cases, biometric processing and telecommunication surveillance may present specific risk and then, must be subject to a prior-checking*”.<sup>2</sup> As we proved that drones are able to process sensitive data like biometric data and to monitor telecommunications, certain processing activities performed by the use of drones should definitely fall under the auspices of the prior-checking.

Furthermore, we argues in Chapter 3 that processing of personal data through the means of drones pose a multitude of risks due to its ubiquitous, aerial, invisible features and its ability to be equipped with a wide range of payloads, including biometric recognition, behavior detection, etc. Consequently, we concluded in the first part of this deliverable that prior-checking is a relevant preventive security measure in the context of civil drones. Whereas a priori certain processing activities through the means of drones should fall under such prior-checking like when they process biometric data, we even recommended Member States to adopt such pro-active monitoring mechanism for any data processed through the means of this sophisticated technology.

However, the UK Data Protection Act did not implement Article 20 of the Directive.<sup>3</sup> Therefore, the UK DPA (ICO) does not exercise prior-checking on activities processing personal data including those processed by civil drones. Such lack of prior control by the UK Data Protection Authority (ICO) increases risks surrounding the processing, the non-compliance with the DPD principles and risks of data breaches.

#### *Example*

In UK, a company which desires to process biometric data through the means of RPAS for commercial purposes will have to respect the requirements related to such type of personal data (sensitive data) and notify the UK DPA. However, the ICO will not assess the dangers of such a processing activity before processing such sensitive data.

### ***Problem 2. Commercial operators and State agencies - Drones used for surveillance operations: fragmentation of surveillance laws and lack of high quality standards***

Britain’s legislation relating to surveillance is patchy, and in some areas there is no protection against infringements committed by public authorities as well as by private organisations.

---

<sup>1</sup> European Parliament and the Council, 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 OJ L 281, 23.11.1995, (“Directive 95/46/EC”), Article 20.

<sup>2</sup> EDPS, Opinion of the European Data Protection Supervisor on a research project funded by the European Union under the Seventh Framework Programme (FP7) for Research and Technology Development - Turbine (TrUsted Revocable Biometric IdeNtitiEs), 01.02.2011.

<sup>3</sup> United Kingdom Parliament, Data Protection Act 1998, 16.07.1998 (“UK DPA 1998”).

The *Surveillance Road Map*<sup>4</sup> established that surveillance legislation is composed of eight different laws and regulations. In Chapter 5 we have already seen that four main regulations may apply to the surveillance performed by RPAS. As a reminder, we have seen that there are three texts applying when drones' operators performed visual surveillance *overtly* in public places, namely the Surveillance Camera Code of Practice<sup>5</sup>, the Data Protection Act<sup>6</sup> and the CCTV Code of Practice<sup>7</sup>. Regarding to the *covert* surveillance carried out by state drones, we found that law enforcement authorities have to respect the RIPA 2000 regardless the type of surveillance (visual and non-visual surveillance) performed.

This fragmentation has led to many overlaps between the different regulations and also to the creation of an un-coordinated approach between different competent authorities. In other words, three different authorities may a priori be competent to verify that drones' operators have complied with the laws mentioned: the Surveillance Camera Code of Practice falls under the auspices of the Surveillance Camera Commissioner (SCC), the Data Protection Act and the CCTV Code of Practice fall under the Information Commissioner's Office and the RIPA falls under the auspices of three different offices: the Office of the Surveillance Commissioners (OSC), Intelligence Services Commissioner (ISC) and the Investigatory Powers Tribunal (IPT).<sup>8</sup>

Besides the multitude of texts and offices existing, it is noteworthy that the new CCTV Commissioner does not have substantive powers, and there is no provision for complaints in case of breach of the Surveillance Camera Code of Practice. So only the ICO has the competence in case of *overt surveillance* to investigate individuals' complaints if drones' operators have breached the DPA. This means that in UK, individuals do not have complaint mechanisms when a drones' operator (a public or a private entity) breach his/her privacy in a public place by mere monitoring. Furthermore, "the ICO cannot award compensation. Individuals have further recourse to claim compensation in the courts if they have suffered damage and/or distress as a result of a contravention of the DPA".<sup>9</sup>

#### *Areas where current regulatory mechanisms are working well and elements of good practice*

In UK, the ICO has issued a multitude of Codes of Practice and other type of guidance (guidelines, handbooks). These allow the specification of data protection principles and requirements for a specific sector, making, therefore, the DPA more understandable for data collectors. Furthermore, some of them go beyond the DPA and the European DPD by recommending that data collectors adopt certain preventive security measures. For drones being used by different types of operators, for different applications and mounted with different technologic payloads, such guidance is very helpful. Whereas we could look to a wide range of codes of practices<sup>10</sup> that may also be relevant for regulating drones, we decided

---

<sup>4</sup> ICO, *Surveillance Roadmap - A shared approach to the regulation of surveillance in the United Kingdom*, 2014, [http://ico.org.uk/about\\_us/how\\_we\\_work/~media/documents/library/Corporate/Practical\\_application/surveillance-road-map.pdf](http://ico.org.uk/about_us/how_we_work/~media/documents/library/Corporate/Practical_application/surveillance-road-map.pdf)

<sup>5</sup> Home Office, *Surveillance Camera Code of Practice*, 2013, <https://www.gov.uk/>

<sup>6</sup> United Kingdom Parliament, Data Protection Act 1998, 16.07.1998 ("UK DPA 1998").

<sup>7</sup> UK ICO, CCTV Code of Practice. Draft for Consultation 20 May 2014 - 1 July 2014", 2014. <http://ico.org>.

<sup>8</sup> ICO, *Surveillance Roadmap*, 2014,

<sup>9</sup> Ibid.

<sup>10</sup> Code of Practice on Notification of data breach, Code of Practice on Data sharing, Code of Practice on Police, justice and borders, etc.

to deeply examine two fundamental aspects in the context of RPAS technology, one being an interesting pro-active approach: Privacy by Design and the other being a controversial application of drone: visual surveillance.

### ***Good practice 1. Commercial operators - A Privacy by Design (PbD) Approach***

As a reminder, Privacy by Design is “an approach to projects that promotes privacy and data protection compliance from the start”. We have found that by adopting this approach drones’ manufacturers will render this surveillance technology privacy-friendly. Furthermore, the adoption of such approach will make the RPAS industry more likely to meet their legal obligations and less likely to breach the Data Protection Act. Regarding to individuals, it will make the RPAS technology less privacy intrusive and then, will have less negative impact on data subjects.<sup>11</sup> We will see later that the adoption of a “Privacy by Design” approach for regulating drones has also been strongly recommended by the Privacy Commissioner of Ontario, Dr. Ann Cavoukian, who has issued a report specifically devoted to the Privacy by Design approach and civil drones. In this report, she explains how a “Privacy by Design (PbD) approach can assist in ensuring that the benefits of UAV technology are facilitated, while simultaneously ensuring that the threat to individual privacy is reduced”.<sup>12</sup>

Although “Privacy by Design” approach is not yet a requirement of the Data Protection Directive that Member States shall implement, the UK Data Protection Authority (the Information Commissioner Office) already “encourages organizations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle”. In this regard, they have issued two Codes of Practice which take integral part of the PbD approach: the Code of Practice on Anonymization and the Code of Practice Privacy impact assessment.

#### ***Code of Practice on Anonymisation***<sup>13</sup>

Recalling that drones’ operators often inadvertently capture data not necessary for the purpose of the flight, the “anonymisation” process must certainly be seen as a privacy-friendly way to help RPAS operators to collect information in the exercise of their activities in compliance with data protection law. Furthermore, “anonymisation safeguards individuals’ privacy and is a practical example of the ‘privacy by design’ principles that data protection law promotes”.<sup>14</sup>

The recital 26 of the current Data Protection Directive states that the principles of data protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. It also says that a code of practice can provide guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible. However, neither the Directive nor the DPA provide any technical advice on anonymisation techniques. In that respect, the UK Data Protection Authority has published the first Code of practice on anonymisation. Although data protection law does not apply to data rendered anonymous, this Code provides fewer legal restrictions

---

<sup>11</sup> ICO, *Privacy by design*, 2014.

[http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/privacy\\_by\\_design](http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_by_design)

<sup>12</sup> Ann Cavoukian, *IPC Report- Privacy and Drones: Unmanned Aerial Vehicles*, 2012, <http://www.ipc.on.ca/images/Resources/pbd-drones.pdf>

<sup>13</sup> ICO, “Anonymisation: managing data protection risk code of practice”, *Code of Practice on anonymisation data protection risk*, 2012. [http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/~/\\_media/documents/library/Data\\_Protection/Practical\\_application/anonymisation-codev2.pdf](http://ico.org.uk/for_organisations/data_protection/topic_guides/~/_media/documents/library/Data_Protection/Practical_application/anonymisation-codev2.pdf)

<sup>14</sup> Ibid

which shall apply to anonymized data. It also provides good practice advice that will be relevant to public as well private entities that convert personal data into a form in which individuals are no longer identifiable. An anonymised dataset can still present residual risks to data subjects, especially risks related to the “re-identification” of data or to the public trust if the disclosure concerned data not 100% anonymized. The Code shows that “the effective anonymisation of personal data is possible, desirable and can help society to make rich data resources”<sup>15</sup> by considering the recommendations of entities’ who have assessed the effectiveness of different anonymisation techniques. Furthermore, it demonstrates that there are some quite simple and very effective techniques for anonymisation, and that it does not need to be an onerous process.

We have also demonstrated in the previous chapters that drones’ uses to process data may raise certain risks regarding to the minimization and the purpose-limitation principles. But it appears that rendering data anonymous, drones’ collector supports by essence the data protection law’s general data minimisation approach and the multiple uses of data for different purposes is legitimate as data are not personal data anymore. We also invoked the fact that public has a certain mistrust regarding to the uses of drones in civilian contexts and the massive amount of information that drones’ operators are able to collect thanks to this technology. However, the UK ICO emphasised in its code that another benefit of such anonymisation techniques for data collectors is that they will gain “the public confidence that data is being used for the public good whilst privacy is being protected”.

*a) A Handbook and Code of Practice on Privacy Impact Assessment*<sup>16</sup>

As mentioned above, in the UK, there is no prior-checking by the Data Protection Authority prior to risky processing activities. This lack of a proactive security mechanism increases even more the risks of data breaches and transparency issues already high in the context of civilian RPAS. However, the UK Data Protection Authority has adopted several guidance helping entities to ensure privacy at the start of their project by conducting initially a Privacy Impact Assessment (PIA). Privacy impact assessments (PIAs) “are a tool that you can use to identify and reduce the privacy risks of your projects. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help you to design more efficient and effective processes for handling personal data”, states the ICO.

Currently, adopting a PIA is not mandatory in Europe. However, the Commission encourages the EU and Member States to adopt progressive privacy impact assessment policies and has included in its Proposal Regulation a requirement for data collectors to adopt PIAs prior risky processing. In this respect, “In July 2007, the UK Information Commissioner’s Office commissioned a team of researchers, to conduct a study into Privacy Impact Assessments (PIAs). The project resulted in a Handbook, which assists organisations in identifying and minimizing the privacy risks of new projects or policies. It also considers how organizations can integrate PIAs into existing project management and risk management methodologies and policies”.<sup>17</sup> Besides this PIA Handbook, the ICO has also issued its own guidance in a Code

---

<sup>15</sup> Ibid.

<sup>16</sup> ICO, *Privacy Impact Assessment Handbook*, 2011.  
[http://ico.org.uk/pia\\_handbook\\_html\\_v2/files/PIAhandbookV2.pdf](http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf) and ICO, *Conducting privacy impact assessments code of practice*, 2014.  
[http://ico.org.uk/for\\_organisations/guidance\\_index/~/\\_media/documents/library/Data\\_Protection/Practical\\_application/pia-code-of-practice-final-draft.pdf](http://ico.org.uk/for_organisations/guidance_index/~/_media/documents/library/Data_Protection/Practical_application/pia-code-of-practice-final-draft.pdf)

<sup>17</sup> ICO, *Privacy Impact Assessment Handbook*, 2011.  
[http://ico.org.uk/pia\\_handbook\\_html\\_v2/files/PIAhandbookV2.pdf](http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf)

of Practice. This Code of Practice “explains the principles which form the basis for a PIA and sets out the basic steps which an organization should carry out during the assessment process”.<sup>18</sup>

Whereas we will see in detail in the next chapter how PIA is an interesting soft-low mechanism in the context of RPAS, we can already highlight that this ICO Code requires that new surveillance systems or the application of new technology to an existing system must be subject to PIAs.<sup>19</sup> Therefore, regardless if certain stakeholders see RPAS as a new surveillance device or as a combination of a new technology (RPAS itself) to existing technologies (payloads), they fall under the project for which a PIA should be conducted, according to the UK Code of Practice. By requiring such preventive mechanism, the ICO will undoubtedly reduce security concerns and risks of data breaches related to drone uses.

### ***Good practice 2. Commercial operators and State agencies– RPAS mounted with a visual photography payload: the CCTV Code of Practice Draft for Consultation 2014***<sup>20</sup>

As examined in our study of the British surveillance regime, there exist in the UK two Codes of Practice applying to the visual surveillance. The *CCTV Code of Practice* reinforces the DPA requirements by providing “good practice advice for those involved in operating CCTV and other surveillance camera devices that view or record individual’s information, and covers other information that relates to individuals”<sup>21</sup> and the *Surveillance Camera Code of Practice* provides “guiding principles that should apply to all surveillance camera systems in public places”<sup>22</sup>. However, it is noteworthy that although they apply to CCTV systems used by private entities, professionals and State authorities in their overt surveillance missions, they do not apply to covert surveillance regulated by the RIPA.<sup>23</sup>

Such best practices are very interesting in the context of visual surveillance performed through the means of drones, as in both codes we found purpose limitation, transparency, accountability and data retention principles specifically designed to apply to the characteristics of visual surveillance technologies.<sup>24</sup> Furthermore, the future CCTV Code of Practice 2014 explicitly covers RPAS technology and sets up a specific chapter on drones. In

---

<sup>18</sup> ICO, *CCTV Code of Practice*, op. cit., 2014.  
[http://ico.org.uk/about\\_us/consultations/~media/documents/library/Data\\_Protection/Research\\_and\\_reports/draft-cctv-cop.pdf](http://ico.org.uk/about_us/consultations/~media/documents/library/Data_Protection/Research_and_reports/draft-cctv-cop.pdf)

<sup>19</sup> Ibid.

<sup>20</sup> Ibid.

<sup>21</sup> Ibid.

<sup>22</sup> Home Office, *Surveillance Camera Code of Practice*, 2013.

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/204775/Surveillance\\_Camera\\_Code\\_of\\_Practice\\_WEB.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf)

<sup>23</sup> The United Kingdom, Regulation of Investigatory Powers Act 2000, 20.07.2000 (“UK RIPA 2000”).

<sup>24</sup> ICO, *CCTV Code of Practice*: op. cit., 2014 and UK Home Office, *Surveillance Camera Code of Practice*, 2013,

[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/204775/Surveillance\\_Camera\\_Code\\_of\\_Practice\\_WEB.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf)

this, the UK DPA recommends to data collectors using RPAS to conduct PIAs, to inform individuals that recording camera is in place but also to adopt Privacy by Design measures like encryption, specific focussing lens, deletion schedules. It also recalls that drones operators have to ensure in their processing activities basic data protection principles. Finally, the Code also provides specific recommendations for certain payloads, like ANPR, which can be mounted on drones.<sup>25</sup> Although there is no enforcement mechanism to enforce these guidelines, this is already a big step in the strengthening of the data protection in RPAS applications.

### 10.2.2 France

*Areas where current regulatory mechanisms are working well and elements of good practice*

#### ***Good Practice 1. Commercial operators - Guide on risks management***<sup>26</sup>

The French legal data protection framework does not require preventive security measures like Privacy by Design, Privacy Impact Assessment. However, its DPA (CNIL) has issued a *Guide on Risks Management* aiming to reinforce the security of data processing. The management of risks existing in many fields, the CNIL has decided to transpose this process to the privacy matter.<sup>27</sup> In order to help data collectors to comply with data protection law and avoid data breaches, this soft-law measure provides guidance to identify different types of risks related to a data processing operation and how to address them prior executing the processing activity.<sup>28</sup> As already discussed, civil drones are likely to pose privacy and security risks as they are very unreliable and their content may be easily hacked. Therefore, such guidance is an interesting pro-active instrument which will help data collectors to mitigate security risks from the start.

#### ***Good Practice 2. Commercial operators, State agencies and Private users: Factsheets on video surveillance***<sup>29</sup>

As pointed out in our analysis of national legal regimes, the French surveillance legal framework encompasses some specific regulations applicable to the visual surveillance, called in France “videoprotection”.<sup>30</sup> We had emphasised that besides the processing of individuals’ images governed by the data protection law, the installation and the use of video surveillance cameras are also regulated by many specific sector laws (security code, labor law, etc.).

While the simple presence of comprehensive and privacy oriented visual-surveillance rules makes already a big difference compared to other Member States, the CNIL has adopted six

---

<sup>25</sup> Ibid.

<sup>26</sup> CNIL, *Guide gérer les risques sur les libertés et la vie privée*, 2012,

[http://www.cnil.fr/fileadmin/documents/Guides\\_pratiques/CNIL-Guide\\_Seurite\\_avance\\_Methode.pdf](http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Seurite_avance_Methode.pdf)

<sup>27</sup> Ibid.

<sup>28</sup> Ibid.

<sup>29</sup> CNIL, Factsheets on video surveillance, 2014, <http://www.cnil.fr/les-themes/videosurveillance>

<sup>30</sup> French word used for visual surveillance.

practical factsheets affording some guidance for individuals, public and private entities using CCTV systems. These factsheets sum up in simple terms the legal rules applicable according to the type of places where the visual surveillance takes place (video surveillance at home, at work, in school buildings, in public places, in shops and in residential buildings).<sup>31</sup> Moreover, they give some practical and high-level privacy protection recommendations.

For example, the factsheet “video surveillance on public places” explains that only public bodies can install and film for specific purposes (preventing criminal infractions, terrorism, environmental disasters, etc.) in public places. Moreover, they require that public authorities inform the public of the presence of a surveillance camera and recommend them to adopt irreversible masking technologic measures like blurring images when private places are on the sight of the camera. Another interesting example regards the factsheet on “video surveillance at home” which remind private individuals that they can only install surveillance camera which film the interior of their own property (excluding all camera overflowing on streets, neighbors backyards). Moreover, it also recommends respecting privacy of the family members by recalling that even inside the house there is a need to respect the relatives’ right to their own image.

These factsheets could be seen as “best practices” and should be seen as an interesting instrument for regulating civil drones. Indeed, whereas the existing video surveillance regulations are a priori applicable to RPAS equipped with visual surveillance payloads, we have previously observed how the implementation of existing legal framework to such new aerial technology may pose some concerns in practice. So either by adopting new factsheets specific to drones or by complementing the existing ones with specific recommendations on mobile cameras as well as other payloads, we recommend to Member States to adopt such kind of guidance to facilitate collectors using RPAS with panoptical payloads to understand and comply with the data protection law and the privacy right.

***Good Practice 3. All operators including private individuals – The Right to one’s own image: the strengthening of the consent requirement (transparency)***

In France, we have seen that in addition to the data protection right, everyone has a right to ones’ own image. This jurisprudential and doctrinal creation allows anyone to object - whatever the nature of the mean used – to the capture and the disclosure of one’s image without their express authorization.<sup>32</sup> Therefore, a double obligation for drones’ operator stems from this right – RPAS operators are obligated to get such consent prior the capture and prior the dissemination of the image in public.<sup>33</sup> Such authorisation/consent of the person concerned must be express and sufficiently precise (including information about the purposes of the image collection and the duration of the image’s retention).<sup>34</sup>

---

<sup>31</sup> CNIL, Factsheets on video surveillance, 2014, <http://www.cnil.fr/les-themes/videosurveillance>

<sup>32</sup> CNIL, « L'utilisation de l'image des personnes », 2005.

<http://www.cnil.fr/linstitution/actualite/article/article/lutilisation-de-limage-des-personnes/>

<sup>33</sup> *ibid.*

<sup>34</sup> *ibid.*

Although there are some exemptions to such right, it strengthens the consent requirement and thus the transparency principle already existing in the Data Protection Act. This right is particularly relevant when drones processing images are performed by a journalist or a private individual as it comes to mitigate the exemption figuring in the data protection law. In other words, through this right individuals from who images have been captured or disclosed by drones' operators without consent may invoke a violation of their privacy and a suppression of the image in front of courts and tribunals, regardless the type of drones' operators (journalists, private individuals, commercial, police). Finally, the violation of such right is punishable under French criminal law to an imprisonment penalty of one year and a fine of 45,000€. <sup>35</sup> Given the deterrent effect of such penalty, drones operator should easily comply with this right.

#### ***Good Practice 4. Specific rules strengthening privacy dimensions***

##### ***a) Commercial operators, journalists and State agencies – The strengthening of the individuals' bodily privacy***

We have to recall that the French Data Protection Act is part of the few Member States data protection regimes that has implemented the prior-checking mechanism as prescribed by Article 25 of the European DPD. <sup>36</sup> By doing so, the French DPA (CNIL) has the obligation to assess all risky processing activities before giving an authorisation of data processing to the collectors. As mentioned, such preventive mechanism is very relevant in the context of civilian drones as whether it applies to them, it would provide to the Supervisory Authority a certain control on the more privacy intrusive processing activities.

Furthermore, the French data protection law applies such prior checking to the biometric data processing. <sup>37</sup> By introducing such higher data protection safeguards, the French law does not only implement the Directive 95/46/EC but it particularly affords a second protection when processing activities interfere with bodily privacy. Drones being able to be fitted with soft biometric recognition systems, they will likely pose concerns with bodily privacy. Therefore, such introduction of rules addressing not only data protection concerns but also mitigating bodily privacy issues can only be seen as an added value.

##### ***b) State agencies - The strengthening of the individuals' location privacy***

Contrary to other Member States, we have seen that the French government has adopted a specific law governing geo-localisation technologies like GPS tracking devices and ANPR systems used for covert surveillance. <sup>38</sup> This law prohibits the use of such surveillance by other actors than law enforcement authorities and affords many safeguards (independent supervisory authority, judicial authorisation, accountability), which tend to especially reinforce location privacy. Therefore, it also reinforces the privacy of individuals when sophisticated and tracking technologies are mounted on civil drones. Besides, bringing further safeguards when drones are fitted with one of these geo-localisation devices such law affords the example that for new intrusive surveillance technologies, stricter rules and safeguards should be adopted.

---

<sup>35</sup> France, Article 226-1 of the Criminal Code, 22.07.1992.

<sup>36</sup> French Parliament, Computer, Files and Liberties Act, 13.10.1978 ("French CFLA 1978"), Article 25.

<sup>37</sup> French CFLA 1978, Article 25

<sup>38</sup> France, The geo-localisation Act , « Loi relative à la géolocalisation », 28.03.2014.

We strongly share the view that for new, intrusive surveillance technologies like drones which raise privacy issues among all privacy dimensions, Member States should set up specific privacy rules besides the ordinary data protection law. Therefore, the French privacy regime should be seen as a model in this regard. Firstly, it takes account of the different dimensions of privacy and not only data privacy like in most of the Member States. Secondly, it shows that there are two ways to introduce such protection, either by adopting higher safeguards in the data protection law itself (general application) or by adopting a specific regulation (for the law enforcement sector). We strongly think that such an approach should be adopted by Member States in order to reinforce the privacy regime applying to the law enforcement sector using new surveillance technologies.

#### ***Good Practice 5. Commercial operators, Journalists and State agencies - Prohibition for magistrates to rely on data processed by a drone to base their judgments***

Can drones operators use the information collected through drones in front courts and tribunals? This question has often been raised in newspapers articles on RPAS. In France, the data protection law itself gives an negative answer “Aucune décision de justice impliquant une appréciation sur le comportement d’une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité. Aucune autre décision produisant des effets juridiques à l’égard d’une personne ne peut être prise sur le seul fondement d’un traitement automatisé de données destiné à définir le profil de l’intéressé ou à évaluer certains aspects de sa personnalité».<sup>39</sup> This prohibition for the judicial authorities to adopt a judgment on evidences which consists in a profile build on the collection of personal data is very protective for individuals. It prevents that personal data processed by drones will constitute sufficient evidences to base a judgment. As drones can be easily hacked, it is very important that a judicial decision cannot rely on such unreliable technology.

#### ***Good Practice 6. Journalists – A strict interpretation of the exemption***

In the Law on Inforatics, Files and Freedoms (the French Data Protection Act), we found also an exemption for processing activities exercised for journalistic purposes. However, contrary to the ECJ case law, the Act stipulates that “the exemption for journalism only applies to professional journalists and not to others exercising their right to freedom of expression”.<sup>40</sup> Therefore, “bloggers”, Youtubers and “citizens-journalists” using drones for disclosure of information to the public do not fall under the exemption. So they have to ensure all principles and data subject rights of the data protection law. Such *sensu stricto* interpretation of the exemption not only reduces risks of voyeurism activities, press scandals but also prevents abuses of personal data disclosure of individuals against their will.

Furthermore, it only applies as long as the “professional journalist” acts in conformity with his own professional-ethical rules and the requirements of those rules are far from precise in certain contexts.<sup>41</sup> Moreover, Article 7 stipulates that “while the Law exempts journalists (and

---

<sup>39</sup> French CFLA 1978, Article 10.

<sup>40</sup> French CFLA, 1978.

<sup>41</sup> European Commission - Directorate-General Justice, Freedom And Security Douwe Korff (Eds.), Comparative Study Different Approaches To New Privacy Challenges, In Particular In The Light Of Technological Developments – France, 2010.

their employers) from the duty to notify, it replaces this with a duty to appoint an in-house data protection official who must ensure compliance with the Law also to journalists (Art. 67(2)).<sup>42</sup> Finally, although “individuals may not be able to exercise their rights of access and correction, etc. under data protection law, they do retain important rights (including privacy rights against publication and the right to reply to publications)” based on other French privacy laws.<sup>43</sup> Such adoption of additional safeguards will necessarily mitigate the risks related to the usage of RPAS by journalists. Therefore, we welcome such French initiatives.

### ***Good Practice 7. State Agencies – processing data through the means of drone for security and criminal matters.***

Unlike to the DPD, which expressly excludes its application to the former third pillar matters (security, defence, State security, or criminal matters), the French DPA applies also to such processing activities.<sup>44</sup> Moreover, although we observe that the right to demand information and access can be limited with regard to processing operations related to national security, defense or public security, here is prior-control from the French DPA and from the judicial power. Indeed, when law enforcement operators desire to process personal information for such purposes, they must to obtain a ministerial decree and an authorisation (prior-checking mechanism) from the French Data Protection Authority (CNIL), which must appoint a judicial member of that body to deal with the matter.<sup>45</sup> Then, “the CNIL member inspects the operations and files concerned on behalf of the data subject, who is only informed of the fact that the inspection has taken place without being informed of the outcome of the inspection (Art. 41(2)), unless the CNIL finds, and the controller agrees, that the privileged matters (national security, etc.) will not be jeopardized by providing the information and/or the data (Art. 41(3))”<sup>46</sup>. Finally, when State agencies use RPAS for visual surveillance in an investigative procedure, the police officer must obtain an ordinary judicial warrant (prosecutor or judge on the basis of specific provisions).

Therefore, there is no legal vacuum when drones are used by French State Agencies for processing data. The law enforcement sector can be sometimes very intrusive in the privacy of individuals particularly through the means of drones as they can be mounted with very sophisticated equipment and being undetectable. However, the need of a warrant from the judicial power and the need of an authorisation from the CNIL reduces the risks of abuses and makes the police sector accountable and responsible in front a supervisory authority. This will improve the trust of the public in such so controversial use.

Nevertheless, we would like to stress that in all cases individuals should be informed of the processing, at least after that the covert surveillance measure has been undertaken if the notification prior the collection would risk to jeopardise the mission.

### ***10.2.3 Germany***

#### ***Current and emerging RPAS applications not adequately covered by existing and proposed national legislation***

---

<sup>42</sup> French CFLA 1978, Article 7.

<sup>43</sup> Douwe Korff (Eds.), op. cit., 2010.

<sup>44</sup> French CFLA 1978 and Douwe Korff (Eds.), op. cit., 2010.

<sup>45</sup> Douwe Korff (Eds.), op. cit., 2010.

<sup>46</sup> French CFLA 1978 and Douwe Korff (Eds.), op. cit., 2010.

### ***Problem 1. State Agencies - Lack of transparency in surveillance operations***

During our analysis of the German surveillance regime, we remarked that the data protection law applies also to data processing performed by State agencies (law enforcement sector).<sup>47</sup> However, it figures certain exceptions regarding individuals' rights. For instance, when police use drones for collecting data related to security (national security, public order, and defense) and criminal matters, they are exempted from enforcing the right to be informed and the right to access data. Furthermore, we have seen that State's intelligence agencies may perform automated wiretaps of domestic and international communications without warrant.<sup>48</sup> Furthermore, after a measure of surveillance "any notification of the person concerned is dispensable if the data is ready for deletion".<sup>49</sup> Although, this legal vacuum has already been pointed out by DPAs during the Conference of Data Protection Commissioners in 2001, the law has not been amended.<sup>50</sup> Applied to the context of the RPAS technology, this means that under certain circumstances, law enforcement authorities would be able to use drones to track individual or to intercept their communications without notifying the individual concerned and without any control from an independent supervisory authority.

Such lack of transparency and supervision by the judicial power will only reinforce the risks related to drones like mission creep, dehumanisation of surveillance, etc. Furthermore, it will certainly lead to abuses from the law enforcement sector when they will use drones in there surveillance operations.

*Areas where current regulatory mechanisms are working well and elements of good practice*

### ***Good Practice 1. Commercial, Journalists and State Agencies – The recognition of data minimisation, anonymisation, pseudonomisation principles and the limitations to profiling activities***

The German data protection regime is one of the strictest in the European Union.<sup>51</sup> For instance, we have discussed that the German Federal Data Protection Act (BDSG) explicitly includes anonymisation, pseudonomisation and data minimisation principles.<sup>52</sup> Furthermore, the admissibility principle (also called legitimacy principle) is stricter than in other Member

---

<sup>47</sup> German Parliament, Federal Data Protection Act, "Bundesdatenschutzgesetz", 20.12.1990

<sup>48</sup> The Constitutional Court has ruled that the police may use GPS technology to track suspects driving motor vehicles in cases of serious crimes even without a judicial warrant; Federal Constitutional Court (Bundesverfassungsgericht), decision of 12 April 2005, reference number 2 BvR 581/01 and the G-10 Law allows warrantless automated wiretaps of domestic and international communications by the national and states' Intelligence Services for purposes of protecting the freedom and the democratic order, preventing terrorism and illegal trade in drugs and weapons.; Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10).

<sup>49</sup> Conference of Data Protection Commissioners (Konferenz der Datenschutzbeauftragten des Bundes und der Länder), Düsseldorf, 8/9 May 2001 and Privacy International, the Electronic Privacy Information Center (EPIC) and the Center for Media and Communications Studies (CMCS), *European Privacy and Human Rights* (EPHR) 2010, p. 313.

<sup>50</sup> Ibid.

<sup>51</sup> Privacy International, the Electronic Privacy Information Center (EPIC) and the Center for Media and Communications Studies (CMCS), *European Privacy and Human Rights* (EPHR) 2010, p. 313.

<sup>52</sup> German DPA1990, Section 3a.

States and the consent requirement is strengthened.<sup>53</sup> Moreover, the German FDA provides very strict limits to “profiling” and “data mining” activities.<sup>54</sup> In this regard the German Data Protection Authority has recently issued: *“The Federal and State Data Protection Commissioners find the following measures to be necessary to protect individuals against unlawful profiling: Profiling should be allowed only on a concrete legal basis which is sensitive to the special threat potential of profiling, or on the basis of the data subject’s informed consent. Effective consent requires comprehensive information about the range and origin of linked data, the purpose of the profile and how it will be used, the controller and planned date of deletion. Consent must be voluntary and revocable at any time. If consent is withdrawn, the profile must be immediately deleted, also by those controllers to which it has been transmitted. For example, there is a prior-checking mechanism for processing activities regarding “behavior monitoring” which includes profiling”*.<sup>55</sup> Additionally, the German Constitutional Court made clear in a recent that profiling activities by public bodies are prohibited unless they meet the standards of the German Constitution.<sup>56</sup>

Consequently, it appears that the German data protection law is going far further in some points than the European Data Protection Directive 95/46/EC. Such reinforcement of basic principles has a general great impact on the protection of data subjects whom the data are subject to processing activities. Additionally, in the context of RPAS technology, this is particularly relevant as we have previously examined that drones pose particular implementation concerns with the data minimisation principle due to the massive amount of data they process and raise risks of discrimination and data breaches in the context of profiling activities. In this respect, we strongly support the recommendation of the German Data Protection Authority, which imposes very strict limitations to profiling activities. We think that such strict approach should also be adopted at the European level, at least when profiling activities aim to serve surveillance missions. Finally, the incorporation of new principles like anonymisation and pseudonomisation are warmly welcomed as they reduce data breaches and unlawful disclosure, highest risks in the context of drones, and promote the Privacy by Design approach.

---

<sup>53</sup> German DPA 1990 ,Section 4. *“Section 4 Lawfulness of data collection, processing and use (1) The collection, processing and use of personal data shall be lawful only if permitted or ordered by this Act or other law, or if the data subject has provided consent.*

*Section 4a Consent*

*(1) Consent shall be effective only when based on the data subject’s free decision. Data subjects shall be informed of the purpose of collection, processing or use and, as necessary in the individual case or on request, of the consequences of withholding consent. Consent shall be given in writing unless special circumstances warrant any other form. If consent is to be given together with other written declarations, it shall be made distinguishable in its appearance”*. German Parliament, Federal Data Protection Act, “Bundesdatenschutzgesetz”, 20.12.1990 (“German DPA1990”), Section 4.

<sup>54</sup> Gerrit, Hornung and Christoph Schnabel, “Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention”, *Computer law & security review*, Vol. 25, 2009, pp. 115-122.

<sup>55</sup> The Federal Commissioner for Data Protection and Freedom of Information, *Comments on the consultation regarding the Communication “A comprehensive approach on personal data protection in the European Union”*, COM(2010) 609 final, 2010.

<sup>56</sup> Douwe Korff, *Comparative study on different approaches to new privacy challenges, In particular in the light of technological developments- Country A. 4 Germany*, 2010.

### ***Good Practice 2. Commercial, Journalists and State Agencies – The strengthening of data protection standards when drones capture images***

In Germany, there exist several specific regulations covering the use of drones mounted with a camera processing images of individuals.

Firstly, it is important to recall that since 2009 the German Federal data protection law encompasses a Section 6b on “monitoring of publicly accessible areas with optic-electronic devices”.<sup>57</sup> Therefore, German drones operators using a RPAS equipped with a visual camera have to respect the general requirements of the FDA but also this specific Section which encompasses more specific obligations. For instance, legitimate purposes, purpose limitations and transparency principles are specified by the German legislator for such kind of processing.

Besides the data protection law whose scope excludes domestic and journalism processing, the German privacy regime encompasses a right to one’s image and personality rights. Like we have seen with the French regime, the right to one’s own image applies in complement to the FDA.<sup>58</sup> This right implies that in case of images are recorded by drones, the individual’s consent is necessarily needed both prior the capture and the prior dissemination in public. Regarding personality rights, the legal basis for these rights is provided “by two separate provisions of the constitution, namely the protection of human dignity (Article 1, para. 1) and the protection of general personal liberty (Article 2, para. 1)”.<sup>59</sup> “Together they form the general right of personality which guarantees each individual the possibility to develop his/her own personality”.<sup>60</sup> Consequently, “private residential property which is shielded and not visible from neighbouring private property or from the public highway is a typical area to which the owner may wish to retreat. “Spying” on someone in this case would therefore infringe their personality rights. This includes photographs or films taken of the property owner from civilian drones. However, this is only the case if the images captured are of good quality. If the images are a blurred bird’s eye view, the property owner’s personality rights would not apply”.<sup>61</sup>

By specifying the data protection law and strengthening the privacy of individuals, these regulations and rights will mitigate the risks pose when drones process images of persons or things. It will particularly reinforce the consent principle already existing in the FDA. Furthermore, these both rights (personality rights and right to one’s own image) are particularly useful when individuals are photographed by a private or a journalistic drone as they do not encompass derogations contrary to the FDA. Therefore, whatever purposes for which they capture images through the means of drones, operators are always required to obtain the consent of the person photographed in Germany.

---

<sup>57</sup> German DPA 1990, Section 6b.

<sup>58</sup> [Solmecke](http://www.wbs-law.de/internetrecht/civilian-drones-legal-issues-surrounding-use-50459/), Christian, “Civilian drones and the legal issues surrounding their use”, 2014, <http://www.wbs-law.de/internetrecht/civilian-drones-legal-issues-surrounding-use-50459/>

<sup>59</sup> German Parliament, Basic Law for the Federal Republic of Germany, “Grundgesetz”, 23.05.1949 (“German Basic Law”),

<sup>60</sup> [Solmecke](#), Christian,, op. cit., 2014.

<sup>61</sup> Ibid.

### ***Good Practice 3. Commercial operators, Journalists and State agencies – The strengthening of the individuals’ bodily privacy and behavior privacy***

It is worth recalling that the Section 4d (4) of the FDA states “(5) *Where automated processing operations present special risks to the rights and freedoms of data subjects, these operations shall be examined before the start of processing (prior checking). Such prior checks shall be carried out in particular if **special categories of personal data (includes data related to the body)** (Section 3 (9)) are to be processed, or the processing of personal data is intended to assess the data subject’s personality and his/her abilities, performance or **behavior***”<sup>62</sup>. So according to this Article, the processing of bodily data or behaviors are subject to a prior-checking by the German DPA.

Fitted with smart surveillance payload like behavior recognition or soft biometric recognition, drones may seriously interfere with the intimate sphere of individuals, particularly by affecting their behavior privacy and bodily privacy. However, through this above-mentioned preventive security measure, the German Data Protection Authority not only protects data privacy but also other aspects of privacy. Consequently, drones operators using RPAS equipped with such privacy intrusive equipment will be assess prior processing and will eventually have to adopt specific measures to prevent privacy and data processing risks.

#### *10.2.4 Italy*

*Current and emerging RPAS applications no adequately covered by existing and proposed national legislation*

#### ***Problem 1. Commercial operators - A simplification of the notification requirement: a lack of transparency and independent supervision***

“Notification is required only with regard to data processing which could jeopardise the rights and freedom of the [data subjects](#) because of the method of processing or the nature of the personal data it relates to”<sup>63</sup>. This statement clarifies Article 37 of the Italian Code on personal data.<sup>64</sup> Therefore, private entities using drones for processing data are only required to notify the Garante when processing activities concerns certain categories of data or is performed through the means of specific technologies.<sup>65</sup> While the Code does not give guidance about what it means by “specific technology”, it gives a list of the categories of data which fall under the prior notification. We can found, for example, genetic and biometric data, data processed for the purpose of analysing or profiling individuals, monitoring use of electronic communications services, data disclosing sex life and the psychological sphere (see Section 37 of the code for additional details).<sup>66</sup> Furthermore, no approval is required and “notification is subject to a fee of EUR 150”<sup>67</sup>, explains a data protection report on the Italian data protection law. Therefore, although we have often emphasised how transparency is a core principle of the data protection, Article 37 of the Italian Code of personal data has made the

---

<sup>62</sup> German DPA 1990, Section 4d.

<sup>63</sup> Linklaters, “Data Protection – Italy”, 2014, <https://clientsites.linklaters.com/Clients/dataprotected/Pages/Italy.aspx>

<sup>64</sup> Italian Parliament, the Data Protection Code, 30.06.2003 (“Italian Data Protection Code 2003”) Section 37.

<sup>65</sup> Italian Data Protection Code 2003, Section 55.

<sup>66</sup> Privacy International, the Electronic Privacy Information Center (EPIC) and the Center for Media and Communications Studies (CMCS), *European Privacy and Human Rights* (EPHR) 2010.

<sup>67</sup> Linklaters, “Data Protection – Italy”, <https://clientsites.linklaters.com/Clients/dataprotected/Pages/Italy.aspx>

notification requirement to the Italian DPA an exception and costly burden for collectors. Furthermore, the Italian Data Protection Code does not require from the data collector a notification to the DPA in case of data breaches.<sup>68</sup>

In addition, Section 47 (Processing for purposes of Justice) and Section 58 (Processing for purposes of Defence and Security) states that State Agencies which process data related to security and criminal matters are exempted from the obligation to inform the data subject concerned.<sup>69</sup> Furthermore, the Criminal Procedure Code (*Codice di Procedura Penale*) which regulates such surveillance measures do not require that law enforcement bodies inform the individuals which have been subject to a measure of surveillance after this latter has been undertaken.<sup>70</sup>

Consequently, today private entities do not always have to notify the DPA when they process data through the means of drones or when there is a data breach. In addition, law enforcement authorities using drones for processing personal information in a surveillance operations related to a criminal offence or national security do not have to inform the Italian DPA (*Garante*) or the data subject concerned. Such lack of transparency and control by an independent supervisory authority should be particularly highlighted in the context of civil RPAS as it means that not only law enforcement bodies but also private and other public entities do not totally comply with the “transparency principle”.<sup>71</sup>

Whereas the simplification of the notification procedure enshrined in the Code of personal data may be justified for processing through the means of non-intrusive technology, we think that RPAS technology poses too many risks for data subjects and then the transparency principle should be ensured. Therefore, we recommend the Italian DPA to include processing by RPAS technology within the specific technologies of Article 37 and 57 under which a notification to the DPA and prior-checking by the Italian DPA (*Garante*) are mandatory.<sup>72</sup> Regarding the notification of data breach, the Italian legislator would have to implement it when the European GDPR is adopted. When law enforcement authorities use drones for surveillance purposes, a sector subject to high risks of abuses and data breaches, but however exempt of most of the data protection rules, we stress that a notification of the surveillance measure at least after it has been undertaken and a notification to the *Garante* should be the key requirements in such sectors.

*Areas where current regulatory mechanisms are working well and elements of good practice*

***Good Practice 1. Commercial operators - Profiling activities: preventive security measures and prohibition for magistrates to use profiles made through the means of data processing***

Previously, we have seen that collecting data for profiling purposes is facilitated by drones as they are able to capture different categories of data through their wide range of payloads. However, we also found in the previous chapters how processing in order to create profiles can be very intrusive for individuals and may bring issues like discrimination and dehumanisation.

---

<sup>68</sup> Italian Data Protection Code 2003, Section 37.

<sup>69</sup> Italian Data Protection Code 2003, Section 47

<sup>70</sup> Italy, the Criminal Procedure Code, “Codice di Procedura Penale”, 22.09.1988.

<sup>71</sup> Transparency principle imposed by the Directive 95/46/EC.

<sup>72</sup> Italian Data Protection Code 2003, Section 37 and 57.

However, we also examined in the Italian data protection code two interesting provisions:

*“A data controller shall **notify** the processing of personal data he/she intends to perform exclusively if said processing concerns: ... d) data processed with the help of electronic means aimed at profiling the data subject and/or his/her personality, analyzing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users”.*<sup>73</sup>

*“No **judicial or administrative act or measure** involving the assessment of a person’s conduct may be based solely on the automated processing of personal data aimed at defining the data subject’s profile or personality”.*<sup>74</sup>

Consequently, the first article reinforces the transparency principle when data are processed for profiling purposes as such processing must be notified (which is an exception in the Italian Code). Furthermore, the data subject rights are reinforced as judicial and administrative bodies cannot base their decisions on persons’ conduct profile which has been built via data capture through the means of drones for profiling purposes. Drones having been often evoked by newspapers as a new technology for collecting evidences, such article at least prevent certain risks for data subject whose evidences would have been captured by drones. However, we stress that no judgment should only be based on personal data collected by drones regardless the purposes of the processing as this RPAS technology is not reliable (can be easily hacked).

### ***Good practice 2. Commercial operators, Journalists – The strengthening of the individuals’ bodily privacy***

As sensitive data are able to be captured by drones, we have highlighted multiple concerns related to such sensitive data captured by a technology still in development (numerous hackings of their contents have already been observed). Nevertheless, like in Germany, biometric data are subject to additional safeguards in Italy. The DPC but also the Italian DPA recalls that *“genetic data may only be collected and processed with the data subject’s “prior, written” and informed consent. This requirement may only be derogated to establish or defend a judicial claim”.*<sup>75</sup> Furthermore, prior communication from the collector and prior checking from the DPA are required in case of such processing. Consequently, drones operators will be less likely to cause risks to bodily privacy as they are subject to additional safeguards when they process biometric data. Thus, we remark a strengthening of the bodily privacy also in Italy.

### ***Good Practice 3. Commercial operators, Journalists - Specific safeguards for “specific technology”***

As already mentioned, the Italian DPC provides a simplification of the notification duty. This later is only required when specific categories of data are processed and when specific technologies are used.<sup>76</sup> Section 55, which requires all data collectors to notify the Italian

---

<sup>73</sup> Italian Data Protection Code 2003, Section 37.

<sup>74</sup> Italian Data Protection Code 2003, Section 14.

<sup>75</sup> Garante, “Rights and Prevention”, 2014, [http://www.garanteprivacy.it/home\\_en/rights](http://www.garanteprivacy.it/home_en/rights)

<sup>76</sup> Italian Data Protection Code 2003, Section 55.

DPA when they use specific technology, is certainly one of the most relevant provisions in the context of RPAS:

*“Where the processing of personal data carries higher risks of harming data subjects by having regard, in particular, to genetic or biometric data banks, technology based on location data, data banks based on particular data processing techniques and the implementation of special technology, the measures and precautions aimed at safeguarding data subjects shall have to be complied with as required by Section 17 and prior communication shall have to be given to the Garante as per Section 39”.*<sup>77</sup>

So according to this provision not only personal data processed by a specific technology should be communicated to the Italian DPA (*Garante*) prior the processing operations but also the DPA should assesses the processing activities and eventually requires additional protection measures if needed (prior-checking mechanism). RPAS being a sophisticated technology, they should be included in such “specific technology” notion and so their processing activities will be subject to prior assessment by the Italian DPA.

Whereas prior checking mechanisms have been adopted by different Member States in compliance with the Directive 95/46/EC, this mechanism generally applies when special categories of data are processed (sensitive data), regardless of the technology used. Therefore, the Italian DP goes further as it also takes in account the risks that may result from certain technologies. Such extension of the prior-processing scope is seen as “a best practice” to control certain technology uses (including RPAS) and therefore, should be adopted by all European Member States.

***Good Practice 4. Commercial operators, Journalists, State agencies, Private individuals: RPAS equipped with a camera or a behavior recognition system: the application of additional high-level safeguards***

Whereas Italy does not encompass a proper comprehensive CCTV regulation but rather many specific sectorial laws, the Italian DPA issued a Decision and some Guidelines on the video surveillance in 2010. These being very protective, some of them need to be emphasised as they will be particularly relevant to govern visual surveillance performed by drones.

First of all, it is noteworthy that the Italian DPA in its guidance strengthens the data protection rules by stricter standards and specifies each core data protection principles according to the type of operator that uses the camera.<sup>78</sup> Furthermore, in conformity with the “best practices” provision of the Directive 95/46/EC, the Italian DPA has decided to issue a leaflet of guidelines to help video surveillance users to comply with its Decision.<sup>79</sup> As we have seen that not only State agencies but also commercial operators, professionals and

---

<sup>77</sup> Ibid.

<sup>78</sup> “As for the use of any equipment intended for filming, with or without recording of the images, areas outside buildings such as parking places, loading/unloading areas, accesses, emergency exits, etc., it should be recalled that the processing must be such as to limit the visual angle to the area(s) to be protected; this means that the neighbouring areas and any irrelevant items (streets, buildings, shops, institutions) may not be filmed”. Decision on the Video Surveillance, 08.04.2010, Article 6.2.3.

<sup>79</sup> Garante, *Video Surveillance Guidelines by the Italian DPA*, 08.04.2010., <http://194.242.234.211/documents/10160/0704/1767009>.

private individuals are also interested in performing visual surveillance through the means of drones, the presence of strong additional safeguards for all type of drones' operators is very important. For example, in accordance with the right to information, the Decision stipulates that a camera used by public bodies must always inform “*data subjects that they are about to enter an area under video surveillance; this also applies to events and/or public shows (e.g. concerts, sports events, etc.)*”.<sup>80</sup> Another example would concern the prior checking mechanism.

Secondly, the Decision extends the application of the prior-checking mechanism enshrined in the DPC to “*smart*” *video surveillance systems*<sup>81</sup> and to *video surveillance systems coupled with the use of biometrics systems*. Consequently, when data collectors use drones equipped with a smart video surveillance systems or with a camera and a soft biometric system, they need to notify the Italian DPA and this latter must assess the risks of such processing before they performed them. As such preventive security measure will reduce risks related to the security of processing and accountability principles, we recommend all Member States to adopt such prior-checking mechanism when drones are equipped with sophisticated technologies like smart surveillance systems or mounted with a combination of payloads like CCTV and biometric recognition. However, we even stress that such preventive security measure (prior-checking,) should be adopt since drones are used to process personal data as they are in itself a sophisticated technology.

#### ***Good Practice 5. Journalists - Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities***

Like the European Directive, the Italian DPC provides derogations to several provisions, including processing activities for journalistic purposes.<sup>82</sup> Nonetheless, the Italian DPA has issued a *Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities* which applies “to professional journalists, free-lance and trainee journalists and to any person carrying out journalistic activities even occasionally”.<sup>83</sup> Therefore, whereas journalists using RPAS in their processing activities are exempted from some DPC provisions, including principles and individuals' rights, they should apply this Code of Practice.

Such guidance affords additional safeguards and suggests that journalists adopt some “best practices”. For example, the first provision explains, “*The journalistic profession is carried out without being subject to authorisation or censorship but must identify themselves, their profession and the purposes of the collection*”.<sup>84</sup> In the context of drones such provision is particularly relevant as it we have seen earlier that a particular feature of RPAS technology is the “non-identification of the operator”. Additionally, journalists are normally exempt to inform data subjects of their processing activities. Therefore, due to this feature and exemption, when drones are used journalistic purposes, this is ordinary most likely that individuals are not informed. However, thanks to this guideline which recommends to

---

<sup>80</sup> Decision on the Video Surveillance, 08.04.2010, Article 3.1.

<sup>81</sup>“ The so-called smart systems, which do not simply film and record images as they can also automatically detect “deviant” behaviour and/or unusual events, send out alerts and record the relevant images.” Decision on the Video Surveillance, 08.04.2010, Article 3.2.1.

<sup>82</sup> Italian Data Protection Code 2003.

<sup>83</sup> Garante, *Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities*, 03 August 1998.

<sup>84</sup> *Ibid.*, Article 1.

journalists to “identify themselves”, individuals will be able to identify the journalist and access to certain of their rights. By introducing this identification requirement, this Code of Practice introduces more or less “a transparency principle” when data are collected by journalists. By doing such this Code of Practice should be seen as a model and the same recommendation should be spread in all member States.

Secondly, we have often evoked the risk that voyeurism activities will increase with the deployment of drones. Nevertheless, there is enshrined in the Code an obligation to refrain from subterfuge, harassment<sup>85</sup>, to spy a person's residence and other private places<sup>86</sup> and to respect the person's sex life.<sup>87</sup> Moreover, Article 13 affords some disciplinary measures for those which did not comply with the provisions of the Code.<sup>88</sup> Therefore, any journalists which would dare to use drones for voyeurism activities will be sanctioned.

#### 10.2.5 Sweden

*Current and emerging RPAS applications not adequately covered by existing and proposed national legislation*

##### ***Problem 1. Commercial operators, State agencies, Journalists – No Data Breach Notification: A lack of transparency and security***

In our analysis of the Swedish Data Protection Act, we found that there is no mandatory requirement in the Act to report data security breaches or losses to the Data Protection Authority and to inform the data subject. Furthermore, when they occur, “data breaches are only handled on a case-by-case basis and only addressed by the Swedish Data Protection Authority if they relate to a large number of data subjects or indicate a general non-compliance issue”.<sup>89</sup>

Given we have seen that drones are easily hacked, security preventive and remedial measures are strongly needed in context of RPAS applications. However, according to these above considerations of the Swedish law, there is a lack of remedial measure, a lack of monitoring mechanism by the Swedish DPA and a lack of transparency towards the data subject. Therefore, this legal vacuum should be addressed.

##### ***Problem 2. State agencies – Interception of communication: a lack of transparency and judicial supervision***

In the framework of the analysis of the Swedish surveillance regime, we observed that the Swedish Intelligence agency can intercept telecommunications and traffic Internet data through the means of drones without the need of a court order from a judicial authority.<sup>90</sup> This lack of supervision by an independent supervisory authority is a real concern in the context of drones as they can pose high risks when they are used for surveillance missions.

---

<sup>85</sup> Ibid., Article 2.

<sup>86</sup> Ibid., Article 3.

<sup>87</sup> Ibid., Article 11.

<sup>88</sup> Ibid., Article 13.

<sup>89</sup> Nilsson, Henrik, “Data Protection and Privacy in 26 jurisdictions worldwide- - Data Protection & Privacy 2014”, in Rosemary P Jay (Eds.), *Getting the Deal Through*, Law Business Research Ltd, Canada, 2013.

<sup>90</sup> Groupe Européen d’Ethique des Sciences et des Nouvelles Technologies, Avis 28 sur l’éthique des technologies de sécurité et de surveillance, Brussels, 20.05.2014.

Consequently, there are likely to cause abuses and there is no accountability to mitigate such misuses.

#### *Areas where current regulatory mechanisms are working well and elements of good practice*

Given that we could not access to an English version of the Swedish guidance issued by the Swedish Data Protection Authority, our analysis of “the privacy and data protection good practices” is very limited in this country.

#### ***Good Practice 1. Commercial operators and State agencies – RPAS equipped with a camera: A strict control on the uses***

In Sweden, private and public entities need a license delivered by the county administrative board concerned for the installation of a video surveillance device in public places.<sup>91</sup> Moreover, this licence is only delivered after having weighed this surveillance interest against the interest for integrity. Applied to RPAS technology, this means that commercial operators and State agencies using a RPAS mounted with a camera will need a license which will only be delivered if the interference into the privacy and integrity of individuals is proportionate to the added value of the surveillance measure. This rule makes reference to the proportionality principle figuring in Article 8 ECHR. Such rule is very relevant in the context of drones as they have been lively criticised when they are used in visual surveillance applications due to the high risks they pose for all type of privacy.<sup>92</sup> This strengthening of the proportionality principle when privacy is at stake and this effective control by an independent supervisory authority is a welcome initiative from the Swedish legislator. This will reinforce the compliance with the data protection law as well as increase the public trust face to the use of RPAS technology.

#### *10.2.6 Denmark*

*Current and emerging RPAS applications no adequately covered by existing and proposed national legislation*

#### ***Problem 1. State agencies – RPAS equipped with camera for visual surveillance: a lack of high-level safeguards***

In our analysis of the Danish surveillance regime we have seen that the interception of communications are governed by high-level standards (obligation to have a warrant<sup>93</sup>, a strict purpose limitation principle<sup>94</sup>, a kind of necessary principle<sup>95</sup>, a requirement as to the nature

---

<sup>91</sup> Swedish Parliament, The Swedish Camera Monitoring Act, 2013 and The Swedish National Council for Crime Prevention, Report on CCTV Surveillance of Stureplan and Medborgarplatsen, 2014.

<sup>92</sup> See Chapter 5 of this deliverable.

<sup>93</sup> Any interception of communications must take place on the basis of a warrant, and the warrant must indicate, for example, the telephone number that is the target of interception, Administration of Justice Act, 06.11.2008, Section 783(1).

<sup>94</sup> There must be certain grounds for assuming that messages to or from a suspect are conveyed by the communication in question, Administration of Justice Act, 06.11.2008., Section 781(1)(i).

<sup>95</sup> The second condition for the interception of communications is that the interference is assumed to be of decisive importance to the investigation, Administration of Justice Act, 06.11.2008, Section 781(1)(ii).

of the crime<sup>96</sup> and a proportionality principle<sup>97</sup>). However, when drones are equipped with a camera devoted to capture image for surveillance purposes, the Danish covert surveillance regime does not seem to provide an equivalent protection. Furthermore, whatever measure of surveillance has been adopted by the police, there is no notification duty to the individuals after the surveillance operation.

This lack of high-quality data protection standards covering the law enforcement operations pose some issues particularly when such surveillance measures are performed by sophisticated technology like civilian RPAS. Indeed, RPAS being generally invisible and able to capture a multitude of data thanks to their variety of payloads, there already exist high risks related to transparency, proportionality, accountability and purpose limitations when they are used by law enforcement authorities. Therefore, there is a need of high-level principles for mitigating these risks, including an effective control by an independent supervisory authority.

*Areas where current regulatory mechanisms are working well and elements of good practice*

### ***Good Practice 1. Commercial operators – A notification duty in cases of data breach***

In reality, the Danish DPA does not contain any specific obligation to inform the Agency or data subjects of a security breach. However, in practice, “the Agency has interpreted the obligation to comply with good practices of processing data as requiring a data controller to notify data subjects of any unintended publication of personal data”.<sup>98</sup> Such good practice is particularly relevant in the context of drones as we have pointed out in the Commercial operators’ scenario that drones will likely process inadvertently personal data. While we think that drones’ operators should also take preventive security measure by putting on their drone a blurring or anonymization technology, such remedial rule is also important to increase the principles of transparency and accountability. So we stress businesses to adopt preventive and remedial measure to reduce the risk of data breach and gain public trust.

### ***Good Practice 2. Commercial operators, Journalists and Private individuals - Drones equipped with a camera: The strengthening of the data protection law***

We have often emphasised the fact that RPAS equipped with a camera may be used to capture images and sounds but also for target observation and large-scale surveillance. However, the Danish DPA provides stricter rules when personal data have been processed by a video surveillance technology. We have observed that when the CCTV systems has been deployed for preventing crimes, the records can only be disclosed to the police with the explicit consent of the data subject concerned and if this disclosure is permitted by law. Furthermore, the images can only be stored for a maximum of 30 days.<sup>99</sup> In the context of RPAS this

---

<sup>96</sup> A requirement as to the nature of the crime, particularly that the investigation concerns an offence with a maximum penalty exceeding six years or contravention of Parts 12 and 13 of the Criminal Code, Administration of Justice Act, 06.11.2008., Section 781(1)(iii).

<sup>97</sup> If in view of the purpose of the interference, the importance of the case and the outrage and inconvenience that the measure is assumed to cause to the person(s) affected by it, it will constitute a disproportionate intrusion, Administration of Justice Act, 06.11.2008, Section 782.

<sup>98</sup> Linklaters, “Data Protection – Denmark”, 2014.  
<https://clientsites.linklaters.com/Clients/dataprotected/Pages/Denmark.aspx>

<sup>99</sup> L. Gras, Marianne, “The Legal Regulation of CCTV in Europe”, *Surveillance & Society*, Vol 2, Issue 2/3, 2004, pp. 216-229.

specific data protection rules applying to the visual surveillance can only be seen as an added value as it reinforces the core data principles and then, this will mitigate the risks of data protection that the most controversial use of RPAS may pose.

### **10.3 Member States preparing RPAS regulations**

#### *10.3.1 Belgium*

*Current and emerging RPAS applications not adequately covered by existing and proposed national legislation*

#### ***Problem 1. State Agencies – Lack of transparency and monitoring by the DPA***

In our study of the Belgian data protection regime, we observed that the data protection law encompasses a main exemption when processing activities relate to criminal or national security matters. Indeed, Article 3 provides that State agencies processing data for national security purposes and for judiciary and police purposes are exempted from the respect of individuals' rights including the obligation to inform the data subject.<sup>100</sup> Moreover, when they only process activities for national security purposes, they do not have to notify the DPA prior to processing. So drones used by law enforcement authorities are always exempted from informing the data subject and in processing activities related to national security, they do not have to notify the Belgian DPA.

Furthermore, as the State agencies using drones for capturing personal data in these matters will also be subject to the surveillance and criminal law, we observe the Belgian Procedure Code and we noticed that no provision requires the notification of the individuals after having undertaken a surveillance measure.

Finally, such lack of transparency when drones are used by State agencies is even increased by the invisibility of the drone and the non-identification of the operator. Consequently, there is in Belgium a real lack of transparency towards the data subject and independent monitoring by a Data Protection Authority when drones are used by State agencies.

*Areas where current regulatory mechanisms are working well and elements of good practice*

#### ***Good practice 1. Commercial operators, journalists and private individuals – FAQ on drones***

This year the Belgian DPA has issued on its website an article in which it answers to the "Frequently Asked Questions" posed on drones.<sup>101</sup> Whereas it has already been mentioned in Chapter 4 on the initiatives taken by the DPAs, some interesting elements must be highlighted.

First of all, this article describes the types of drones and payloads that are available and the purposes for which they can be used. Second, it also briefly mentions the privacy and data protection risks they can entail in relation to their characteristics. Second, it explains to

---

<sup>100</sup> Belgium Parliament, The Privacy Act, 08.12.1992 ("Belgian Privacy Act 1992"), Article 3.

<sup>101</sup> Belgian Data Protection Authority, "FAQ sur les drones", 2014, <http://www.privacycommission.be/fr/faq-themas/drones>

journalists and private individuals in which extent they are partially (journalists) or wholly (private individuals) exempted from certain provisions. Thirdly, it clarifies how certain data protection principles and CCTV rules should be understood in the context of drones. In this regards, this guidance is a “goldmine” for RPAS operators as it helps them to better understand and comply with the regulations. Among the principles explains and tailored by the DPA, we can find: data processing security, privacy by design, proportionality, purposes limitation, transparency, legitimacy, necessary, data minimisation. Fourthly, we found also recommendations to manufacturers, designers, commercial operators which go beyond the Belgian rules. For instance, it recommends that companies using drones put their logo on the drone in order to make it identifiable by the general public. Finally, it raise similar remaining implementation gaps than those we analysed the previous chapter.

***Good practice 2. Commercial operators, journalists and private individuals – The right to one’s image: the strengthening of the consent requirement (transparency)***

In Belgium like in France and Germany, it exists besides the right to privacy and the data protection law (Loi vie Privée 1992), a right to one’s image.

This right stems from the doctrine and jurisprudence surrounding the data protection law and Article 10 of the Copyright law.<sup>102</sup> The right to one’s image is the right according to which for all captures of an image of an individual and uses of such image consents of the person concerned are required. Applied to RPAS technology, it implies for drones’ operators that they must have the a) *consent of the individual concerned before capturing the image of this person but also have to re-ask for to receive b) the consent of the same individual before using/disclosure of this image.*<sup>103</sup> This right to ones’ own image provides some exceptions, for example regarding to public figures, the consents are not require neither for the capture nor for the use/disclosure whether the image of the public figure is used for information purposes (not commercial) and if the image of the public figure has been captured in the exercise of her/his public activities and then, respect her/his private life.

Firstly, this right has for benefit to strengthen, in general, the transparency principle and the data subject rights of the data protection law.

**Example 1.**

A Belgian university calls for a marketing company to advertising the new facilities. This company decides to launch a drone and film different students on the campus. However, before recording images of students and disclosing the film through television advertising, the company had to obtain the consent of each student filmed twice.

Secondly, journalists being exempted to respect individuals’ rights under the data protection law, including the right to inform the person concerned, this right to one’s image came to mitigate this exemption.

---

<sup>102</sup> Belgium Parliament, The Privacy Act, 08.12.1992 (“Belgian Privacy Act 1992”) and Belgium Parliament, Copyright law, 30.06.1994, (“La loi (LDA) relative au droit d’auteur et aux droits voisins) », Article 10.

<sup>103</sup> SPF Economie, « Le droit à l’image », 2014, [http://economie.fgov.be/fr/entreprises/propriete\\_intellectuelle/droit\\_d\\_auteur/droit\\_image/#.VDj7OPmsWZM](http://economie.fgov.be/fr/entreprises/propriete_intellectuelle/droit_d_auteur/droit_image/#.VDj7OPmsWZM)

Example 2.

After having heard that the Belgian royal family is going on holiday in the South of France, a drone is launched by a journalist for capturing photography of the Belgian Prince relaxing on the beach with the Princess. In conformity with Article 3§3b) of the data protection law, the journalist could capture and disclose the images without requiring the consent or informing the subject concerned, *in casu*, the Prince and the Princess. Under the right to image, the journalist has to receive the consent of the Prince and Princess at both times, before the capture and the use/disclosure, the images of these public figures being not captured in the framework of a public activity.

***Good Practice 3. Commercial operators - Recommendation on Direct Marketing and personal data protection***

The Belgian Data Protection Authority (*Privacy Commission*) has recently issued a recommendation in which it explains how all data protection principles should be interpreted when the processing activities have been executed for direct marketing purposes.<sup>104</sup> Furthermore, it also give some guidance to help data collectors processing data for direct marketing purposes to reduce risks related to such processing activities and better comply with the data protection principles.

For example one of the first best practices issued by the DPA that is particularly relevant for drones is the one concerning “consent”.<sup>105</sup> Although the Belgian data protection law, like the European data protection directive, provides different criteria to the data collector for making data processing legitimate (obtain consent or under the basis of a contract basis or for a legitimate aim), the Belgian Data Protection Authority strongly recommends Belgian data collectors to obtain consent of the individuals concerned through a declaration of confidentiality when they processing data for profiling.<sup>106</sup> We have seen in the previous chapters that using commercial drones for profiling activities may create some risks related to the transparency principle (non-identification of the operator and the drone). By building the data processing activities under the basis of the consent of the individual concerned, drones collectors will reduce the risks related to transparency and reinforce the data subjects’ rights.

Besides risks related to transparency, we also found that commercial drones uses could pose some implementation risks surrounding the purpose limitation principle. However, in its recommendation, the DPA gives some guidance to drones collectors on the manner they should describe their legitimate finalities. It also reminds that the sale of data processed for direct marketing purposes, constitutes in itself a first finality for which data have been processed. So drones operators cannot sell data that they have firstly processed for another purpose as they will necessarily be found incompatible.

---

<sup>104</sup> Belgian Data Protection Authority, *Recommendation on Direct Marketing and personal data protection* (CO-AR-2012-007), 02/2013 - 11/44, 2013.

<sup>105</sup> Ibid.

<sup>106</sup> Belgian Data Protection Authority, *Recommendation* 02/2013 - 11/44, op. cit., 2013.

#### ***Good practice 4. Commercial operators, State agencies - Guidance strengthening the security of processing***

As a reminder, the Belgian data protection principles include “the data security principle”. This requires the data controllers to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against all other unlawful forms of processing.

To reinforce this security principle, the Belgian Data Protection Authority provides guidance documents. Firstly, the Belgian DPA has issued a document called the *Reference Measures for the security of any personal data processing*.<sup>107</sup> This document contains a list of eleven domains of action relating to information security, for each of which any organisation keeping, processing or communicating personal data – be it a corporation, a company or a public authority – is to take. The second document consists in guidelines for information security.<sup>108</sup> These guidelines define all security finalities that organisations have to respect when they process sensitive data (personal data subject to a prior authorisation).

In Chapter 3, we highlighted the fact that RPAS technology poses some security risks that traditional surveillance technology do not. Among them, we emphasised the risk of hijacking the content of drones which has been particularly pointed out in several newspapers. We also often focused on their ability to process data inadvertently. However, these recommendations, which affords security best practice on a step-by-step approach, seems a good way to help commercial operators and state agencies to process data through the means of drones in compliance with the data protection law.

#### ***Good practice 5. State agencies – The use of RPAS equipped with a camera in public places for visual surveillance purposes: A strict restriction on the uses***

Previously, we, firstly, observed that one of the first drones’ use is the visual surveillance regardless the drones’ operator (commercial operators, journalists, State agencies, private individuals). However, we also emphasised that drones are considered by the Belgian law on surveillance camera 2007 as a mobile surveillance camera. According to the same law, we found that mobile surveillance cameras may only be used by law enforcement authorities in public places. In addition, they can only be performed in the framework of great gatherings, for non-permanent monitoring missions in a public place or in a close place accessible by the public. In other words, this means that drones mounted with a surveillance camera may only be used by police officers for monitoring great gatherings for a limited duration.

---

<sup>107</sup> Belgian Data Protection Authority, *Reference Measures for the security of any personal data processing - Version 1.0*, 2014.,  
[http://www.privacycommission.be/sites/privacycommission/files/documents/reference\\_measures\\_security\\_personal\\_data\\_processing\\_1.pdf](http://www.privacycommission.be/sites/privacycommission/files/documents/reference_measures_security_personal_data_processing_1.pdf)

<sup>108</sup> Belgian Data Protection Authority, *Lignes Directrices Pour La Sécurité De L'information De Données, À Caractère Personnel*, 2012.  
[http://www.privacycommission.be/sites/privacycommission/files/documents/lignes\\_directrices\\_securite\\_de\\_l\\_information\\_0.pdf](http://www.privacycommission.be/sites/privacycommission/files/documents/lignes_directrices_securite_de_l_information_0.pdf)

Such restriction on the use of mobile cameras supports proportionality and purpose limitation principles as it requires that the use of drones equipped of surveillance cameras is strictly limited to a specific type of operator and to certain finalities. Nevertheless, while this legal approach is particularly privacy oriented and brings high level standards, the Belgian Data Protection Authority has already highlighted that such strict limitations on the use of mobile camera will raise issues with technological developments like drones. This is the reason why legislators intends on one hand, to extend the applications for which law enforcement authorities will be able to use mobile surveillance cameras and, on the other hand, extend the use of mobile surveillance cameras to civil security services officers and inspection and monitoring services officers. While such changes will thus allow new operators to use drones on public places will allow using drones for more applications, the future visual surveillance law will still encompass strict limitations to the usage of such technology.

#### **10.4 Concluding Observations - The legal gaps remaining**

In this last section, we will summarise for each type of drones' operator our findings. However, it is noteworthy to recall that if the present chapter encompasses a comprehensive study of the adequacy of the national regimes for all types of operators, the focus of this research project is on commercial uses of drones. Therefore, for commercial operators we will not only sum up the analysis of this present chapter but also we will interpret them in accordance to different scenarios examined in Chapters 7 and 8.

Before starting with the concluding observations, it is important to remember that the remaining implementation gaps figuring in the European privacy and data protection regimes studied in the previous chapter which also exist in the national data protection law of the Member States have not been repeated with a view of avoiding duplication.

##### *10.4.1 Commercial operators*

Firstly, this comparative analysis shows that all RPAS applications carried out by commercial operators fall under the national data protection regimes. Therefore, regardless the type of processing activity drones' operators perform, commercial drones' operators have to respect the obligations and rights of their national data protection law since they process personal data. Secondly, this study points out that there are two main remaining legal gaps. Above all, we should emphasise that by using the wording "commercial operators", we mean all operators using RPAS for professional uses. Therefore, this includes commercial operators as well as any other corporate or self-employed professionals like farmers, except journalists.

The first legal gap regards to the fact that the national data protection laws which apply to commercial operators do not address adequately the **high risks surrounding the security of processing** that RPAS pose due to its atypical features. As a reminder, we have seen in the first deliverable that drones are likely to process personal data accidentally, they can be easily hacked by another RPAS, they can process massive amount of different data in a same flight and while they automated process data and there is "no possibility of changing the processing environment when in the air".<sup>109</sup> By inadequate standards, we firstly refer to the fact that in some Member States the prior checking duty operated by DPAs when they face risky

---

<sup>109</sup> Bláhová, Jitka, "Data protection implications of the use of RPAS and recommendations", *Policy Recommendations for the Civil Use of RPAS*, European Commission workshop, Directorate General Enterprise, 29 March 2014.

processing operations is nonexistent. Furthermore, we should also mention that there is no clarification of what type of “organizational and technological security measures” data collectors should undertake. We also observed that national data protection laws do not have a duty of notification to the DPA and to the data subject in cases of accidental processing of data or any other data breaches. Consequently, like we observed at the European level, national data protection regimes which apply to the processing of personal data through the means of commercial drones **do not provide sufficient preventive security and remedial safeguards** for preventing the security risks inherent to the RPAS technology.

*Scenario 1. Commercial operators: Monitoring infrastructure - United Kingdom DPA 1998*

In the monitoring infrastructure scenario, we have seen that commercial operators by flying a drone for inspecting an infrastructure in a rural location or residential area will likely inadvertently capture footages of individuals, cars and houses. So we highlighted that such scenario might result in the accidental collection of personal data and misuses related to their disclosure: high risks for the individuals’ rights to privacy and data protection (risks of transparency, voyeurism, accountability, data minimization, proportionality, etc. - for a full description, see Chapter 8. Privacy, data protection and ethics in RPAS scenarios).

*Does the UK data protection law afford preventive and remedial security measure to adequately address such risks?*

The UK DPA does not impose rules on RPAS designers and manufacturers. It requires that drones collector adopt “organizational and technical measures” for preventing risks related to the security of processing but no guidance explains what they should understand by “organizational and technical measures”. Furthermore, there are neither prior-checking mechanism performed by the ICO when collectors exercise risky processing activities, nor a notification duty after a data breach (accidental processing and disclosure). Consequently, due to this lack of preventive and remedial security, risks will remain present. Therefore, the UK data protection law does not address adequately the drone issues related to such commercial uses.

The second legal gap figuring in the national laws concerns **the lack of tailored privacy and data protection standards applying to commercial drones equipped with a visual payload in public places**. In the first part of this chapter we have firstly seen that commercial RPAS pose the very high privacy and data protection risks when they are mounted with visual payloads. This is related, on one hand, to its **unique abilities to monitor people** from everywhere, to track people and objects, to lead target observation as well as large-scale surveillance and on the other hand, to the wide range of sophisticated camera with which they can be mounted. Second, we analysed that the data protection law applies to the use of RPAS by commercial operators when they are mounted with a recording or non-recording visual device (video transmission directly to a screen of the operator) but does not address the specific privacy risks related to such use like chilling effect. Besides the data protection law, we have noticed the presence of a vast quantity of CCTV regulations in the Member States. These latter have been issued in order tackle the specific privacy and data protection challenges posed by the CCTV systems. They encompass same standards than those figuring in the data protection law but these latter are tailored to the CCTV technology and reinforced by additional safeguards. For example, we can find that CCTV systems users need an authorisation of installation and post pictogram to comply with the transparency and

accountability principles. We thought that these latter could apply to the RPAS technology but, in reality, these CCTV regulations are fragmented and there is a lack of harmonisation between the Member States. Moreover, it is not so clear if they are adapted to RPAS mounted with camera as most of them are specific to static cameras (except Belgium). The approach is also divergent from a Member States to another; certain issued a general CCTV regulation while others have adopted specific sectorial CCTV laws. Furthermore, we remarked that the use of video surveillance camera in public places is generally prohibited to private entities (strictly reserved to public authorities). So Member States have seldom created an obstacle for visual surveillance technology by adopting such rules. Consequently, we think that **such CCTV regulations are not well tailored to apply to the use of commercial RPAS equipped with a visual photography payload in public places.**

#### Example 2. Commercial operators – Belgium

A professional operator hired by a NGO uses a drone equipped with a visual surveillance camera to monitor people in a free festival organized by the NGO for an awareness campaign. The film is wirelessly online transmitted to screens of the organisers and to screens hold by security agents hired for the event. After the event, the recordings are stored in the archives of the NGO and the professional operator. Such commercial use of drone may pose high risks surrounding privacy and data protection as personal data of citizens have been collected and stored (transparency and visibility, accountability and voyeurism, function creep, proportionality, etc.).

*Does Belgian CCTV law afford an adequate regime for addressing such concerns?*

In Belgium, the current CCTV regulation provides that mobile camera in public places and places accessible to citizens can only be used by law enforcement authorities in great gatherings for a short period. **Consequently, if such CCTV law applies to drones as well, the usage of a RPAS mounted with a camera in public places is prohibited in Belgium. Such usage restriction seems not adapted and unrealistic as in another Member States like UK, drones equipped with a surveillance camera are allowed for commercial operators.**

#### 10.4.2 Journalists

Regarding journalists, we have observed in the first part of this deliverable that they use drones for capturing information to disclose to the public. However, by doing so they are also likely to pose high risks surrounding privacy, data protection and ethics for individuals. Second, we examined that there is an exemption for the processing of personal data for journalistic activities in the European and national data protection regimes.

Having not been harmonised at the European level, national data protection laws **hold different approaches to the concept of “journalist”**. Therefore, from a Member States to another, the exemption figuring in the data protection law will not apply to the same processing activities operated through the means of drones. Are Youtubers, citizens-paparazzi journalists? Do they fall under the exemption and then do not have to respect the individuals’ rights? All these questions not harmoniously answered pose some concerns that we have already largely discussed in the analysis of the adequacy of European legal framework. Therefore, we refer the reader to our previous chapter for more detailed concluding observations.

### 10.4.3 State agencies

In the first part of this deliverable, we have seen that State agencies will use mostly drones for tracking a person or an object or for capturing personal data of individuals in the context of surveillance missions. They could also use them for other regulatory enforcement applications like monitoring a public event. Furthermore, we also examined that State agencies are likely to require access to personal information previously captured by a drone in the framework of investigations. State agencies are often criticised for these controversial usages and we have seen in our risks analysis that they are likely to engender high privacy, data protection and ethical risks including chilling effect, mission creep, transparency, accountability, visibility, proportionality, purpose limitations, etc. (for a more detailed overview see Chapter 8. Privacy, data protection and ethics in RPAS scenarios). Second, we observed that they are subject to two different regimes at the national level, the national data protection law since they process personal data and the surveillance laws of the law enforcement sector (CCTV regulations, Telecommunication laws and Criminal Procedure Code). However, this chapter argues that neither regime adequately addresses the above-mentioned risks.

The first gap concerned the fact that Member States data protection law **exempts the processing of personal data carried out by State agencies in security and criminal matters from almost all data protection provisions**. These exemptions includes, among other, articles related to the individuals' rights, the core data protection principles and even in some Member States the notification to the DPA and the prior checking by the DPA. While the application of specific data protection rules to the particular law enforcement sector are needed, as they sometimes have to covertly collect secret data, the exemptions figuring in the national regime are too broad and provide **blanket exemption** (not given on a case-by-case basis). Moreover, the fact that certain provisions fall under the **exemption is unjustified**, for instance the duty to notify the DPA and the prior-checking mechanism. Consequently, data protection risks raised by the RPAS when they are used by State agencies for processing personal data in relation to national security or criminal area will not be adequately mitigate by national data protection law.

The second gap concerns the fact that in general the current surveillance regimes in the Member States have not been updated and so do not address the challenges and risks raised when State agencies use sophisticated surveillance technology like drones. **Surveillance regimes are fragmented** in a multitude of specific sub-sectorial regulations, they are **not harmonised** between the Member States, the regulations ordinary **only focus on the interception of communications and the capture of images of individuals and objects**. What about geo-localisation data, biometric data, the detection of behavior, etc.? This lack of explicit laws authorising and legitimising such technologies and defining the scope of their use means that the impacts on individuals are not foreseen in their application.<sup>110</sup> Furthermore, the provisions are broadly conceived and **do not provide sufficient privacy safeguards**. For instance, in Germany and Sweden, it is possible for certain State agencies to intercept communications without warrant from a judicial power. In the majority of Member States, they are **no transparency obligations** after a measure of surveillance and **no effective control by an independent supervisory authority**. Consequently, individuals' right and privacy and data protection standards risk to be often putted aside when State agencies use drones in surveillance missions.

---

<sup>110</sup> Groupe Européen d'Ethique des Sciences et des Nouvelles Technologies, Avis 28 sur l'éthique des technologies de sécurité et de surveillance, Brussels, 20.05.2014, p. 44.

A third legal gap concerns **the lack of high-level standards in the national regime applying when in the context of an investigation State agencies request to access to personal data which have been initially captured by drones**. Indeed, it is important to remember that in certain cases State agencies can access and conserve personal data initially processed by Telecommunication providers since the adoption and implementation of the European Data Retention Directive. In addition, other national rules allow to State agencies to access and to use personal data in criminal investigations which had been previously collected by commercial or private individuals for other purposes. Nevertheless, we have observed that such rules have different duration of retention from a Member States to another and do not encompass sufficient safeguards for the individuals concerned (no obligation to notify the individual after the judicial investigation ended). Our vision seems in a certain way also shared by the European Court of Justice, which recently issued a decision in which it declares that the European Data Retention Directive is invalid for incompatibility with the primary European law.<sup>111</sup>

#### *10.4.4 Private individuals (including recreational and private uses)*

Like at the European level, private individuals who operate RPAS for personal use are **not covered by the national data protection law**. Therefore, when private individuals will use a drone processing data for household, recreational (including hobbyists) or personal uses, no regulation applies. However, we have seen that unlike at the EU level, Member States encompass some privacy-oriented regulations which allow to address certain risks that RPAS private users might raise.

In Civil law countries, we found that criminal and civil actions for property violations and harassments may have deterrent effects on voyeurs. We also observed that the right to ones' own image applies to private individuals operators. In common law countries, particular common law and statutory torts may represent constraints on the use of drones. For example, in UK, "the common law's protection of privacy has never been direct, at least in the sense of privacy itself being a justiciable right. Instead, it has historically been protected by one of two means: i) the occupation of property; and ii) the law governing confidential information. In the first case, the common law provided a range of protections against intrusion, whether by way of the criminal law or such torts as trespass and nuisance".<sup>112</sup> Consequently, such rules will mitigate and reduce risks related to the use of drones by private individuals.

These Concluding Observations will help us to examine what kind of regulations should be adopted to address the remaining gaps (hard law, soft law, European level, national level) and then suggest policy recommendations for each stakeholder involved with the RPAS technology.

#### *10.4.5 Concluding Observations*

Besides these remaining gaps, we also observed that Member States encompass some elements of good practices that might mitigate certain risks posed by drones. Some of them will also certainly permit several remaining risks pointed out above to be reduced due to the current legal gaps in the national regimes. In that respect, this present analysis of national

---

<sup>111</sup> European Court of Justice, Judgment of the 8th April 2014, Joined Cases C-293/12 and C-594/12.

<sup>112</sup> Justice, *Report on Freedom from Suspicion - Surveillance Reform for a Digital Age*, London, 2011, <http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf>

elements of good practice will be used in the next chapter to set up a list of legislative initiatives and soft law measures which should be adopted to mitigate the risks posed by RPAS. Additionally, they will also help us to suggest policy recommendation in Chapter 13.

## **11 COMPLEMENTARY MEASURES TO ASSIST IN ADDRESSING PRIVACY, DATA PROTECTION AND ETHICAL ISSUES**

### **11.1 Introduction and overview**

In the previous chapters, we observed that the European and national privacy and data protection frameworks are largely adequately address the RPAS technology, especially for commercial operators, and most remaining gaps will be covered by the proposed General Data Protection Regulation. Additionally, we have pointed out implementation difficulties for data collectors and individuals to exercise their obligation and rights stemming from the data protection legislation. However, the analysis of the adequacy of the national regimes in Chapter 10 allows us to identify several good elements of regulatory instruments of the Member States and good practices that may assist in mitigating these gaps.

Consequently, the following sections focus on four main areas to highlight which policy instruments should be envisaged by RPAS stakeholders to rectify the shortcomings of the current regimes. To address the tension between the privacy and the RPAS, we believe that the four following solutions should be envisaged:

- Legislative solutions
- Technological solutions
- Voluntary solutions – self regulation governance
- Social solutions (education and awareness)

This chapter will discuss the first three solutions and the final solution will be addressed in Chapter 13. We begin our analysis at section with 11.2, which addresses *legislative solutions*. Section 11.3 then examines certain *soft-law instruments* that involve both technological solutions and voluntary solutions.

### **11.2 Legislative solutions**

Enacting hard law is indispensable in achieving harmonised regulation for the sophisticated technological capabilities of drones, when compared with soft law measures enforced by states. However, we have seen that traditional regulations also pose challenges. Industry experts suggest that legislative intervention can have the effect of delaying or stifling the deployment of the drone industry.<sup>1</sup> In addition, as we have seen with the Data Protection Directive, neutral technological norms are often broad, vague and difficult to operationalise.<sup>2</sup> Therefore, their notions like “journalistic purposes” result in many interpretations. This is why we will make recommendations for legislative solutions, rather focussing on soft law measures.

---

<sup>1</sup> Koebler, Jason, “Drone Industry: Privacy ‘Distractions’ Could Have Major Economic Impacts”, *U.S. News & World Rep*, 2013. <http://www.usnews.com/news/articles/2013/03/13/drone-industry-privacy-distractions-could-have-major-economic-impacts>

<sup>2</sup> Groupe Européen d’Ethique des Sciences et des Nouvelles Technologies, Avis 28 sur l’éthique des technologies de sécurité et de surveillance, Brussels, 20.05.2014, p. 59.

### 11.2.1 Commercial operators

#### *At the European Union level*

To rectify the shortcomings of the current Directive 95/46/EC in relation to **the lack of preventive and remedial security measures and to reduce its implementation concerns, we recommend the European Union to adopt the Parliament Proposal of the General Data Protection Regulation**<sup>3</sup> (hereafter, the GDPR).

Firstly, we strongly believe that the data processing security risks related to the commercial use of RPAS, such as the accidental collection of personal data or the processing of massive amount of non-necessary personal information, could be mitigated through the introduction of the following new elements of the Draft GDPR:

- The clarification of the data minimization principle<sup>4</sup>
- The Data Protection by Design and Data Protection by Default (DPbD) approach<sup>5</sup>
- The duty to conduct a Data Protection Impact Assessment<sup>6</sup>
- The duty to notify a data breach<sup>7</sup>

To avoid repetition, we refer the reader to our discussion of the data minimisation principle and the duty to notify a data breach at Chapter 9 of this deliverable. Here, we focus on technological solutions of the PbD approach and the duty to conduct a Data Protection Impact Assessment.

Second, we welcome the introduction of an *accountability principle* and two new individuals' rights, the *right to be forgotten* and the *right to object to data processing for profiling activities*, as they will reduce the implementation concerns inherent to the RPAS technology that commercial operators and data subjects face.

#### a) The accountability principle

In our analysis of the adequacy of the current data protection law to the RPAS technology, we emphasised the difficulties in achieving effective implementation. We also pointed out that the issues of implementing the “theory” into practice is partly due to the technology neutral character of the Directive. There is, therefore, a need to tailor the legal requirements to the features of the technology and risks posed with self-regulation. In addition, “to encourage data protection in practice”, Article 29 WP also calls for the adoption of additional mechanisms in the EU data protection legal framework itself through the adoption of a general accountability principle.<sup>8</sup>

---

<sup>3</sup> European Parliament on the legislative resolution on the 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 (GDPR) (COM(2012)0011, 12 March 2014.

<sup>4</sup> Ibid., Article 5.

<sup>5</sup> European Parliament, op. cit., 2014, Article 23.

<sup>6</sup> Ibid., Article 33.

<sup>7</sup> European Parliament, op.cit., 2014, Article 31 and Article 32.

<sup>8</sup> Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, Brussels, 13 July 2010.

In the data protection area, the term “accountability” means “*an obligation to report and explain, combined with principles of transparency and traceability, with a view to identify and document the measures implemented to comply with data privacy law requirements. It also implies an obligation for the data controller to assume liability and warrant a result, namely the efficacy of the data protection and the verifiability of the measures taken to this end*”.<sup>9</sup> In fact, Article 22 of the proposed GDPR introduces such a principle that requires “data controllers 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 the data privacy legislation”.<sup>10</sup> Thus, the burden of proof has been reversed and under the GDPR, the responsibility to prove that the data protection law has been respected is borne by the RPAS controller who must be “able at any time to demonstrate compliance with data protection provisions to data subjects, to the general public and to supervisory authorities”.<sup>11</sup> In its Opinion on the Principle of Accountability, the Article 29 Working Party explains that the accountability principle engenders a twofold obligation for the controller, which must:

- “Put in place measures which would – under normal circumstances – guarantee that data protection rules are adhered to in the context of processing operations and
- Have documentation ready which proves to data subjects and to supervisory authorities what measures have been taken to achieve adherence to the data protection rules”<sup>12</sup>.

In the context of RPAS, such a principle is very relevant as we have seen that in many times the data controller could be tempted to put aside the data protection requirements when the data subjects are not aware of the collection. Hence, a RPAS company is responsible for setting up the mechanisms for making individuals aware that their data have been processed either by creating a web portal or by any other means. Furthermore, companies must be in a position to show a DPA that they have implemented all data protection law requirements in their processing activities when utilising drones in that capacity. For instance, we also envisage that before flying a drone a company will have to record that they carried out a PIA to a CAA agent. The effect of such measures is that RPAS data collectors can no longer hide behind the excuse that the requirements are too difficult to implement.

- b) New individuals’ rights: the right to be forgotten and the right to object to data processing for profiling activities

It is unequivocal that the GDPR proposal strengthens the position of the data subjects. It has maintained the existing rights, reinforces the obligation of transparency on data controllers, includes procedures to assist the data subjects in the exercise of their rights,<sup>13</sup> and it includes new rights such as the right to be forgotten and to erasure and the right to object to data processing for profiling activities.

---

<sup>9</sup> Bensoussan, Alain, “Accountability and Protection of Personal Data”, 2014.  
<http://www.globalprivacybook.com/blog-european-union/306-accountability-and-protection-of-personal-data>

<sup>10</sup> European Parliament, op. cit., 2014, Article 22; Bensoussan, op. cit, 2014.

<sup>11</sup> European Union Agency for Fundamental Human Rights (FRA), *Handbook on European data protection law*, the European Union Agency for Fundamental Rights and the Council of Europe, Belgium, 2014.

<sup>12</sup> Article 29 Data Protection Working Party, op. cit., 2010.

<sup>13</sup> European Parliament, op. cit., 2014, Articles 11 and 12.

Firstly, the right to be forgotten and to erasure is defined as “*the right of individuals to have their data no longer processed and deleted when they are no longer needed for legitimate purposes*”.<sup>14</sup> So this right refers to, and strengthens, the retention, necessary and lawfulness principles. In the context of RPAS technology, we have seen that not only personal data are often inadvertently processed but also that most of the time, data subjects are not aware that their personal data have been processed. However, with the introduction of this new right, data subjects will not only be able to ask for suppression when the data has been accidentally collected but also to require the erasure when the data is no longer used by the data collector for legitimate purposes. This self-determination right<sup>15</sup> adds real value for individuals as it will allow them to suppress their existence in databases and will reduce the risks of data breach. For instance, in the scenario we studied on new services, we have seen that the roof insulation company has collected an important amount of data by processing images of roofs in residential areas. Some of them will be combined with addresses and used for sending a tailored discount offer. By enforcing his/her right to be forgotten and erasure, data subjects will oblige the company to suppress all data related to him/her once the campaign offer (purpose of the processing) is over. By exercising such right they also ensure that their personal data are not subsequently and illegally sold and re-used by another company, such as an insurance company willing to increase its rates.

Second, we analysed in the first part of this deliverable that because RPAS technology is capable of being fitted with multiple payloads, it is a perfect tool for profiling activities. However, we also highlighted that profiling activities that create abstract profiles increase the already existing data protection risks related to drones processing, as well as producing new privacy risks, including discrimination, dehumanisation, etc. Therefore, we support the introduction of additional safeguards related to profiling activities added in the GDPR. Further, RPAS operators processing personal data for profiling activities must respect these new requirements like conducting a PIA<sup>16</sup> and respect additional safeguards. Furthermore, data subjects under certain legal circumstances will have the right to not be subject or block profiling activities<sup>17</sup>. Consequently, the GDPR will reinforce the security of processing when companies used drones for creating profiles but it will also permit to individuals to have a prior control in the processing of their personal data.

#### *At the national level*

At a national level, we highlighted that the current national CCTV regulations are not well adapted to adequately govern the use of drones equipped with a visual surveillance camera used by commercial operators. Second, we emphasised that there is a lack of tailored privacy standards which would address the privacy and ethical risks related to the use of drones equipped with a visual payload in public places for other purposes than surveillance.

**Therefore, we firstly recommend that the Member States clarify the extent to which their CCTV regulations apply to the use of drones mounted with a visual surveillance camera in a commercial context. In addition, we encourage them to update the current CCTV**

---

<sup>14</sup> European Commission, A comprehensive approach on personal data protection in the European Union, Communication From the Commission to the European Parliament, the Council, the Economic And Social Committee and the Committee of the Regions, COM(2010) 609 final, 04.11.2010., p. 8.

<sup>15</sup> Costa, Luiz and Yves, Poulet, “Privacy and the regulation of 2012”, *Computer Law & Security Review*, Vol. 28, 2012, p. 256.

<sup>16</sup> European Parliament, op. cit., 2014, Article 32a and Article 33.

<sup>17</sup> Ibid., Article 19 and 20.

**regulations to the challenges raised by the new intrusive technologies in order make sure that private entities using drones for surveillance purposes are subject to high-level of privacy and data protection standards.**

Second, to address the privacy and ethical risks that commercial operators pose by using drones equipped with panoptic payload and other such sophisticated technology, **we encourage Member States to adopt privacy and ethical standards tailored to the RPAS technology. In order to achieve harmonisation in this area, specific rules should be based on an instrument erected at the European level like a European Code of Conduct sets up by the Article 29 Working Party.**

### *11.2.2 State agencies*

#### *At the European Union level*

In Chapter 5, we observed that personal data processing activities carried out by Member State agencies using drones are not covered by the current European data protection framework. Additionally, we observed that the current Framework Decision 977/2008/JAI does not adequately address the processing risks raised by the use of State drones when data are processed in a cross border context. However, the Draft Police and Criminal Justice Data Protection Directive extends its scope to the domestic processing. Furthermore, it will improve the protective level of the current standards as it introduces new preventive security measures like PIAs and PbD. Nevertheless, we still notice some broad exemptions related to the individuals rights to adequately address the threats posed by new technologies like RPAS. For instance, we had emphasized in Chapter 5 that the obligation to inform individuals, essential to allow individuals to exercise their rights particularly in the context of RPAS, is subject to too broad derogations clause. Consequently, **we recommend the European Union to revise the Proposed Directive in the view to better address the challenges posed by atypical intrusive surveillance technology like RPAS<sup>18</sup>.**

#### *At the national level*

At the Member States level, we have firstly seen that the current data protection legislation encompass too many exemption clause and too few processing security measure when drones are used by State agencies to process personal information in the context of national security, defence and criminal investigation. In this regard, **we encourage Member States to revise their current data protection law by limiting the derogations and by introducing an obligation for State agencies drones' operators to set up preventive and remedial security measure, similar to obligations imposed on commercial operators.** For instance, such measures could include conducting a PIA and by ensuring the DPbD approach.

Second, in many Member States we observed that existing surveillance legislation have not been updated to the new digital era. Thus, they are not adequate to address the risks posed by State agencies using RPAS in surveillance missions. In this regard, **we urge Member States to enact or revise their legislation in the area of surveillance to make them adequate to the usage of the RPAS technology.** In this respect, we promote the idea that **Member States**

---

<sup>18</sup> Groupe Européen d'Ethique des Sciences et des Nouvelles Technologies, Avis 28 sur l'éthique des technologies de sécurité et de surveillance, Brussels, 20 May 2014 and Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 10.04.2014.

should enact a special law in which the following principles should be tailored to the features and risks inherent to the RPAS technology:

- **Proportionality principle;**
- **Purpose limitation principle;**
- **Necessary principle;**
- **Transparency principle.**<sup>19</sup>

Special consideration should be given to reinforcing the transparency principle. In this regard, we suggest that Member States create **a duty to notify individuals of the surveillance measures** performed by drones. If such information could jeopardize the objective of the surveillance mission, the notification must at least be performed within a reasonable time after the surveillance operation. Furthermore, an **obligation to balance the interests at stake, privacy vs. security, and an effective control by an independent supervisory authority before each operation** should be incorporated (the check and balance principle). Consideration should be given to introduce as general rule that State agencies must obtain **a court order** prior to launch an RPAS<sup>20</sup>. This would refer the issue to judicial power to check that all principles and requirements have been met.

Thirdly, given the unreliability of the RPAS technology, we think that **Member States should adopt a rule that prevents judicial authorities and public administrative authorities to adopt decisions based on personal data that have been initially processed by a drone**. Finally, we recall to the Member States to take in account the recent decision issued by the ECJ that declares the retention directive invalid<sup>21</sup>. In that respect, **we urge Member States to enact new strict legislation, which regulate in which extent State agencies may request to RPAS processors to access to personal data processed by drones**. Same high-level protective standards including proportionality, necessary, transparency principles and independent control need to be set up.

### 11.2.3 Journalists

#### *At the European Union level and national level*

At both level, we criticised the lack of clear and harmonised rules explaining to RPAS operators which kind of journalists fall under the data protection exemption enshrined in the national data protection legislations and the European Directive. Furthermore, the broad concept of “necessary” prevents a journalist using RPAS to understand when they are covered by the exemption. To rectify these shortcomings, **the member States should make clear in their legislation that this is not a blanket exemption, and that it only applies to balance the interests of privacy and freedom of expression. The application of this exemption should be reevaluated before each RPAS operation (on a case-by-case basis).**

---

<sup>19</sup> Groupe Européen d’Ethique des Sciences et des Nouvelles Technologies, op. cit., 2014 and Article 29 Data Protection Working Party, op. cit., 2014.

<sup>20</sup> International Working Group on Data Protection in Telecommunications, Working Paper on Privacy and Aerial Surveillance, Berlin, 2-3 September 2013; Stanley, Jay and Catherine Crump, *Report on Protecting Privacy From Aerial Surveillance - Recommendations for Government Use of Drone Aircraft*, ACLU, New-York, 2011. It is noteworthy that in the United States, many States have already enacted a State Law requiring State agencies to obtain a warrant before using a drone.

<sup>21</sup> European Court of Justice, Judgment of the 8th April 2014, Joined Cases C-293/12 and C-594/12.

#### 11.2.4 Private individuals

To reduce the risks related to the use of model RPAS for recreational and private purposes, **Member States should introduce privacy-oriented rules in their safety airspace regulations. This would specifically address the use of RPAS by hobbyists who could be directed to fly a model aircraft inside specific boundaries (an area away from the residential buildings and cities).**

### 11.3 Soft law measures: technological and voluntary solutions

Soft-law is “*the term applied to EU measures, such as guidelines, recommendations, declarations and opinions, which – in contrast to regulations, directives, and decisions – are not binding on those to whom they are addressed*”. Contrary to state law, these alternative instruments have the advantage to be flexible and tailored to the interests of industries and the citizens. Whereas they are not accompanied by penalties, which fall within the jurisdiction stipulated by traditional regulations. Soft law measures may also include a clause having deterrent effects and therefore change the behaviour of actors concerned.

By being technologically neutral, privacy and data protection legislation can be vague, broad and difficult to understand and thus, difficult to implement in practice. This is the reason why soft law measures have often been chosen to regulate “the tension between privacy and (new) technology”<sup>22</sup>, as a complement to State law. In the context of this study we will firstly examine three technological solutions, including the Privacy by Design (PbD) approach, the Privacy Impact Assessment (PIAs); and the Surveillance Impact Assessments (SIAs). Second, the four following voluntary solutions will be discussed, including: the Privacy Audit; the Self-Regulatory measures; the Privacy Certification scheme; and the Usage Restrictions. For each type of soft-law measure we will first, define the concept including an analysis of this measure within the Draft of the GDPR. Second, we will examine whether they have already been implemented and proved to be a “good practice” in other data processing/technology context. Thirdly, we will assess whether in the context of RPAS applications and in regard to the risks they raise, the soft law instrument studied should be seen as a “good practice”<sup>23</sup> and encouraged to be adopted. Finally, we will attempt to give some examples of their application in relation to the scenarios studied.

#### 11.3.1 Technological solution - Privacy by Design

##### *Concept*

Privacy by Design (PbD) “*is an approach developed by Ann Cavoukian, the Privacy Commissioner of Ontario, which consists to protect privacy by embedding it into the design specifications of technologies, business practices, and networked infrastructures, as default,*

---

<sup>22</sup> The European Group On Ethics In Science And New Technologies, *Opinion No. 28 - Ethics Of Security And Surveillance Technologies*, Brussels, 20.05.2014, p. 59.

<sup>23</sup> A “good practice” under the UK Data Protection Act is defined “as practices for processing personal data which appear to be desirable”.

*right from the outset*".<sup>24</sup> Technology that anonymises data, blurs individuals, objects and images, or that mask data are part of the PbD measures.

As explained by Cavoukian, this approach has the following main objectives "for individuals, ensuring privacy and gaining personal control over one's information and, for organizations, a sustainable competitive advantage". Notably, the "Best Practice Institute" has already recognized such an approach as a "Best Practice". In addition, the International Data Protection and Privacy Commissioners described it as "an essential component of fundamental privacy protection" at their annual conference in 2010.<sup>25</sup>

#### *Implementation – Article 23 and 30 of the GDPR*

We can already observe such an approach in third country privacy instruments, including those of the Canadian, Australian, US and UK governments.<sup>26</sup> At the European Union level, we observed that the current data protection law does not embrace a PbD approach, but this should be amended as part of ongoing reforms. Indeed, both proposed new data protection instruments include Data Protection by Design principle.<sup>27</sup> Such new incorporation would imply for data collectors to ensure all principles and rights stemming from the GDPR and the Directive by Design. In addition, we observe Security by Design and Security by Default approaches, as Article 30 requires data collector to set up security measures "in taking account of developments in technology and solutions for privacy by design and data protection by default".<sup>28</sup>

By being embedded in the technology itself, PbD involves designers, developers and manufacturers. The objective is thus to transfer a part of the responsibility currently wholly borne by the data collectors onto those who design technical specifications and those who actually build or implement applications or operating systems. However, the draft of the GDPR seems to target users of the relevant data processing techniques and technologies as the bearers of liability.<sup>29</sup> Nevertheless, the underlying "idea seems to be that by making data controllers responsible (and liable), they will force developers to come up with the right types of technologies".<sup>30</sup> Furthermore, we remarked that the Proposal speaks about "Data Protection by Design" rather "Privacy by Design". Therefore, we can wonder whether by adopting such wording the European Commission had for aim to "only target privacy insofar as implied in data protection".<sup>31</sup> Whereas this is view shared by several scholars, the Parliament seems to

---

<sup>24</sup> Ann Cavoukian, *Operationalising Privacy by Design: A Guide to Implementing Strong Privacy Practices*, Privacy Commissioner of Ontario, Ontario, 2013.

<http://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf>

<sup>25</sup> European Parliament, op. cit., 2014, Recitals 75 &76 and Article 30.

<sup>26</sup> For the UK PbD approach, see "United Kingdom - Good practices" in Chapter 10.

<sup>27</sup> European Parliament, op. cit., 2014, Article 23; European Commission, Proposal for a Directive Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Article 19.

<sup>28</sup> Hildebrandt, Mireille and Laura, Tielemans, "Data protection by design and technology neutral law", *Computer Law & Security Review*, Vol. 29, 2013, p. 517.

<sup>29</sup> Ibid.

<sup>30</sup> Hildebrandt, Mireille and Laura, Tielemans, op. cit., 2013, p.517.

<sup>31</sup> De Hert, P and S. Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power', in Erik Claes, Antony Duff and S. Gutwirth (Eds.), *Privacy and the Criminal Law*, Oxford Intersentia, Antwerpen, 2006 and Hildebrandt, Mireille and Laura, Tielemans, op. cit., 2013, p. 517.

have put an end to such concern by introducing the “Privacy by Design” expression at the Recital 75.<sup>32</sup>

#### *Privacy by default and privacy by design measures in diverse technologic areas*

Privacy by Design measures have already been set up for different technologies like Smart Grids, Biometric systems, RFID technologies, visual surveillance technologies (CCTV systems), geo-localisation devices, etc<sup>33</sup>.

As Cavoukian explains, there are no “one-size-fits-all” responses for all development of technologies.<sup>34</sup> Each technology process different type of data and for each of them, different PbD measures must be adopted. This is particularly emphasised by the publication *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices* in which Cavoukian details for multiple technology applications which PbD measure has been adopted by public and private entities in their activities. For example, for Face Recognition Systems Cavoukian states that “to avoid collecting, transmitting or retaining any identity information about viewers, the technology uses pattern detection (not recognition) algorithms to scan real time video feeds, looking for patterns that match the software’s understanding of faces. Furthermore, the data is logged and the video destroyed on the fly – with nothing in the process recognizing the individuals who passed by in front of the sensors”.<sup>35</sup>

Besides this sophisticated technology, technology developers and data collectors can also use simpler measures to ensure the PbD principles. For instance, by minimising the collection of data at the outset to only what is strictly necessary or by adopting data masking or blurring images technologies which do not allow to identify individuals.<sup>36</sup> Anonymisation and pseudonymisation processes have also been identified in this regard, particularly in the context of remote surveillance systems and biometric systems uses, to avoid the disclosure or re-use of sensitive data. In biometric technology applications, some data collectors have adopted encryption systems. Encryption “is a method for securing communications from unauthorised eavesdropping. Therefore, this cryptographic algorithm ensures that biometric data are not connected to any personal data, by default”.<sup>37</sup>

#### *Privacy by default and privacy by design measures in the context of drone technology*

Does the PbD approach fit with the RPAS technology? As discussed earlier in the context of security processing, PbD measures have for benefit to be preventive, proactive. In the context of drones, this is essential, as we have seen in the *Infrastructure Monitoring Scenario* that, on

---

<sup>32</sup> European Parliament, op. cit., 2012, Recital 75.

<sup>33</sup> Ann Cavoukian, Privacy Commissioner of Ontario and founder of the PbD approach, has already applied the PbD to the following application areas: CCTV/Surveillance Cameras in Mass Transit Systems; Biometrics Used in Casinos and Gaming Facilities; Smart Meters and the Smart Grid; Mobile Devices & Communications; Near Field communications (NFC); RFIDs and Sensor Technologies; Redesigning IP Geolocation Data; Remote Home Health Care; Big Data and Data Analytics.

<sup>34</sup> Cavoukian, Ann, op. cit., 2013.

<sup>35</sup> Ibid.

<sup>36</sup> ‘Security Breaches’ Administrator, ”Implementation Of Privacy By Design And Technical And Organizational Security Measures: The Data Masking Solution”, *The Blog Security Breach*, 2012. [http://blog.security-breaches.com/2012/06/26/implementation\\_of\\_privacy\\_by\\_design\\_and\\_technical\\_and\\_organizational\\_security\\_measures\\_the\\_data\\_masking\\_solution/](http://blog.security-breaches.com/2012/06/26/implementation_of_privacy_by_design_and_technical_and_organizational_security_measures_the_data_masking_solution/)

<sup>37</sup> Ibid.; Cavoukian, Ann, op. cit., 2013.

one hand, drones are likely to process non-necessary data and, on the other hand, they are invisible and their operator is often non-identifiable. Therefore, they pose high security risks in relation to the data minimization principle and raise transparency implementation concerns. However, by adopting a PbD technology such as camera with image blurring, the RPAS operators prevent risks from the outset and then, avoid the economic and administrative burden to inform individuals about the collection of personal data that it does not need.

Among other parties interested in implementing the PbD approach for regulating RPAS include, the founder of the PbD, Ann Cavoukian, the Belgian data protection authority (Privacy Commission) and the Article 29 Working Party have issued publications on regulating RPAS technology by PbD. In its report “*Privacy and Drones: Unmanned Aerial Vehicles*”<sup>38</sup>, and Cavoukian expressly claims that RPAS organizations “should take a proactive PbD approach to developing and operating a UAV program which respects privacy”<sup>39</sup>. Furthermore, she details for each of the seven principles of the PbD approach how they should be understood and implemented in the context of drones. For instance, concerning the “Privacy is embedded into the Design Principle”, she recommends that **Commercial operators using RPAS mounted with video recording camera where “there is a strong possibility of collecting personally identifiable information UAVs will make use of video recording to consider the use of anonymous video analytics”**.<sup>40</sup> Regarding to the “Privacy as Default Setting Principle”, she states that **State agencies using RPAS for collection information “may be used only for the purposes of the stated rationale and objectives set out to protect public safety, and to detect (or deter) and assist in investigating criminal activity”**.<sup>41</sup> This report is a goldmine for legislators and it could be used to establish a checklist of PbD measures for RPAS manufacturers and users to observe.

In its FAQ on drones<sup>42</sup>, the Belgian Privacy Commission also underlines the importance of taking a PbD approach in the case of drones. Firstly, it states that **according to the finalities for which drones aim to be used, RPAS manufacturers should integrate them in their design technical modalities in order to prevent that drones will be used for any other purposes**. Secondly, the DPA gives different concrete applications of the PbD principle in the context of RPAS. For instance, it states that drones operators should equip its RPAS only with the necessary payloads to carry out the objectives for which they are used.<sup>43</sup> “Therefore, a **drone used for recreational purpose by a private operator in its backyard should not technically be able to fly at higher altitude than it is necessary for such use**, which otherwise would be disproportionate”, clarifies the Privacy Commission.<sup>44</sup> It also refers to encryption systems and image blurring techniques as the best way to avoid accidental capture of personal data. Finally, it is noteworthy that besides these two data protection authorities, many other privacy specialists promote embedding privacy protection measures into the

---

<sup>38</sup> Ann Cavoukian, Privacy Commissioner of Ontario, Privacy and Drones: Unmanned Aerial Vehicles”, 2012, <http://www.ipc.on.ca/images/Resources/pbd-drones.pdf>

<sup>39</sup> Ibid.

<sup>40</sup> Cavoukian, Ann, op. cit., 2012.

<sup>41</sup> Ibid.

<sup>42</sup> The Belgian Privacy Commission, “Questions les plus fréquemment posées – Drones », FAQ 2014, <http://www.privacycommission.be/fr/faq-page/7346>

<sup>43</sup> Ibid.

<sup>44</sup> The Belgian Privacy Commission, op. cit., 2014..

technology, and specifically, that RPAS developers and manufactures should build Privacy by Design in the fabrication of drones and payloads.<sup>45</sup>

These last considerations prove that the PbD should be used for regulating RPAS technology. Consequently, **we urge industries organizations to create guidance on PbD measures that manufacturers and designers will have to enhance in the creation of drones and payload. Furthermore, we recommend data collectors to use privacy enhanced drones**

### 11.3.2 Technological solution - Data Protection Impact Assessment

#### Concept

Designed to promote Privacy by Design, a Privacy Impact Assessment (PIA)<sup>46</sup> “*is a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme and finding ways to mitigate or avoid any adverse effects*”.<sup>47</sup> It is noteworthy that the definitions of this term as well as the methodologies employed vary “from one regime to another, from a company to another”.<sup>48</sup> Nevertheless, all PIAs have for common objective to identify and evaluate the risks of the project, the legislation or even the processing activity in relation to a certain technology and to recommend measures or initiatives to address these risks.

Impact assessments policies have already been put in place in several third states like Australia, Canada, Hong Kong, New Zealand and the United States. Inside the European Union, we found that neither the Member States legislation nor the European Directive 95/46/EC refer to PIAs. However, in UK PIAs have already been conducted in some organisations. This comes from the fact that the UK Information Commissioner has already issued a Handbook<sup>49</sup> and a Code of Practice<sup>50</sup>, which recommends that organisations processing personal data ought to conduct a PIA and “set out the basic steps which an organisation should carry out during the assessment process”.<sup>51</sup> Furthermore, the European Commission issued a Recommendation in 2009 in which it called upon “*the member states to ensure that the industry, in collaboration with relevant stakeholders, develops a framework for privacy and data protection impact assessment for the development of radio frequency*

---

<sup>45</sup> Joseph, Jerome, “Domestic Drones Should Embrace Privacy By Design”, Future of Privacy Forum, 2013. <http://www.futureofprivacy.org/2013/04/05/domestic-drones-should-embrace-privacy-by-design/>;  
Schlehahn, Eva, Marit, Hansen, Jaro, Sterbik-Lamina, Javier, Sempere Samaniego, *Report on surveillance technology and privacy enhancing design*, EU Surprise Project – Deliverable 3.1, 2013 and Uri, Volovelsky, “Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study”, *Computer Law and Security Review*, Vol. 30, 2014, p. 320.

<sup>46</sup> For more information about the concept of PIA, see: De Vries Ekaterina and Mireille Hildebrandt, *Security impact assessment measure - a decision support system for security technology investments (SIAM)*, Deliverable D9.7. Report on the Legal Framework of the Use of SMTs at EU and International Level, 2014; Kloza Dariusz, “Privacy Impact Assessments as a Means to Achieve the Objectives of Procedural Justice”. *Jusletter IT. Die Zeitschrift für IT und Recht*, 2014 and Wright, David and Paul, De Hert, *Privacy Impact Assessment*, Springer, 2012.

<sup>47</sup> PIAF Project, *A Privacy Impact Assessment Framework*, 2012. <http://www.piafproject.eu>

<sup>48</sup> Wright, David and Paul de Hert, “Introduction to Privacy Impact Assessment”, in Wright, David and Paul de Hert (Eds.), *Privacy Impact Assessment*, Springer, London, 2012.

<sup>49</sup> UK Information Commissioner’s Office, “Privacy impact assessments Handbook”, [http://ico.org.uk/pia\\_handbook\\_html\\_v2/files/PIAhandbookV2.pdf](http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf)

<sup>50</sup> UK Information Commissioner’s Office, “Conducting privacy impact assessments code of practice”, [http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/privacy\\_impact\\_assessment](http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment)

<sup>51</sup> Ibid.

identification (RFID) tags which was destined to be submitted for endorsement to the Article 29 Data Protection Working Party”<sup>52</sup>. Since the UK and the European Commission initiatives, there have been frequent calls for PIA in Europe. For example, in its recommendation on biometrics, the Article 29 Working Party recommends that “*the one that defines the purpose and the means of the device execute privacy impact assessments as an integral part of the design phase of systems dealing with this type of data. It can be the manufacturer, the integrator or the final client*”.<sup>53</sup> In addition, European Commission Vice President, Viviane Reding, stated in 2010 that “*Businesses and public authorities... will need to better assume their responsibilities by putting in place certain mechanisms such as the appointment of Data Protection Officers, the carrying out of Privacy Impact Assessments and applying a 'Privacy by Design' approach*”.<sup>54</sup>

All these initiatives are not in vain as Data Protection Impact Assessments (DPIAs) are formally acknowledged in the draft Regulation.<sup>55</sup> Whereas a definition of the concept is not provided, Article 33 requires from data collectors to conduct such DPIA when processing operations are likely to present specific risks. So they are no to be find generalised application.<sup>56</sup> In the Parliament proposal, we can even find a list of categories of risks for which collectors need to carry out a DPIA.

#### *Privacy impact assessments in the context of RFID data processing activities*

As previously mentioned, PIAs have already been carried out in the context of certain data processing activities. At the European level, RFID companies are strongly recommended to carry out PIAs. Indeed, since the Commission’s Recommendation mentioned earlier and the endorsement of the PIA Framework by the Article 29 Working Party, RFID companies are encouraged to sign up to the "Privacy and Data Protection Impact Assessment (PIA) Framework for RFID Applications" under which they agree to carry out a privacy and data protection risk assessment of products containing RFID chips prior selling them (for manufacturers) or prior processing data (for data collector).<sup>57</sup> Although carrying out a PIA is not mandatory for RFID operators, Member States are responsible with promoting that RFID operators conduct a privacy and data protection impact assessment (PIA) of RFID applications based on the PIA Framework before they are deployed. Furthermore, Member States should also ensure that the RFID operators will make the resulting PIA Reports available to the competent authority.<sup>58</sup>

As such, the EU as well as industry organisation and academics have recognised that conducting a PIA, on a case-by-case basis, represents a “*good practice*” as this soft-law measure is “*well understood, and readily applied by any organisation*”<sup>59</sup>. However, PIAs are

---

<sup>52</sup> European Commission, Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, 12.05.2009.

<sup>53</sup> Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, 27 April 2012.

<sup>54</sup> Viviane Reding, “Towards a true Single Market of data protection”, *Speech /10/386*. 14 July 2010.

<sup>55</sup> European Parliament, op. cit., 2012, Article 33.

<sup>56</sup> De Hert, Paul and Vagelis, Papakonstantinou, “The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals”, *Computer Law & Security Review*, Vol. 28, 2012, p. 140.

<sup>57</sup> Wright, David and Paul, De Hert, *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

<sup>58</sup> Ibid.

<sup>59</sup> Roger Clarke, “The regulation of civilian drones’ impacts on behavioural privacy”, *Computer law & Security review*, Vol. 30, 2014, pp. 286 -305.

still at its beginning of implementation and then, we lack of practical evidences of its pros and cons. Nevertheless, privacy impact assessment specialists have already highlighted several general benefits. *From the company perspective*, adopting a PIA will “facilitate their compliance with the privacy and data protection law and will mitigate the greatly the legal uncertainties around the deployment of such applications”.<sup>60</sup> Furthermore, there can be financial benefits to conducting a PIA<sup>61</sup> as the costs of fixing a project at the planning stage will be a fraction of those incurred later on<sup>62</sup>. By identifying a problem early, they help company to adopt a simpler and less costly solution. In addition, an organisation that undertakes a PIA “appropriately demonstrates that it takes societal concerns into account”<sup>63</sup> Therefore, by conducting and publishing a PIA, it is a means of reassuring the public and RPAS organisations build public trust and confidence in their services. Moreover, the actions taken during and after the PIA process can improve an organisation’s understanding of their customers. Regulators will also be more “sympathetic towards organisations that undertake PIAs than those that do not. A PIA is a self- or co-regulatory instrument that may obviate the need for severe enforcement of “hard” law. Thus, if organisations are seen to carry out proper (full-blooded) PIAs, they may escape the more onerous burdens imposed by legislation”.<sup>64</sup> *From the individual perspective*, an organisation that has carried out a PIA follows the best practices and thus a priori ensures the data protection principles and respects its rights. Furthermore, a project that has been subject to a PIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way.<sup>65</sup> A third benefit to individuals is that a PIA, in principle, “improves transparency and makes it easier for them to understand how and why their information is being used”.<sup>66</sup>

#### *Privacy Impact Assessment in the context of RPAS technology*

Before determining whether adopting the PIA approach in the context of civilian drones would be a good practice, it is noteworthy to consider that this idea of conducting Privacy Impact Assessments has already been invoked by different privacy authors<sup>67</sup>, as well as by data protection authorities. The Data Protection Authority of Ontario (Canada) has highlighted the importance of undertaking PIA in the context of civil drones when she stated “an assessment should be conducted of the effects that the proposed UAV system may have on personal privacy, and the ways in which any adverse effects can be mitigated, by examining the collection, use, disclosure, and retention of personal information”.<sup>68</sup>

---

<sup>60</sup> Beslay, L. and A.-C., Lacoste, “Double Take: Getting to the RFID PIA Framework” in Wright, David and Paul de Hert (Eds.), *Privacy Impact Assessment*, Springer, London, 2012.

<sup>61</sup> UK Information Commissioner’s Office, “Conducting privacy impact assessments code of practice”, 2014, [http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/privacy\\_impact\\_assessment](http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment)

<sup>62</sup> Wright, David and Charles, D. Raab, “Constructing a surveillance impact assessment”, *Computer Law and Security Review*, Vol. 28, 2012, pp. 613- 626.

<sup>63</sup> Ibid.

<sup>64</sup> Wright, David and Charles, D. Raab, op. cit 2012, pp. 613 – 626.

<sup>65</sup> UK Information Commissioner’s Office, “Conducting privacy impact assessments code of practice”, 2014, [http://ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/privacy\\_impact\\_assessment](http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment)

<sup>66</sup> Ibid. and for more information on the benefits of conducting PIAs, see Wright, David and Paul de Hert, “Introduction to Privacy Impact Assessment”, in Wright, David and Paul de Hert (Eds.), *Privacy Impact Assessment*, Springer, London, 2012, p.10.

<sup>67</sup> “Privacy Impact Assessment”, *Considerati*, 2014. <http://www.considerati.com/services/legal/529-2/privacy-impact-assessment/>

<sup>68</sup> Cavoukian, Ann Privacy Commissioner of Ontario, “Privacy and Drones: Unmanned Aerial Vehicles”, 2012, <http://www.ipc.on.ca/images/Resources/pbd-drones.pdf>

Furthermore, the Commissioner has since included the conduct of a PIA among its recommendations,

*A PIA can allow for a systematic examination of the impacts and associated benefits involved in deploying UAVs. Before engaging in an activity that involves UAV technology, an assessment should be conducted of the effects that the proposed UAV system may have on personal privacy, and the ways in which any adverse effects can be mitigated, by examining the collection, use, disclosure, and retention of personal information.*<sup>69</sup>

Another report issued by the Surveillance Studies Centre *Surveillance Drones: Privacy implications of the spread of Unmanned Aerial Vehicles (UAVs) in Canada* has also included in its recommendations that “current regulations standards for UAVs should include mandatory Privacy Impact Assessment...”.<sup>70</sup> Moreover, the data protection authority of Queensland has also emphasised the idea of carrying IPAs when personal information are processed through the means of drones: “A Privacy Impact Assessment may be one mechanism for engaging with the community concerning drone use and management”.<sup>71</sup>

Now we get down to the question “is PIA the perfect tool to mitigate the privacy, data protection and ethical risks posed by the RPAS technology?” PIA is a risk assessment tool that can be tailored to your technology and multiple considerations. Moreover, they can also **take in account of the specificity of their individual operation, the capabilities of their RPAS, the payloads that it would carry and the data that would be collected.** Therefore, PIAs are particularly suited to technology like RPAS. **They will not only focus on the data protection risks raised by the technology but they will also evaluate the privacy, ethical and social concerns that a specific RPAS usage can pose.** In addition, **being also a preventive security measure, PIAs would allow to drones’ operators to address the processing security risks inherent to its features like preventing to process inadvertently data.** Consequently, **by introducing the obligation for commercial operators to conduct a PIA on a case-by-case basis, legislators would fill the current legal remaining gap related to the lack of preventive security measures applying to commercial operators.** Furthermore, by carrying out a PIA, drones operators would easier implement the data protection requirements and ensure the individuals’ rights. For instance, we have seen in the *Real Estate scenario* that a real estate company which makes a video showcasing a home for sale is likely to pose risks surrounding privacy, data protection and ethics when she/flies her RPAS above a residential area. However, by conducting a PIA all these risks will be identified prior the flight and the Real Estate Company will be informed by the privacy specialist of the additional measures it should adopt. In certain cases like this one a simple measure like blurring technology will be even sufficient.

Now, having considered the number of reasons supporting the adoption of PIAs, we now turn our examination to the adoption of PIAs in the context of drones. Whereas we have emphasised throughout this deliverable that PIAs should be adopted by the RPAS collector

---

<sup>69</sup> Ibid.

<sup>70</sup> Surveillance Studies Centre “Surveillance Drones: Privacy implications of the spread of Unmanned Aerial Vehicles (UAVs) in Canada”, Kingston, 2014.

<sup>71</sup> Office of the Information Commissioner Queensland, “Drones - collection, storage and security of personal information”, 2014. <http://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/applying-the-privacy-principles/drones-collection,-storage-and-security-of-personal-information>

prior its operations, **we recommend the European Union and the Member States adopt PIAs at all levels.** In other words, we promote the idea that **PIA should not only be adopted by the user of the technology but also at the stage of the policy decision-making process.** In the context of RPAS this means that **any legislation or policies relating to a drone application regardless of whether the matter concerns privacy, safety or insurance should be subject to a privacy impact assessment before being adopted.** By doing this legislator will already prevent themselves from enacting rules which might impact privacy.

Under the Draft GDPR, the PIA will only be mandatory for RPAS collectors when their processing activities will likely to pose one or more of the following specific risks:

- (a) processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;*
- (b) processing of special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large scale filing systems;*
- (c) profiling on which measures are based that produce legal effects concerning the individual or similarly significantly affect the individual;*
- (d) processing of personal data for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;*
- (e) automated monitoring of publicly accessible areas on a large scale;*
- (f) other processing operations for which the consultation of the data protection officer or supervisory authority is required pursuant to point (b) of Article 34(2);*
- (g) where a personal data breach would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject.<sup>72</sup>*

Scholars in this area do not all share the same view. Some scholars promote that each time an organisation use a new technology which impacts privacy, they should conduct a PIA.<sup>73</sup> Others defend that it will depend on the type of data collected, the purposes of the collection, the type of drones' operators, the accuracy of the payload mounted on the drone, etc. For example, private operators do not need to conduct a PIA for taking footages during her/his birthday party with a drone equipped of a camera. However, if the operator is a company which collect data through the means of RPAS for commercial purposes, a PIA can be needed.

Whereas it is hard to determine a list of circumstances in which a PIA should be conducted in the context of drones, we think that there are several cases not included in the draft of the GDPR in which PIAs should be mandatory for RPAS operators:

- the RPAS operator risks to process inadvertently personal data;
- the processing activity is made by a visual payload and takes place in public places;
- the data processing activity is performed by state agencies in the framework of a covert surveillance investigation;

---

<sup>72</sup> European Parliament, op. cit., 2012, Article 32a§2.

<sup>73</sup> Wright, David and De Hert Paul, "Findings and Recommendations in Privacy Impact Assessment" in, Wright, David and De Hert Paul (Eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

- the processing activity aims to build profiles or to make direct marketing thanks to the personal data which will be collected.

In this respect, like it has recommended in the context of biometric data processing<sup>74</sup>, **we recommend that the Article 29 Working Party issues relevant guidelines helping RPAS operators to decide when and how they should carry out a PIA.**

A final focus question for discussion could be: “*how to monitor that RPAS operators have conducted a PIA before the operation?*” It seems that the more pragmatic way to enforce PIAs would be in two steps. Firstly, we think that DPAs are the best suited to evaluate that a PIA has been well conducted. These latter could then after evaluation certify operators. Such certification will be then checked by CAAs which on this basis will permit commercial operators to launch their drones in the air.

### 11.3.3 Technological solution - Surveillance Impact Assessment

#### Concept

Derived from the Privacy Impact Assessment concept discussed above, a SIA differs from a PIA by its scope above all.<sup>75</sup> An SIA is mainly “focused on groups or society as a whole. While a PIA may also consider societal effects of privacy intrusions caused by a new technology, project or service, its starting point is the individual”.<sup>76</sup> In other words, a PIA “would not catch all of the implications raised by a surveillance project”.<sup>77</sup> However, like PIA, SIAs methodologies differ from a surveillance project to another, from an industry to another.

The first reference to Surveillance Impact Assessment (SIA) comes from the Surveillance Society report prepared by the Surveillance Studies Network European in 2006.<sup>78</sup> In 2001, the Commission’s Directorate General Enterprise, proposed the development of a surveillance impact assessment methodology in the Sapien project<sup>79</sup> which set up “a privacy impact assessment framework designed to address the particularities of existing and envisioned smart surveillance systems, technologies, projects and policies”<sup>80</sup>.

---

<sup>74</sup> In its opinion of 3/2012 on developments in biometric technologies, the Article 29 Working Party refers to a previous Opinion in 2012 in which it recommends to biometric data operators to undertake a PIA: “*The one that defines the purpose and the means of the device execute privacy impact assessments as an integral part of the design phase of systems dealing with this type of data. It can be the manufacturer, the integrator or the final client. When the PIA has been conducted by the manufacturer or the integrator, the deployment of the biometric system can also require an additional assessment to take into account the specificities of the data controller*”.

<sup>75</sup> Wright, David and Charles, D. Raab, op. cit., 2012, p. 613.

<sup>76</sup> Ibid.

<sup>77</sup> Ibid.

<sup>78</sup> Surveillance Studies Network (SSN), *A Report on the Surveillance Society*, prepared for the Information Commissioner, September 2006. <http://www.ico.gov.uk/Global/Search.aspx?collection%40ico&keywords%40surveillance%40report>.

<sup>79</sup> SAPIENT consortium, “The SAPIENT project” 2011-2014, <http://www.sapientproject.eu/>

<sup>80</sup> Wright, David and Charles, D. Raab, op. cit., 2012, p. 613.

### *Surveillance impact assessments in the context of data processed by civil drones*

Able to perform all types of surveillance (watching, listening, location, detecting, dataveillance<sup>81</sup>, covert, visible, personal, mass surveillance, sousveillance<sup>82</sup>) thanks to its wide range of payloads, it is unequivocal that the RPAS technology is a technology of surveillance. They go so far as to refer it as the “perfect surveillance tool”. Therefore, it is clear that conducting a SIA or including a SIA into a PIA would be an interesting way to address the concerns that a simple PIA does not, economic, financial, political, criminal and psychological issues.

However, as we cannot find discussions in the literatures about SIAs in the context of civil drones and as no SIAs have been implemented, we cannot bring practical evidences showing that conducting a SIA would be the “Best Practice” that each RPAS companies performing surveillance should adopt. However, it is clear that the scope of the SIA will depend on the type of surveillance performed, the type of operator, the contextual factors, the payloads to be used, the purpose of the surveillance, where and when it will be deployed, and so on. In this regard, we support the comment of the Report on the Surveillance Society clarifying that “Any SIA, like any PIA, would have to be tailored to the specific characteristics of the practices or technologies in question”.<sup>83</sup> Nevertheless, **this does not prevent the surveillance sector and the commercial sector performing surveillance operations to adopt a Code of Conduct setting up some common practices and common requirements they should met.**

#### *11.3.4 Voluntary Solutions - Privacy Audits*

##### *Concept*

A Privacy Audit may be defined as “A *systematic and independent examination to determine whether activities involving the processing of personal data are carried out in accordance with an organization’s data protection policies and procedures, and whether this processing meets the requirement of the Data Protection Law*”.<sup>84</sup> Audits may be voluntary or mandatory.

Therefore, in privacy matters, an audit has the objective of guiding enterprises and administrations to understand and comply with privacy and data protection legislation in their processing activities.<sup>85</sup> The work of auditors consists to identify processing activities of entities carried out in their daily basis and analyse them with objective and independent standards based on the applicable legislation and entities’ own policies and procedures<sup>86</sup> in order to determine if corrective measures should be undertaken<sup>87</sup>.

---

<sup>81</sup> Dataveillance is “*the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons*”. Clarke, Roger, op. cit., 2014, pp. 286 -305.

<sup>82</sup> Sousveillance is “*the use of veillance techniques and technologies by the less powerful, usually individuals, against the more powerful, usually organisations*”. Clarke, Roger, op. cit., 2014, pp. 286 -305.

<sup>83</sup> Surveillance Studies Network (SSN), op. cit., 2006.

<sup>84</sup> France, Elizabeth, “Data Protection Audit Manual”, 2001.

[http://www.privacylaws.com/Documents/External/data\\_protection\\_complete\\_audit\\_guide.pdf](http://www.privacylaws.com/Documents/External/data_protection_complete_audit_guide.pdf)

<sup>85</sup> Goblet, Cédric, “Audit en matière de vie privée & de données à caractère personnel”, 2014.

[http://www.lexconsult.pro/avocat\\_services/audit-de-conformite-legislation-vie-privee-et-donnees-a-caractere-personnel.php](http://www.lexconsult.pro/avocat_services/audit-de-conformite-legislation-vie-privee-et-donnees-a-caractere-personnel.php)

<sup>86</sup> According to Roger Clarke, auditors have “*a professional obligation to examine plans, policies, manual and automated procedures and practices, for compliance with the law, and with corporate privacy strategy and*

Contrary to Privacy Impact Assessment (PIA), a Privacy Audit “presumes the existence of specific laws and/or standards with which a proposal or project needs to comply”.<sup>88</sup> Moreover, it does not assess a specific processing activity but generally evaluates the performance of an already existing operational system. However, both have the same objective which is “effectively identifying and controlling risks to prevent breaching the data protection law”.<sup>89</sup>

In Europe, the current Data Protection Directive 95/46/EC do not make any reference to Privacy Audit but the Proposal Regulation will operate a change in this regard as it stipulates in its Article 22(3): “*the controller must implement mechanisms to ensure the verification of the effectiveness of measures outlined in Article 22 (1) and (2) (i.e., data processing, data protection impacts assessments and data security). Further, “If proportionate, this verification shall be carried out by independent internal or external auditors”.*”<sup>90</sup>

#### *Privacy audits in the context of biometric processing activities*

Privacy specialists particularly recommend businesses and public authorities to carry out Privacy Audits when they process sensitive data like biometric data.

Regarding biometric data processing activities, we observed that the Biometric Institute has issued Biometric Privacy Guidelines in which it set up several principles including a Principle Five in which it requires: “*The data controller or equivalent person(s) should be accountable for protecting biometric data collected. This should include... annual or regular **Privacy Audits** that examine and report on privacy compliance and can detect any degradation of the privacy environment. The auditing personnel should report to a high level officer in the company or agency*”.<sup>91</sup> Els de Busser, in its book entirely devoted to biometrics data processing activities, also suggest that entities processing biometric data must undertake “*organizational measures*” by carrying out regular and systematic Self-Auditing and Certification. She particularly emphasizes that Privacy Audit is a “good practice” for assessing the effectiveness of security measures such as encryption and ensuring that threats have been identified and correctly addressed by additional safeguards.<sup>92</sup>

However in RFID technologies, the Privacy Impact Assessment instrument has been preferred. Claude Tételin, member of the Centre National de Référence RFID, informs us of the reasons:

*A privacy compliance audit differs from a privacy impact assessment in that the compliance audit determines an institution’s current level of compliance with the law and identifies steps to avoid future non-compliance with the law... The primary concern of a compliance audit is simply to meet the requirements of the law, whereas*

---

*policy. They accordingly have a responsibility to keep themselves informed of developments in relevant law, and in privacy-relevant technologies”.* Clarke, Roger, “Information Systems Audit & Information Privacy”, 1999, <http://www.rogerclarke.com/DV/Audit.html>

<sup>87</sup> Goblet, op. cit., 2014.

<sup>88</sup> Clarke, Roger, “Privacy Impact Assessments”, 2003. <http://www.rogerclarke.com/DV/PIA.html>

<sup>89</sup> Ibid.

<sup>90</sup> European Parliament, op. cit., 2014, Article 22(3).

<sup>91</sup> The Biometric Institute, “Biometrics Privacy Guidelines”, 2013.

[http://www.biometricsinstitute.org/data/Privacy/BiometricsInstitute\\_BIOMETRICS\\_GUIDELINES\\_V1.pdf](http://www.biometricsinstitute.org/data/Privacy/BiometricsInstitute_BIOMETRICS_GUIDELINES_V1.pdf)

<sup>92</sup> J. Kindt, Els, *Privacy and Data Protection Issues of Biometric Applications- A comparative analysis*, Springer, Dordrecht, 2013, p. 818.

*a privacy impact assessment is intended to investigate further in order to identify ways to safeguard privacy optimally.*<sup>93</sup>

In Europe, privacy audits are mostly confidential. Therefore, it is hard to find literature which explains the positive data protection changes that Privacy Audits have operated for certain entities. However, the UK data protection authority has issued reports in which it lists good practice activities they observe during their privacy audits and which positively impact the organization's ability to comply with the data protection obligations. For example, in the private sector, it has observed the following good practices: "annual internal audit plan and control self-assessment and compliance testing is completed on a quarterly basis at business unit level against key business processes and information security; data protection representatives have been nominated in each business unit; etc."<sup>94</sup>

#### *Privacy audits in the context of data processed by civil drones*

Different American scholars and privacy watchdogs have issued reports in which they affirm that a privacy audit should be carried out by entities using drones for processing personal information. In its report on civilian drones, American Civil Liberties Union (ACLU) has included Privacy Audit in its recommendation:

*...And if aerial surveillance technology is deployed, independent **audits** should be put in place to track the use of UAVs by government, so that citizens and other watchdogs can tell generally how and how often they are being used, whether the original rationale for their deployment is holding up, whether they represent a worthwhile public expenditure, and whether they are being used for improper or expanded purposes.*<sup>95</sup>

Furthermore, it has also evoked Privacy Audits in its comments to the FAA: "The FAA must ensure that appropriate oversight is in place to monitor compliance with the final rule, including independent audits and community involvement."<sup>96</sup>

Additionally, the scholar Ben Jenkins explains why governments could consider including security mechanisms like Privacy Audits in their RPAS legislations:

*Drone Aircraft Privacy and Transparency Act of 2013 (DAPTA) should require random external program audits of drone operators in accordance with government auditing standards. Random audits would discourage malfeasance and verify the accuracy of operators' data collection and minimizations statements... Auditing would provide a direct link between transparency and the credibility of the public sector entity. Auditing ensures all of the information disclosed to the public about drone operational activities is honest and complete. For example, if an operator reports that information gathered through a particular surveillance operation was destroyed on a*

---

<sup>93</sup> Tételin, Claude, "RFID and Privacy Impact Assessment (PIA)", 2014, [http://webistem.com/ursif2014/output\\_directory/website/data/articles/000011.pdf](http://webistem.com/ursif2014/output_directory/website/data/articles/000011.pdf)

<sup>94</sup> For more information on UK privacy audits, see ICO, "What is an audit and how can I request one?", 2014, [http://ico.org.uk/for\\_organisations/data\\_protection/working\\_with\\_the\\_ico/audits](http://ico.org.uk/for_organisations/data_protection/working_with_the_ico/audits)

<sup>95</sup> Stanley, Jay, "Comments on the FAA on the agency's incorporation of privacy into its drone "test zones" program". *ACLU*, New-York, 2011.

<sup>96</sup> Stanley, Jay and Catherine, Crump, "Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft", *ACLU*, New-York, 2011.

*specific date, the operator is aware that if audited, and his information does not correlate, he might face a lawsuit and forfeiture of his license. The persistent possibility of an audit encourages compliance with statutes and regulations even if U.S. residents become complacent due to changes in privacy norms.*<sup>97</sup>

In Europe, there is a greater tendency towards the adoption of PIAs as the lesser economic and administrative burden on entities. This is also the choice adopted by Proposal Data Protection Regulation that requires collectors to carry out a PIA prior to risky processing operations. However, the Act also proscribes the adoption of security mechanism like external audit.<sup>98</sup> In this regard, we think that **full annual-audits should also be made available to RPAS companies on a voluntary basis to evaluate and reinforce the security of their data processing systems.**

### 11.3.5 Voluntary solution - Self-Regulations

#### Codes of conduct, Guidelines, Codes of Ethic, Recommendations, Communications

##### *Concept*

Over the past decade, the EU and its Member States have been developing a new regulatory policy, giving birth to alternative instruments at their ordinary state laws. Such complementary instruments are called “self-regulations”. Self-regulations have been defined by the European Commission as “*the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements)*”.<sup>99</sup> These quasi-legal instruments are non-binding and may be freely interpreted. In privacy matters, soft law instruments are generally issued by data protection authority, companies and industry organisations. Their objective is to “promote behaviour by involving stakeholders and establishing bottom-up soft regulations”.<sup>100</sup> They also take different forms - codes of conduct, guidelines, codes of ethic, recommendations, communications and we can encounter them in many areas: environment, justice, and economic matters but also in privacy and data protection matters. At the European level, the current Data Protection Directive 95/46/EC promotes the adoption of privacy self-regulations, “self-governance”:

*Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation<sup>101</sup>”. In the GDPR proposal we found the same encouragement for the adoption of codes of conduct. Nevertheless, the proposal goes even further as it specifies in which areas*

---

<sup>97</sup> Jenkins, Ben, “Watching the Watchmen: Drone Privacy and the Need for Oversight”, *Kentucky Law Journal*, Vol. 102, pp. 161-182.

<sup>98</sup> European Parliament, op. cit., 2014, Article 22 and 37.

<sup>99</sup> Communication from the Commission, Action plan ‘Simplifying and improving the regulatory environment’, COM(2002) 278 final, 05.06.2002.

<sup>100</sup> The European Group On Ethics In Science And New Technologies, Opinion No. 28 on ethics of security and surveillance technologies, Brussels, 20.05.2014, p. 59.

<sup>101</sup> European Parliament and the Council, 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 OJ L 281, 23.11.1995, (“Directive 95/46/EC”), Preamble.

*such codes should be particularly set up and also recommends to data protection authorities and associations of collectors and processors to enact such codes.*<sup>102</sup>

### *Self-regulations in the context of CCTV systems uses*

Privacy and data protection self-regulations have been adopted by different institutions (data protection authorities, industries, user and manufacturer associations, etc.) and for governing different type of technologies and profession (CCTV systems, Internet, journalism,). It is also noteworthy that “various statutory and self-regulatory bodies oversee and enforce industry codes, guidelines, Code of Conduct which protect against invasions of privacy. For example, website owners, commercial televisions, radio broadcasters and journalists”.<sup>103</sup> In our analysis of Member States surveillance regulations, we observed that data protection authorities have specifically issued self-regulations (Code of Practice, Recommendations, Guidelines) covering uses of CCTV systems. Footages of persons being subject to the national data protection law and other CCTV legislation, we had seen that DPAs have principally issued CCTV code of Practice to clarify and tailor for each user the specific rules they must comply with. In this regard, we had highlighted the Factsheets published by the French Data Protection authority.

Whereas the self-regulations are encouraged at national and European levels, different academic studies have examined whether privacy and data protection standards should be rather adopted by governmental regulations or self-regulations. In reality, privacy scholars do not all held the same view regarding the well-funded of “self-regulation”. While certain promote the merits of self-regulations, others emphasise that “self-regulation” as a solution to address privacy and data protection concerns posed by new technologies failed<sup>104</sup>. Finally, besides the pros and cons of “self-regulation”, there are also a category of authors which aware of advantages and limitations of both regimes, states that a combination of governmental and voluntary regulations is the best model to adopt for governing the ICTs.<sup>105</sup>

### *Self-regulation for RPAS technologies?*

In the previous deliverable, we examined that there exists very few self-regulations related to the civil use of RPAS. We identify only three voluntary regulations: the Recommended Guidelines for the Use of Unmanned Aircraft issued by the International Association of Chiefs of Police Aviation Committee, the Unmanned Aircraft System Operations Industry “Code of Conduct adopted by the Association for Unmanned Vehicles Systems International (AUVSI) and the Drone Journalism Code sets up by the journalism instructor of the College of the North Atlantic. While analysing the privacy rules into these self-regulations, we found that they are very few privacy and data protection oriented standards, they are general, vague,

---

<sup>102</sup> European Commission, op. cit., 2012, Article 38.

<sup>103</sup> Australian Government, *Overview of Current Law - Industry codes and guidelines*, 2014, <http://www.alrc.gov.au/publications/3-overview-current-law/industry-codes-and-guidelines>

<sup>104</sup> “Self-regulation has allowed the development of new tracking technologies, and the continued employment of old ones. Self-regulation allows companies to obfuscate their practices, leaving consumers in the dark. Emerging technologies represent serious threats to privacy and are not addressed by self-regulation or law. Self-regulation has failed to produce usable anonymous payment mechanisms. We now know that self-regulation failed to address security” Hoofnagle, Chris Jay, “Privacy Self-Regulation: A Decade of Disappointment”, in Jane K. Winn, (ed.), *Consumer Protection in the Age of the Information Economy*, Ashgate, 2006.

<sup>105</sup> Dumortier, Jos and Caroline Goemans, “Discussion Paper prepared for the CEN/ISSS Open Seminar on data protection”, ICRI, 2010, p. 23-24.

and they do not have any enforcement mechanisms, sanctions or other measures that would otherwise deter invasive technologies and their use.

Roger Clarke, a privacy specialist, has also recently examined whether it would be relevant that RPAS operators, industries and organisations adopt self-regulations. Regarding Self-Regulation Organisation, he explains that there is no such self-regulations related to civil drones or other surveillance technologies in Australia and then that, “in the absence of any evidence of commitments by organisations in relation to responsible use of surveillance technologies, it is difficult to see organisational self-regulation playing any role in the control of drone surveillance”.<sup>106</sup>

Furthermore, Roger Clarke opines that “Self-Regulatory Forms” are not the “Best Practices” to adopt for addressing privacy concerns related to surveillance technologies including drones. He further concludes:

*None of the soft regulatory forms make any significant contribution towards satisfying the criteria for effective regulation... They provide virtually no protections against unjustified, disproportionate and unsafe surveillance. The protection of behavioural privacy against undue surveillance is therefore entirely dependent on formal regulatory arrangements.*<sup>107</sup>

However, after examining the cons of self-regulations, we have also found several privacy scholars<sup>108</sup> who recommend that RPAS manufacturers and organisations of drones’ operators adopt well-set-up Codes of Conduct. Therefore, we should now analyse what are the benefits that such Codes of Conduct could afford in the regulation of RPAS.

First, being technologically neutral the data protection law applies to all technologies but it presents problems because of the general nature of that application and the generality of the laws that produce rules that are abstract and difficult to operationalise by data collectors.<sup>109</sup>

**Developing code of practices which tailor a rule to a specific technology and set up practical examples allow to make the data protection law a more practical and living instrument for RPAS manufacturers and operators.** So by adopting such codes, DPAs gives clear-cut information to assist RPAS operators and industry participants to better understand how they should comply with the data protection law. Furthermore, being flexible and easily reviewable, these codes can also incorporate privacy, ethical and moral recommendations and not only focusing on the data protection ones. Consequently, we stress Data Protection Authorities and more particularly the Article 29 Working Party to adopt an Opinion or a Code of Conduct in which they could for instance set up a checklist of the duties that each kind of RPAS collector operator must achieve and explain how they should be ensure them in the context of RPAS processing.

---

<sup>106</sup> Clarke, Roger, “The Regulation of the Impact of Civilian Drones on Behavioural Privacy”, *Computer, Law & Security Review*, Vol. 30, no. 3, 2014, pp. 286-305.

<sup>107</sup> Ibid.

<sup>108</sup> Cavoukian, Ann Privacy Commissioner of Ontario, op. cit., 2012. [Uri Volovelsky](#), “Civilian uses of unmanned aerial vehicles and the threat to the right to privacy – An Israeli case study”, *Computer Law and Security Review*, Vol. 30, 2014, p. 320.

<sup>109</sup> Groupe Européen d’Ethique des Sciences et des Nouvelles Technologies, op. cit., 014.

Example. Checklist for commercial data collectors (under the Directive 95/46/EC)

RPAS controllers must:

- process data legally and fairly;
- process for explicit and legitimate purposes and used accordingly;
- process adequate, relevant and not excessive personal data in relation to the purposes for which it is collected and/or further processed;
- process accurate data and must update them where necessary;
- do not keep data any longer than strictly necessary;
- implement the appropriate security measures to protect personal data against accidental or unlawful processing, destruction, loss, alteration and disclosure;
- inform the data subjects concerned and give them a right to access for free to their data;
- ensure that data subjects can rectify, remove or block incorrect data about themselves;
- notify the competent supervisory authority of their processing operations (must be done prior processing operations when he/she intends to carry out risky processing activities).

Second, manufacturing and design industries are certainly the most concern with respect to self-regulation. Indeed, by setting up self-regulation measures, they will **encourage a respect of privacy from the outset and will support manufacturers in enhancing privacy features of the RPAS**. Further, self-regulations fitting well with PbD measures<sup>110</sup>, they can even help RPAS developers in the achievement of such measures by describing them and their implementation step-by-step. **Provider's organisations** are also concerned by RPAS self-regulations. For instance, they **should push RPAS providers to incorporate privacy instructions on the packaging box or include a website link in which RPAS users could learn how to use their drones by respecting safety and privacy rules**.

**Thirdly, RPAS companies** using drones are also encouraged to enact codes **by adopting guidelines and show the public that they are aware of their obligations and follow best practices issued by privacy experts**. This will not only “re-assure those whose information is being captured but also inspire wider public trust and confidence”<sup>111</sup> in the use of RPAS, but it will also save companies time and money (no fines as they respect rules) and “contribute to the efficient deployment and operation”<sup>112</sup> of RPAS. Such advantages have been observed by Jeff Bezos, the CEO of Amazon, during Amazon's recent announcement that its e-commerce company plans to self-regulate their drones' uses. For instance, Bezos has committed Amazon to only use operators who have “completed training on the normal, abnormal, and emergency procedures in specific details and demonstrated proficiency with the sUAS being operated. Operators and observers will be in constant contact and if contact is broken between them, or if either individual spots a safety risk, the

---

<sup>110</sup> Adler, Jim, “When Self-Regulation Works, Your Privacy Is In Good Hands”, *Truste Blog* 2012, <http://www.truste.com/blog/2012/07/27/when-self-regulation-works-your-privacy-is-in-good-hands/#sthash.LuFPCRoK.dpuf>

<sup>111</sup> UK Information Commissioner's Office, “CCTV code of practice – Draft for consultation 2014”, 2014, [http://ico.org.uk/about\\_us/consultations/~/\\_media/documents/library/Data\\_Protection/Research\\_and\\_reports/draft-cctv-cop.pdf](http://ico.org.uk/about_us/consultations/~/_media/documents/library/Data_Protection/Research_and_reports/draft-cctv-cop.pdf)

<sup>112</sup> Ibid.

operator will immediately conclude the flight”.<sup>113</sup> Although this statement appears to deal only with safety standards, we could foresee its relation to a situation where only operators who have completed training related to privacy risks and safeguards are hired.

Thirdly, it is apparent that **among the different RPAS risks we have highlighted some of them, such as voyeurism, chilling effect and discriminatory targeting, will not be well addressed by state laws as they are more a matter of ethics and morals.** We think that private users such as hobbyists are not subject to the data protection framework. The benefit of developing codes of conduct is that they outline specific practices that are acceptable and unacceptable, based on previously gathered, expert information. Furthermore, such codes of conduct may provide a combination of safety rules, ethical values, privacy and data protection rules and may easily be accompanied of enforcement mechanisms or rules having a deterrent effect. For instance, a RPAS hobbyist club could enact a code of conduct that prohibits a hobbyist from processing personal information about individuals and/ or equipping its drone with thermal and infrared cameras. In the code, they could enshrine a rule stipulating, “any operator undertakes himself/herself to not use their domestic RPAS in contrariety with this code of conduct otherwise in case of breach of such rule they will be excluded from the club”.

Finally, in the area of **surveillance and law enforcement**, we have seen in the previous chapter that progress needs to be made to better address the new challenges posed by the emerging technologies. While we have up until now encouraged Member States to enact and revise regulations in this area, we share the idea issued by the EGE that “a more process oriented approach might be start with self-regulatory measures” as well.<sup>114</sup> **The UK Code of Conduct on CCTV systems is an example that the European Union and Member States should promote among the supervisory authorities and inside law enforcement bodies.**

### 11.3.6 Voluntary solution - Privacy Certification Schemes

#### *Concept*

In e-commerce, area where Privacy Seals are born, Privacy Seals (or certification schemes) are defined as “*voluntary privacy measures adopted as a self-regulatory initiative to promote consumer trust and confidence in e-commerce*”.<sup>115</sup> They enable organisations to demonstrate respect for privacy and develop a trustworthy image.<sup>116</sup> These trust marks are issued by an independent third party certifying the compliance of the products or services of an organisation (manufacturers and vendors) with European regulations on privacy and data security. For instance, TRUSTe<sup>117</sup> and EuroPriSe<sup>118</sup> are independent certification body providing such privacy seals.

---

<sup>113</sup> Mc Neal, Gregory, “Six Things You Should Know About Amazon's Drones”, *Forbes*, 2014, <http://www.forbes.com/sites/gregorymccneal/2014/07/11/six-things-you-need-to-know-about-amazons-drones/>

<sup>114</sup> The European Group On Ethics In Science And New Technologies, “Opinion No. 28 - Ethics Of Security And Surveillance Technologies, Brussels, 20.05.2014, p. 59.

<sup>115</sup> European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee of the Regions, A European Consumer Agenda - Boosting confidence and Growth SWD (2012) 132 final Brussels, 22.05.2012.

<sup>116</sup> European Commission, EU Privacy seals project - Inventory and analysis of privacy certification schemes Final Report Study Deliverable 1.4, 2013, <http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf>

<sup>117</sup> TRUSTe, <http://www.truste.com/>

<sup>118</sup> EuroPriSe, <https://www.european-privacy-seal.eu/EPS-en/About-EuroPriSe>

This important privacy protection mechanism has been recognised by governments, industries and public communities at the international, European and national levels.<sup>119</sup> Although we cannot find any reference in the current Directive 95/46/EC to privacy seals, the proposed General Data Protection Regulation contains specific provisions relevant to certification, data protection seals, and marks. In Article 39, the future regulation calls for “*the establishment of data protection certification mechanisms and of data protection seals and marks, as a means of enabling data subjects to assess the level of data protection provided by controllers and processors*”.<sup>120</sup> Further it also states “*the Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks*”.<sup>121</sup> Moreover, through amendments the European Parliament introduces a call for “standardized icon-based representations”.<sup>122</sup> The European Union Agency for Network and Information Security explains this amendment 51 by the fact that there is a need for reliable and verifiable possibilities to assess the seals and marks used.<sup>123</sup> Therefore, the European Institutions seems also calling for the creation of uniform standards which would apply to privacy seals at a European level.

#### *Privacy Seals in e-Commerce, in Cloud Computing, PETs, etc.*

Today, privacy certification schemes are particularly used for certifying e-commerce and Cloud Web sites. However, the European Commission has recently encouraged the adoption of this instrument in the framework of other technologies as it stated in its Communication on privacy-enhancing technologies (PETs) that “privacy seals as they facilitate consumers’ informed choice are also a mean for encouraging consumers to use privacy enhancing technologies (PETs)”.<sup>124</sup>

---

<sup>119</sup> European Commission, EU Privacy seals project - Inventory and analysis of privacy certification schemes Final Report Study Deliverable 1.4, 2013, <http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf>; Rodrigues, Rowena, David Wright and Kush Wadhwa, “Developing a privacy seal scheme (that works)” *International Data Privacy Law*, Vol. 3, Issue 2, 2013, pp. 100-116; Bennett, Colin J., and Charles D. Raab, “The Governance of Privacy: Policy Instruments in Global Perspective”, *MIT Press*, 2006, p. 122; Miyazaki, A., and S Krishnamurthy, “Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions”, *Journal of Consumer Affairs*, Vol. 36, No. 1, 2002, p. 28; Cline, Jay, “Computer World: Web Site Privacy Seals: Are they worth it?”, 2003, <http://www.computerworld.com/article/2569776/e-commerce/web-site-privacy-seals--are-they-worth-it-.html>

<sup>120</sup> European Parliament, The legislative resolution of 12 March 2014 on the 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)0011 – C7-0025/2012 – 2012/0011(COD)), Article 39.

<sup>121</sup> Ibid.

<sup>122</sup> European Union Agency for Network and Information Security, Opinion On the security, privacy and usability of online seals – An overview, 2013.

<sup>123</sup> “*In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms, data protection seals and marks should be encouraged, allowing data subjects to quickly, reliably and verifiably assess the level of data protection of relevant products and services.*” Draft European Parliament Legislative Resolution on the 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), Article 51 and European Union Agency for Network and Information Security, Opinion on the security, privacy and usability of online seals – An overview, 2013.

<sup>124</sup> European Commission, Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), COM/2007/0228 final, Brussels, 02.05.2007.

In different sectors, privacy seals schemes have already proved to have some pros and cons. The study of its benefits has been made in an EC-funded Privacy seals project. The found the following:

*From the regulator's perspective*, privacy seal schemes may help reduce the regulatory and enforcement burden –meaning less need for regulation (greater regulation entails greater legal compliance and enforcement costs) and greater flexibility. Privacy seal schemes have the capacity to foster a respect for legal and industry standards that lessens the need to increase legal regulation which comes with its own costs. *From the industry's perspective*, privacy seals promote certified entities, build consumer trust and confidence and bring market advantages. Privacy certification helps organisations demonstrate their privacy values and commitments. *From the community perspective*, privacy seals help consumers, users and the general public make quick judgements about an organisation's privacy and data protection policies and practices.<sup>125</sup>

However, if “privacy seals” have been recognised aside the government regulations as a leading force pushing for more privacy disclosures<sup>126</sup>, privacy scholars have also enlightened the weaknesses of the existing privacy seals schemes<sup>127</sup>. We observed that when privacy specialists speak about privacy seals, they face three similar concerns. Firstly, there is real lack of standardisation. “Although trust mark seals all appear similar, the level of privacy protection varies a great deal. Some seals are backed by detailed standards and independent audits. Other seals are provided with no requirements or checks (other than payment)”<sup>128</sup>, states Chris Connolly, a well-known privacy advocate. ENISA, the European Union Agency for Network and Information Security, goes even stronger when it stipulates in its report on privacy seals that “The trustmark sector is completely unregulated and there are no published standards or even basic guidelines for running a trustmark service. Standardisation of OSPS will be important to make them easily recognisable and correctly understood. Standardisation bodies should also define standards for trustworthy OSPS”.<sup>129</sup> Secondly, we observe a lack of awareness: “One of the main problems encountered during the research related to the availability of information.”<sup>130</sup>, explains the EU project on Privacy Seals. Therefore, many

---

<sup>125</sup> European Commission, EU Privacy seals project - Inventory and analysis of privacy certification schemes Final Report Study Deliverable 1.4, 2013, <http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf>

<sup>126</sup> Dr. Bhasin, Madan Lal, “Guarding Online Privacy: Privacy Seals And Government Regulations”, *European Journal of Business and Social Sciences*, Vol. 1, No. 9, December 2012, pp. 1-20.

<sup>127</sup> European Union Agency for Network and Information Security, On the security, privacy and usability of online seals – An overview, 2013; European Commission, EU Privacy seals project - Inventory and analysis of privacy certification schemes Final Report Study Deliverable 1.4, 2013.

<http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf>; Cui, Jing, “Assurance Seals: Security and Privacy Seals”, 2014. <http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626%20Assurance%20Seals%20J%20Cui.pdf>;

Connolly, Chris, *Trustmark Schemes Struggle to Protect Privacy*, Galexia, Australia, 2008 and Iacovos Kirlappos, M. Angela Sasse and Nigel Harvey, “Why Trust Seals Don’t Work: A study of user perceptions and behavior”, in, Stefan Katzenbeisser, Edgar Weippl, L. Jean Camp, Melanie Volkamer, Mike Reiter, Xinwen Zhang (Eds.), *Trust and Trustworthy Computing – 5th International Conference Vienna*, Austria, June 13-15, 2012.

<sup>128</sup> Connolly, Chris, *Trustmark Schemes Struggle to Protect Privacy*, Galexia, Australia, 2008.

European Union Agency for Network and Information Security, Opinion on the security, privacy and usability of online seals – An overview, 2013.

<sup>130</sup> European Commission, EU Privacy seals project - Inventory and analysis of privacy certification schemes Final Report Study Deliverable 1.4, 2013, <http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf>

users are not aware of the existence of certification schemes.<sup>131</sup> In this regard, ENISA and Jing Cui call for institutions and business provide “educational material to spread knowledge of the existence and meaning of these certification schemes”.<sup>132</sup> So customers are educated about the seals and the return-on- investment (ROI) in the seals can be maximised.<sup>133</sup> Finally, we found a lack of enforcement. Today there are too many businesses which, after obtaining a seal, do not continue to pass predesigned monitoring tests on an ongoing basis. Therefore, in these cases there is no guarantee that a security breach would not occur in the future.

#### *Privacy Seals Scheme in the context of data processed by civil drones*

Using privacy scheme in the context of RPAS technology could be seen as **an interesting way to implement the data protection law and to reward commercial operators for their compliance**. Indeed, we could imagine that DPAs grant companies and professionals a privacy certificate after they have implemented the requirements and rights of the data protection legislation. For instance, these **privacy seals could be granted by privacy specialists to RPAS companies which have hire their services for carrying out a PIA**. We can also relate privacy seal to the prior-checking conducted by DPAs. For instance, **after having carry out a priori-checking DPAs could grant companies with a privacy seal when they prove having adopted the additional safeguards required by the DPA**. By doing such DPA will not only be able to exercise an effective control on RPAS operators but also will reward compliant operators as granted with such certificate they will gain the trust of their customers and the general public.

We could even go further by requiring that the CAAs check before each operation that drones operators hold an updated privacy certification. For example, let’s come back to the Real Estate scenario in which the Real Estate Company has collected personal image via a drone in a residential area for making a video showcasing a home for sale. In this context we observed that such use has not respected the proportionality principle, the data minimisation principle and, moreover, if the video is disclosed, there is violation of the transparency principle because individuals are not informed that their data have been collected. This is an issue of implementation and enforcement. However, by linking the privacy certificate to the licence, Real Estate Company will not have other choice than complying with the data protection principles to obtain the privacy certification scheme. Otherwise, the CAA will remove the licence of the drone operator.

#### *11.3.7 Usage restrictions*

##### *Concept*

In the context of technologies, a use restriction is a limitation on the way that a technology can be used. This use restriction may be used to limit the use of a specific technology to a certain type of *person*, to certain *purposes*, to certain *environment*, or based on certain *modalities*. For example, a law which restricts the use of ANPR by law enforcement authorities is a restriction on the use regarding to the person which use it. However, a rule

---

<sup>131</sup>European Union Agency for Network and Information Security, Opinion on the security, privacy and usability of online seals – An overview, 2013.

<sup>132</sup> Ibid.

<sup>133</sup> Cui, Jing, “Assurance Seals: Security and Privacy Seals”, 2014.

<http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626%20Assurance%20Seals%20J%20Cui.pdf>

which prohibits intercepting telecommunications without a warrant is a use restriction based on a specific modality/requirement. These usage restrictions are generally imposed by law but there also exists certain organisations which self-restrict their uses in order to gain the trust of the public and consumers. For example, a hospital could have as internal policy that CCTV systems can only be installed in the parking area but not inside the building.

These usage restrictions have for main benefits to prevent security, privacy and ethical risks and to reassure the public.

#### *Use restrictions in the area of visual surveillance*

As examined in the Chapter 5, the use of visual surveillance is often restricted in national regimes of Member States either by state regulation or by soft laws (guidelines, codes of conducts) adopted by the national DPAs. As a reminder, we have seen in Belgium that the Camera Act 2007 restrict the use of mobile camera to law enforcement bodies (restriction use % person) for monitoring great gatherings (restriction use related to purposes) in the context of a non-permanent operation (use restriction related to modalities).<sup>134</sup> Another example would be the factsheets on surveillance issued by the France DPA (CNIL).<sup>135</sup> Through these factsheets, we have seen that monitoring on public places is reserved to public bodies (restriction use related to the person) for the prevention of terrorism attack and for the security of persons and goods (restriction use related to purpose) after an authorisation of the Prefect (restriction use related to modalities).

#### *Usage restrictions in the context of RPAS technology*

In the context of civilian drones, imposing or suggesting usage restrictions seems to be a simple and logical way to regulate certain RPAS aspects and reduce certain privacy, data protection and ethical risks posed by the technology. Usage restrictions could be used to limit RPAS uses to certain type of operators, certain applications (purpose of flight), certain equipment, or by requiring certain requirements/modalities prior the flight. For instance, a hobbyist club could restrict RPAS hobbyists members to equip their drones with sophisticated visual payload.

##### a) Commercial application

Firstly, it is important to note that at the state level, the European Directive on Free services and goods is prohibited from putting a **usage restriction on the sales** of goods including RPAS. However, nothing prevents companies from self-restricting their sales of certain type of drones.

Second, usage restrictions could also be developed **to limit the use of RPAS to certain purposes** like profiling. In Chapter 3 we emphasised how profiling activities may result in privacy threats for individuals. Several Member States contain profiling restrictions in their data protection act like prior-checking but it is not a harmonised area. The GDPR proposal of the Parliament suggests adding a right to object for individual to profiling activities but this Act is still in negotiation. Therefore, **usage restrictions on profiling activities** could be developed by RPAS-using organisations in code of conducts or guidelines. By adopting such use restrictions, RPAS organisations will reduce risks related to profiling activities

---

<sup>134</sup> Belgium Parliament, Camera Surveillance Act, 21.03.2007.

<sup>135</sup> CNIL, Factsheets on video surveillance, 2014, <http://www.cnil.fr/les-themes/videosurveillance>

(discriminatory targeting, security breach, dehumanisation, etc.) while their commercial companies member will gain trust of the public and regulators.

Thirdly, if state law cannot prohibit the sale of goods like drones, they can **restrict certain type of operators from purchasing intrusive or unsafe payloads**. RPAS technology is evolving and in parallel equipment becomes also more intrusive and sophisticated like behaviour recognition camera, biometric recognition etc. Furthermore, we observe a “drone it-yourself” trend among private individuals. This trend consists to make and equip itself a drone with original payloads not always initially designed for RPAS. Imagine now an employer which decides to launch a drone equipped with a behaviour recognition camera to monitor its employees on a building site. European should not have to worry to be scrutinised permanently by drones. Therefore, **usage restrictions regarding to certain intrusive technologic payloads like biometric and behaviour detection systems should be set up**. Regarding to this example, it is noteworthy that if existing CCTV law do not already prohibit use of mobile camera to monitor employees, such usage restriction should be set up.

#### **11.4 Concluding remarks**

This present chapter was designed to examine what kind of policy regulations should be adopted to address the remaining legal gaps and implementation difficulties raised in the two previous chapters. Firstly, we examine potential legislative solutions to enact. In this regard, we have concluded that the few remaining gaps figuring in the current Directive, which applies to commercial operators, will be mitigated by the adoption of the Regulation proposal. However, regarding State agencies we have concluded that at the national level current legislation applying to them must be revised and updated in order to adequately address the numerous risks raised by the usage of drones in this sector. Secondly, complementary measures have been studied. Three technological solutions - PbD, PIA, SIA- and four voluntary solutions - Privacy Audit, Self-regulations, Privacy seals scheme, Usage restrictions – have been deeply analysed in order to determine if they should be adopted to reduce risks and implementation concerns. Whereas this second section shows that all of them are relevant in the context of drones, we demonstrated that PIA, PbD, Self-regulations and Privacy Seals are particularly well-suited instruments to address the specific features and risks in RPAS applications. The analysis stemming from these both sections has then been used for issuing policy recommendations figuring in Chapter 13.

## **12 RPAS REGULATION AND CIVIL AVIATION AUTHORITIES**

Eleven EU Member States have already adopted national regulations on the commercial use of RPAS under 150 kg: Austria, the Czech Republic, Denmark, France, Germany, Ireland, Italy, Poland, Romania, Sweden and the United Kingdom. Belgium, Finland, Lithuania, the Netherlands and Slovenia do not yet have regulations that explicitly provide for the commercial use of RPAS but do permit some flights on a case-by-case basis, as does Norway, which is not a Member States but is formally associated with EU policy development in many areas. Some of these states, in particular Belgium, plan new laws or Directives to regulate the commercial use of UAS. An overview of the situation in each of these Member States is provided in Annex B to this report, below. The purpose of this chapter is to determine whether Civil Aviation Authorities could be mobilised to act as regulators for privacy, data protection and ethical issues with respect to RPAS by using their current frameworks as indicators of the types of issues they are examining.

The analysis finds that some CAAs are including a reference to privacy and data protection rules that must be followed by RPAS operators. Specifically, the French, German, Norwegian and UK regulations appear to contain dedicated provisions, but these are primarily related to visual photography or surveillance. This sort of formulation is inadequate to protect privacy and data protection, as it does not account for the other payloads that might also raise risks.

However, most of the CAAs discussed in Annex B require RPAS operators to be licenced, registered and/or apply for permission to operate RPAS for civil purposes. As such, there is some scope for inserting issues related to privacy, data protection and ethics into these requirements. The stakeholder analysis in Chapter 6 clearly demonstrates that CAAs do not feel that they have adequate knowledge and expertise to evaluate or enforce privacy and data protection issues. Nevertheless, this chapter argues that it is possible for CAAs to act as civil and commercial RPAS gatekeepers, and to ensure that some sort of privacy and data protection risk assessment has taken place much as they ensure pilots have licenses.

### **12.1 Privacy and data protection issues addressed**

As noted above, some CAAs do have specific provisions related to privacy and data protection in their regulation of civil RPAS. In Germany, RPAS operators have to apply for a permit to fly, which must be accompanied by a declaration that the operations will not violate the individual rights of persons in Germany. As such, any RPAS which collects data that might refer to people, must consider how their operations might impact members of the public, and certify that fundamental rights will be adequately protected. The UK also has a specific provision related to “small unmanned surveillance aircraft”, which are defined as small RPAS equipped to undertake any form of surveillance or data acquisition. For these missions, permission is required from the CAA to fly over or within 150 metres of any congested area; over or within 150 metres of an organised open-air assembly of more than 1,000 persons; within 50 metres of any vessel, vehicle or structure which is not under the control of the person in charge of the aircraft; or within 50 metres of any person. Both the German and UK provisions are strengthened by the fact that they are technology neutral, and not specific to particular types of payloads or data collection. Additionally, in the UK both the Information Commissioner’s Office (the UK DPA) and the Civil Aviation Authority’s websites cross-reference one another, to assist RPAS operators in acquiring useful information about these issues.

In addition to these general provisions, some Civil Aviation Authorities have specific requirements with respect to visual photography from the air. For example, in Norway, anyone wishing to undertake missions involving aerial photography must apply for permission to the National Security Authority. In France, there is a special category of RPAS operations that include activities such as photography, observation and aerial surveys and these require a special declaration to the DGAC at least two weeks before the intended operation. RPAS equipped with non-visual data collection devices (thermal images, radar, etc.) only require a general authorisation. Such requirements certainly encourage RPAS operators to consider how their use of visual photography might raise privacy and data risks and obligations. However, a focus on visual payloads only makes this requirement inadequate to address the other payloads and data collection devices that could raise risks to privacy, data protection and ethics, e.g., the collection of thermal images or location data. As such, while the spirit of the regulations are useful, they are too narrow to address all of the potential and emerging risks to privacy, data protection and ethics.

Despite their differences, all of these provisions represent good practice as they encourage operators to consider how their operations might impact members of the public. Norway and France stand out from the other CAAs as having specific provisions related to privacy and data protection, but their focus on a particular technology (visual surveillance) means that they will become increasingly inadequate as RPAS operations expand beyond visual photography. Nevertheless, they are useful in the sense that they raise a “red flag” in relation to these particular uses of RPAS that are likely to infringe on privacy, data protection and ethics. In contrast, the technology neutral provisions in the German and British regulations can apply to all different types of payloads and data collection practices. While these provisions might be less clear for RPAS operators and do not indicate such “red flags”, they make clear that RPAS operators must consider their liability in relation to these issues. In order to assist in providing this clarity, CAAs should follow the UK and Belgian examples and work closely with their national DPAs in order to provide more clarity to RPAS operators.

## 12.2 General RPAS flight requirements

While the other RPAS regulations do not specifically mention issues related to privacy, data protection and ethics, there are a number of other requirements that must be met by RPAS operators. In many cases, these requirements provide an opportunity for CAAs to use their existing oversight mechanisms to ensure that privacy and data protection issues are considered. Specifically, many require RPAS pilots to have licenses for specific devices or activities, most RPAS regulations require commercial RPAS to apply for a permit for aerial work and there are additional flight and registration requirements.

In addition to aerial work permits, some CAAs require operators of RPAS, and particularly medium sized RPAS, to obtain a license to pilot the aircraft or to have attended specific training courses. The most strict requirement is in Italy, where pilots must demonstrate sufficient knowledge to pilot an RPAS, which can be demonstrated by the possession of a civil pilot’s license or of an Italian VDS (pleasure flying) pilot license. In addition, all pilots operating in Italy must have attended a specific training program for the RPAS. In the UK, all commercial RPAV pilots must have a Basic National UAS Certificate (BNUC).<sup>1</sup> (The 2014

---

<sup>1</sup> “Are UAV's Legal?”, *UnmannedTech.co.uk*, no date. <http://www.unmannedtech.co.uk/regulations.html>

Belgian Royal Decree on RPAS will likely include a requirement that RPAS pilots or operators be licensed or certified.<sup>2)</sup> Other countries, including France, Denmark and Austria require pilots operating in populated areas to have a specific license. In France, a private aeroplane, helicopter or glider licence (PPL(A) or PPL(H)) is required, the most restrictive in Denmark, where operators must hold a commercial pilot license to operate in populated areas. In addition to needing a license in populated areas, operators in Austria also need a license to operate an RPAS over 5kg, which means that many medium sized RPAS, such as those used by professional, corporate or commercial users would require a pilot qualification.<sup>3</sup> As noted above, while none of these requirements specifically mention pilots needing training in privacy, data protection or ethics, such training could be added to the curriculums of these training courses (if they are not already present). As such, the requirement that RPAS operators have a license could function as a way to ensure that they have some training in the risks their operations might pose to individuals on the ground, and that they are trained in ways to identify and mitigate those risks. In this way, CAAs could indirectly regulate pilots' expertise in these issues.

In addition to pilot licensing, many of the CAAs examined in Annex B require an aerial work permit for commercial RPAS operations. While in Sweden, Norway and Finland permission is required for all RPAS flights, the Czech Republic and Ireland have a blanket requirement that a specific permit is required for aerial work. However, in Denmark, this aerial work permit application for medium sized aircraft (7-150kg) operating in line of sight must include a description of the RPAS' intended activities. In Germany, work permit applications must also include a brief description of the planned operation as well as permission from the landowner or the local Council, a sketch of the flight area and the estimated time of flight, and systems weighing 5 kg to 25 kg require individual permits for every flight. In both Italy and the UK, work permits are specifically required for operations taking place near people, property or infrastructure.

While none of these work permit requirements specifically mention privacy, data protection or ethics, they do offer an existing infrastructure in which RPAS operations are evaluated. Where appropriate, they could be adapted to require those applying for aerial work permits to describe the privacy, data protection or ethical risk mitigation measures that they have used to minimise such potential impacts of their operations. In this scenario, the CAAs would not necessarily have to evaluate these measures, they would simply certify that they have been considered and included and/or refer complex cases to the national DPAs. In addition, some aspects of the existing systems could also be extended to assist RPAS operators in engaging in good practice in relation to specific privacy and data protection risk mitigation measures. Specifically, the German system could be easily adapted to enable better transparency. The required description of the planned operation and the information about the flight area and time could be made publicly available to enable members of the public to find out what the RPAS is doing and who is operating it. As such, the requirement to obtain an aerial work permit could assist in reducing risks associated with privacy, data protection and ethics.

---

<sup>2</sup> Billen, Erika, "Belgian approach related to remotely piloted aircraft systems (RPAS) and their insertion into non-segregated airspace", *Belgian Civil Aviation Authority*, Feluy, 20 November 2013.

[http://eo.belspo.be/Docs/Resources/Presentations/beodays2013/402\\_Belgian\\_Approach\\_UAV.pdf](http://eo.belspo.be/Docs/Resources/Presentations/beodays2013/402_Belgian_Approach_UAV.pdf)

<sup>3</sup> AAI UAS Working Group, "NEW Austrian regulation for UAS Class 1 (VLOS): AAI Fact Sheet", no date. [https://www.aaig.at/wp-content/uploads/2014AAI\\_Factsheet\\_UAS\\_Class1\\_VLOS\\_AustrianRegulation\\_OverviewEnglish.pdf](https://www.aaig.at/wp-content/uploads/2014AAI_Factsheet_UAS_Class1_VLOS_AustrianRegulation_OverviewEnglish.pdf)

Further flight and oversight requirements, such as risk assessment, line-of-sight obligations and registration can also assist in indirectly regulating the privacy, data protection and ethical issues associated with RPAS. Specifically, although the Netherlands does not allow RPAS outside of rural areas, they do require pilots to conduct a risk assessment for each flight. While this risk assessment likely focuses on safety and does not mention anything about impacts on fundamental rights, it could be used as an existing framework through which issues related to privacy, data protection and ethics can be inserted. Many other countries (AU, CZ, DE, DK, IRL, SE) also stipulate that RPAS must be flown within the operator's line of sight. This also assists transparency, where people on the ground are much more likely to be able to identify who is operating the RPAS and to directly raise questions or issues with the operator or team. Finally, some Civil Aviation Authorities require commercial RPAS operators or RPAS themselves to be registered with their national CAA. In the UK and Ireland, all RPAS with an operating mass greater than 20kg must be registered. In Austria, the Czech Republic and France, only commercial users or uses of RPAS need to be registered. However, the Czech CAA also requires all RPAS being used for commercial purposes to have an ID label and registration mark.<sup>4</sup> (The 2014 Belgian Royal Decree on RPAS will also likely include a stipulation that RPAS must be registered.<sup>5</sup>) In practice, these requirements to register RPAS and also to ensure that RPAS have identifying marks or labels also contribute to transparency. If this information is held by the CAAs and made available to the public upon request, members of the public would be better informed about who owns and operates RPAS and the purpose for which it is being used. It also provides an existing infrastructure upon which a pan-European RPAS database can be built, and which would represent a powerful transparency tool.

### 12.3 Summary

This analysis finds that there are a number of elements of existing CAA RPAS regulations that could be mobilised, built upon and expanded to enable CAAs to act as indirect regulators of privacy, data protection and ethical issues. It is clear from the CAA consultation that aviation authorities do not feel that they have adequate competence in these issues, and that their primary focus is on safety and liability. Rather it is DPAs that have this competence and expertise. Nevertheless, CAAs are the natural gatekeepers for the commercial RPAS industry. As such, there are ways in which CAAs and DPAs can collaborate to ensure that citizens' fundamental rights are protected. Pilot qualification, certification and licensing courses could include information fed from DPAs about identifying, recognising and reducing risks associated with privacy, data protection and ethics. Specifically, it could include information or a template for conducting a privacy impact assessment (PIA) of RPAS operations. Similarly, requirements to register RPAS and for them to have an identifying mark would also aid transparency, accountability and rights to access of personal data by enabling RPAS operators to be identifiable. Requirements to obtain an aerial work permit could also include a requirement to undertake a privacy impact assessment of any activities that may collect information about people, either purposely or inadvertently. While CAAs would not be in a position to evaluate the quality of that PIA, they could ensure that it has been completed and refer special cases to DPAs.

---

<sup>4</sup> ULTRA Consortium, "Identification of gaps and new/modified regulations within the existing regulatory framework", 2013, p. 39.

<http://ultraconsortium.eu/index.php/deliverable?download=33:ultra-wp1-indra-d1-1-reg-gaps-pu-v3-0>

<sup>5</sup> Billen, op. cit., 2013.

Finally, the regulations that are in place, or any regulations that may be put into place in the future, need to be technology neutral and consider issues in addition to visual surveillance. While the addition of requirements to consider the privacy and data protection issues associated with visual photography are useful and highlight missions that might specifically include risks, they may inadvertently send a message that all other flights do not pose such risks. This is problematic as there are many RPAS missions and capabilities that do not include visual photography but which raise privacy, data protection and ethical issues. Instead, all missions that may include information about people should be evaluated, regardless of the technology utilised.

In conclusion, the current RPAS CAA regulations are certainly inadequate to address privacy, data protection and ethical issues. However, there is significant scope to amend and expand existing regulations to enable CAAs to act as gatekeepers for the RPAS industry and indirectly regulate these issues. This will require CAAs to work closely with DPAs to ensure that both safety and privacy, data protection and ethical issues are addressed by future RPAS regulatory frameworks.

## **B POLICY RECOMMENDATIONS FOR PRIVACY AND DATA PROTECTION ISSUES IN CIVIL RPAS**

### **13.1 Introduction**

The research project into the potential privacy, data protection and ethical issues associated with remotely piloted aircraft systems (RPAS) culminates in a series of recommendations to assist European policy-makers and industry in ensuring that the civil deployment of RPAS respects these issues. As such, this chapter builds on the research conducted in the RPAS project to identify recommendations for European and national policy-makers, Data Protection Authorities, Civil Aviation Authorities and industry to assist in this endeavour. These are primarily based on the Chapter 9 and 10 findings that the existing legal framework is largely adequate to address the privacy, data protection and ethical issues raised by civil RPAS. Although some gaps remain, it is primarily education about and enforcement of this legal framework that are lacking.

These recommendations also stem from two technical and legal premises. First, technologically speaking, RPAS are complex machines with diverse capabilities and a multitude of potential applications in a dynamic sector. Therefore, an over-arching framework for their regulation by a centralised, European authority would be necessarily inadequate and almost immediately obsolete. Second, the recommendations are built on the finding that definitions of personal data vary between different Member States, between different experts and certainly between different contexts of data collection and processing. Furthermore, the relationship between RPAS and the protection of privacy and personal data is best analysed using notions of risk, rather than applicability. For example, the collection of blurry images in one context may result in a negligible risk to privacy and data protection, while in another context they might represent a medium or high risk. Consider the distinction between the collection of blurry images of a person in their yard in the infrastructure inspection scenario with the collection of blurry images in the image bank scenario. One represents a medium risk to data protection, whilst the other represents a very low risk, but in both cases, data protection laws are applicable. Furthermore, risks to privacy are engendered whether an RPAS is collecting personal data or not, as privacy can be infringed simply by feeling discomfort with the presence of an RPAS. Given this complex interaction, these recommendations are broadly focused on two key ideas – providing recommendations on how the RPAS industry and other stakeholders might minimise these risks and providing tools and expertise to ensure that these risks are identified early and do not represent an additional “cost” to the RPAS industry, regulators or members of the public.

This issue of cost is particularly significant as the current state of affairs is unsustainable. First, the research in Chapter 6 has found that many RPAS operators are probably collecting and processing personal data. As such, they have clear obligations under current European and national laws as well as the forthcoming General Data Protection Regulation. However, many RPAS industry representatives do not appear to be aware of these obligations and are consequently not meeting them. This places both the RPAS industry, European and national policy-makers and members of the public at risk. Industry representatives are leaving themselves open to liability and penalties that could negatively impact the sector. Citizens are at risk of serious infringement of their fundamental rights. European and national policy-makers, as well as the RPAS industry, are leaving themselves open to a loss of trust by the public as a result of these infringements, which can negatively impact those stakeholders. As

such, the current situation is associated with clear and serious vulnerabilities for all of the stakeholders involved.

These policy recommendations focus on action items and soft law measures, rather than specific changes to European and national legislation, given the issues associated with risk and the need to ensure that any measures are technologically neutral to account for RPAS heterogeneity. In particular, they are organised under five main headings:

- Industry-specific recommendations for reducing risk
- Raising awareness of privacy and data protection requirements in the RPAS industry
- Enacting information and transparency protocols
- Conducting mandatory assessments of privacy and data protection issues for each type of operation (privacy impact assessments)
- Identifying stakeholders to monitor good practice in privacy and data protection.

Each of the key stakeholders involved in the RPAS eco-system has roles to play to meet these obligations. As such, under each of these broad recommendations, we include information specific to different stakeholder types. Broadly speaking, the different stakeholders involved in the RPAS eco-system have relatively stable roles and obligations across these recommendations. For example, the implementation of most of these recommendations involves the RPAS industry, and specifically RPAS industry associations, working closely together with Data Protection Authorities to agree common strategies to ensure privacy and data protection risks are mitigated. Yet, these organisations must be supported in this collaboration, which is the role of the European Commission and national policy-makers. Finally, it often falls on Civil Aviation Authorities to provide some form of check and certification that appropriate procedures have been conducted.

Where possible, we provide suggested measures, options or steps to achieve each of these goals. Each of these policy recommendations, and their specific sub-recommendations, represents improved practice in meeting privacy and data protection requirements. Taken together, these measures provide a comprehensive, good-practice package that encourages responsible use of RPAS in civil applications.

## 13.2 Industry-specific recommendations

First, **RPAS manufacturers and operators need to be proactive in understanding how to minimise the amount of data they collect** in order to reduce their risks in relation to privacy and data protection. In relation to privacy, **it is essential for RPAS operators to enact information sharing practices** to provide members of the public with knowledge about the specific activities being undertaken by the RPAS. This is discussed in more detail in section 13.4 below, but RPAS operators need to be proactive about establishing this good practice. In relation to data protection, recommendations for reducing risks in relation primarily require RPAS operations not focused on people to consider the following data minimisation features:

1. Reduce the presence of people and their identifying objects (e.g., vehicles) at the site. Some RPAS operators have enacted this data minimisation feature by flying RPAS missions during workers' lunch breaks, or public holidays, or flying RPAS missions that do not require visual optics at night.
2. Only record images when absolutely necessary. This will ensure that if people do, inadvertently, appear on the footage, it is as infrequent as possible. Specifically,

consider not recording the whole flight – only press record once the RPAS is in place and stop recording immediately after the mission aspect of the flight is finished.

3. Enact privacy-by-design features, such as blurring of images, during data collection or immediately afterwards, to make people and their objects as anonymous as possible.
4. For sites that are visited frequently, inform people who may be captured on the footage what the RPAS is doing and provide relevant contact details to ensure that members of the public can exercise their rights to consent, access, rectification and erasure. Should an individual choose not to consent to their data potentially being collected, find a privacy-by-design feature that solves this problem. Otherwise, the mission may need to be cancelled.
5. Ensure that the data about or including people or their property is only utilised for the purpose for which it was originally collected and processed. For example, if an RPAS collects visual information for mapping a landscape, this footage should not be re-used to assist in a navigation application or for any other purpose not related to landscape mapping.
6. Ensure that the data collected is adequately secured. This may include considering both the types of hardware and software used in data collection, transfer, storage and processing to ensure that the data is not accessible to anyone but authorised persons.
7. Avoid storing unnecessary information about people or their property, and consider transferring such data to the clients without keeping a copy in order to reduce risks to privacy, personal data and ethics.
8. Where possible, RPAS operators should contractually establish whether they, or the client, have control over the “why” and “how” of processing activities, and are acting as the data controller, with all of the associated obligations.

Should an RPAS operator be asked to fly a mission that is focused on people or is very likely to collect personal data, RPAS operators should seek immediate legal advice before conducting the mission.

### 13.3 Raising awareness

The survey conducted with RPAS operators and manufacturers revealed that raising awareness of privacy and data protection is of key importance to ensure adequate protection of privacy, personal data and ethical values. Specifically, the survey revealed that many RPAS operators were not aware that they were collecting personal data. This is specifically related to images of people or vehicles captured “in the background” during inspections and other missions. Furthermore, the survey revealed that many RPAS operators and manufacturers reported a “basic” or “poor” understanding of European and national privacy and data protection regulations. This is not surprising, as most RPAS operators are not legal experts and require assistance in navigating these complex legal frameworks. In order to assist civil RPAS operators in bridging the gap between their understanding of privacy and data protection law and the data they collect, **RPAS operators need to be supported to better understand privacy and data protection obligations.** This will require at least two specific actions and commitments from many RPAS stakeholders.

Second, **the development of training courses and high-quality information materials for industry representatives needs to be supported.** These training courses should cover European privacy and data protection legislation, the Charter of Fundamental Rights of the European Union, the Data Protection Directive and the proposed General Data Protection Regulation (GDPR). Focusing the training on the GDPR, in particular, will ensure that RPAS

operators are prepared for the introduction of this legislation and that they are meeting the most robust requirements for the protection of personal data available – thus providing robust protection for members of the public. This training should focus on understanding what may be considered personal data in different contexts (potentially through the use of scenarios) as well as the data protection principles outlined in this report, including, but not limited to:

- Transparency
- Data minimisation
- Proportionality
- Purpose limitation
- Consent
- Accountability
- Data security
- Rights of access
- Rights of correction
- Rights of erasure
- Third country transfers.

These issues are specific to the European data protection framework, and they may need to be adapted to national requirements. The training could focus on how to conduct a privacy impact assessment (or a similar assessment) that would include meeting privacy and data protection requirements and reducing industry representatives' risk in relation to privacy and data protection. The training may also need to be offered in Member States and focus on the privacy and data protection requirements associated with those Member States. The training should also include lectures by experienced and established industry representatives who can provide good practice information in meeting these requirements whilst satisfying customer needs. These training courses could be offered in various European languages to ensure their reach and applicability to the largest possible population of RPAS operators.

The **European Commission** should support this action by supporting and providing space where RPAS stakeholders can interact. This could include workshops between industry, Data Protection Authorities and policy-makers, seminars and other events or even an online portal. The EC could also consider setting up a working group that meets regularly to ensure that progress is made in ironing out these issues rather than re-hashing the same debates. An important aspect of such stakeholder interaction will be the involvement of Civil Aviation Authorities in these processes.

The **European Commission** should also organise the construction of a one-stop information resource to assist RPAS operators in meeting obligations across EU Member States. In particular, this should include publication of informational materials on privacy and data protection in major European languages to assist RPAS operators operating across European borders to understand what these obligations are both at a European level, and in the Member States in which they are operating.

**Member States** should organise the construction their own reference materials, including codes of practice, related to privacy and data protection to ensure both local operators and operators from other Member States are adequately informed about national privacy and data protection obligations as well as other fundamental rights.

These information materials should be in local languages and cover issues associated with national rights to privacy, data protection legislation and other relevant laws (for example, CCTV legislation). In addition, these national materials should be fed to the EC central information resource to assist RPAS operators in other Member States interested in working in that national context.

**Industry stakeholders** need to be proactive to educate themselves and ensure that they are complying with European and national privacy and data protection laws as well as other relevant legislation. Although it is individual companies that are liable under these laws, industry associations have a clear role to play in raising awareness of these issues. Industry associations should organise training courses, produce information materials, again, including a code of practice, for their members and organise awareness-raising events, as responsible operators are likely to be engaged in such associations. Industry associations can also encourage Data Protection Authorities to produce materials that are useful for industry representatives in their individual countries to assist them in protecting privacy and other fundamental rights during RPAS operations. However, as mentioned above, RPAS manufacturers and operators themselves must be proactive, as they are ultimately liable if these rights are infringed.

**Data Protection Authorities** should recognise their role in the RPAS ecosystem and actively work with the RPAS industry to offer concrete advice that goes beyond legal jargon (for example, the aforementioned code of practice and, possibly, a PIA template). Most RPAS manufactures and operators do not have legal expertise. Furthermore, privacy and data protection laws are complex, context-dependent and intentionally broad in order to achieve technological neutrality. All of these characteristics leave RPAS operators vulnerable when they attempt to interpret these laws without expert help. DPAs should produce guidance materials in local languages to enable RPAS operators to adequately meet their obligations. Furthermore, these guidance materials should offer concrete advice, possibly based on common scenarios, to ensure that RPAS operators have actionable ideas to reduce risks in this area. Furthermore, a number of legal issues require further clarity from Data Protection Authorities.

- The relationship between data processors and data controllers. RPAS operators would commonly be understood as data processors and the clients, data controllers. However, if the RPAS operator is encouraged to take increasing responsibility for the collection of data and make decisions about that collection, then the operator may be understood as a joint controller with different and additional obligations. DPAs should assist in clarifying the positions of these different actors to ensure that liability is properly addressed.
- The applicability of the Directive and Member State data protection laws to the monitoring of visual images by commercial RPAS operators without recording, particularly where this monitoring is associated with flight operations rather than the specific commercial mission.
- The contexts in which indistinct images might be considered personal data.

**Civil Aviation Authorities** should also encourage RPAS operators to consider privacy and data protection issues when applying for permission to operate an RPAS for aerial work. While this could be through part of a certification process or some sort of risk assessment (discussed below), at the very least, CAAs should provide linkages to DPA

websites or other information materials to ensure that RPAS operators are aware of these obligations. Activities by the UK, French and Belgian CAAs provide useful examples here.

Second, in addition to having access to standardised information materials, the heterogeneity of RPAS capabilities and operations means that industry representatives may sometimes require tailored advice on issues related to privacy, data protection and other fundamental rights. As such, **opportunities should be developed for RPAS manufacturers and operators to ask specific privacy and data protection questions and receive tailored advice.** Providing space where RPAS operators can receive low-cost or free advice will lower entry barriers to the civil RPAS sector and ensure the protection of citizens' fundamental rights. Furthermore, involving industry associations and data protection authorities will ensure that RPAS operators receive consistent, high-quality advice from reputable sources.

The **European Commission** should support such a service, either through an online portal or forum through which different stakeholders can interact.

**Member States** should develop these opportunities by providing similar fora where industry, legal experts and DPAs can interact to provide such advice in local languages.

Finally, **Data Protection Authorities** must commit resources to such an endeavour to enable responsible RPAS operators who have specific concerns to receive understandable answers to enable them to reduce their risks in this area.

Providing support for such awareness-raising activities will facilitate responsible practices among reputable civil RPAS operators. They will be able to provide a high quality service and shield themselves and their customers from liability in respect of practices that breach data protection regulations. Furthermore, they will develop their profile in this field, including among members of the public, who are more likely to consent to additional RPAS deployments if they are satisfied that their rights are being adequately considered and protected.

### 13.4 Information and transparency protocols

A key element of ensuring public acceptance of RPAS is to educate members of the public about the activities RPAS are undertaking in the civil sphere and the types of data they are collecting. Such transparency is a requirement when collecting personal data and represents good practice in allaying concerns around privacy and ethics. Specifically, one of the privacy-invasive aspects of civil RPAS, even those that are not collecting data about people, is that members of the public do not know what the RPAS is being used for and may be concerned that it *is* collecting data about them. Consequently, greater awareness by members of the public about RPAS operators and operations will likely increase public acceptance of RPAS and enable the sector to grow. As such, **civil RPAS operators should be subject to information and transparency protocols**, to provide the public with this information. These transparency protocols could take a number of forms, and each would address obligations related to consent, accountability and rights of access to correction and erasure.

The first potential format involves **the development of a national or cross-national information resource to enable citizens to identify the missions and operators associated with individual RPAS**. With the highest functionality, this resource could function similar to the existing Flight Radar 24 system ([www.flightradar24.com](http://www.flightradar24.com)) and provide real-time information about RPAS flying overhead. This would require RPAS to carry mandatory, unique identifiers that would enable the RPAS to be tracked via GPS using a centralised system.<sup>1</sup> It would require a centralised database of RPAS and their unique identifiers and well as their operators and contact information. Such a system should be a robust transparency tool that would enable citizens to immediately identify the RPAS, the operator and the avenue through which they could find additional information. At a lower end of functionality, RPAS should be marked with mandatory identifiers (e.g., tail numbers or serial numbers) which could be matched to information in a centralised database.<sup>2</sup> The database should contain the contact details of the RPAS operator, and this information should be made available to members of the public on request. However, this second option requires members of the public to undertake significant labour to identify the appropriate CAA contacts as well as RPAS operator contacts. These systems would enable RPAS operators to meet requirements for transparency, accountability, rights of access, correction and erasure as well as foster public confidence in civil RPAS operation. In order to achieve such a system, different RPAS stakeholders would have to work together.

The **European Commission** should support a collaboration mechanism involving industry, Civil Aviation Authorities and technology experts to design the system of serial numbers, website and database and agree the specifications.

**European and national policy-makers** would have to work together to decide where the competence lies for creating such a system and how it would be funded. Ideally, it should be organised and constructed at the European level through the European Aviation Safety Authority with funding contributions from different Member States relative to their population of RPAS operators.

**Industry associations** should design and agree common standards for such an identification mechanism, including serial numbers, signals and GPS tracking capabilities.

**RPAS manufacturers** should include individual serial numbers on RPAS platforms, and participate in industry discussions as to standards and mechanisms for enabling GPS location.

**Civil Aviation Authorities** should participate in the development of these systems, and once standards are agreed, should require RPAS to include identification and tracking

---

<sup>1</sup> Such a system was suggested by the International Working Group on Data Protection in Telecommunications, *Working Paper on Privacy and Aerial Surveillance*, 54th Meeting, Berlin, 2-3 September 2013.

<sup>2</sup> Although the tracking of a moving or small drone would be very difficult using binoculars, such identifiers would improve transparency, and are essential in the event that an RPAS crashes.

technologies.

For RPAS that are being used regularly in fixed locations (e.g., patrol for infrastructure inspection or environmental protection), such transparency elements could include **signposts and/or information sheets in those locations**. The signposts could take two forms. One possibility is that RPAS industry associations could develop a graphic, similar to CCTV signs, indicating that an RPAS patrol is taking place and providing contact details for additional information. Another possibility is that the signpost could simply describe the operation and the data collected and provide contact details for more information. The first option would require the RPAS industry to launch their own awareness-raising campaign to familiarise members of the public with the graphic and what it means. While this would require an initial outlay of resources, such an icon could become a recognisable information tool and an inexpensive way for industry (particularly SMEs) to indicate RPAS missions. The second signpost option represents an opportunity to provide more detailed information (e.g., RPAS mission purpose, operator, type of data collected and contact details for additional information) and may provide an opportunity to allay public fears, particularly in situations where personal data is not being collected. Finally, information leaflets could provide the most detailed information, and for some complex missions, might be the most appropriate. In each case, the signposts or leaflets could be placed at the entrance to or perimeter of the site or area in which the RPAS may operate. Providing contact details for the organisation flying the RPAS mission is essential, as these details enable accountability and the exercise of rights to access, correction and erasure of personal data. Finally, they also allow individuals to opt out of having data collected by the RPAS (even inadvertently) by choosing not to enter the particular area.

**Information leaflets would be appropriate in locations where RPAS missions occur infrequently or on a one-time basis.** For example, where RPAS are being used to collect information for mapping purposes, the information sheet should detail when the mission would be occurring, what areas were likely to be captured by the filming, what specific data will be collected and where individuals can find out additional information. The leaflets should be distributed to homes, businesses and other organisations in the area that may be impacted, either via mass mailing or some other form of physical distribution. This would allow people to choose not to consent to the filming by removing themselves from the area during the time of filming. Furthermore, it should provide information about who is doing the filming, and the different options for accessing, correcting and erasing any personal data (including exercising data minimisation measures such as having their house blurred in the footage). The leaflet would also include information that would allow people to question the filming or contact a data protection or other authority if they had specific concerns. RPAS operations explicitly involving the collection of data for purposes such as marketing must abide by the additional regulations around mandatory opt-in requirements, etc., before undertaking such operations. However, in both cases, it is important to stress that these are suggestions, and RPAS operators should be encouraged to develop innovative means of providing transparency without additional burdens on individual organisations.

**Industry associations** should consider the development of a recognisable RPAS icon to communicate to members of the public that an RPAS operation may be taking place in a particular area. These associations should encourage their members to use this icon and provide associated mission information as frequently as possible, even when they

are not collecting data about persons. Finally, industry associations should encourage their members to suggest or trial innovative transparency tools that reduce burdens on organisations.

**RPAS operators** should commit to providing information (e.g., RPAS mission purpose, operator, type of data collected and contact details for additional information) to members of the public about RPAS operations. This is a legal obligation when personal data may be collected, and it can assist in providing long-term support for the RPAS industry by allaying public fears.

**Data Protection Authorities** should offer advice as to when such transparency measures are required by law and how these obligations should be met.

**Civil Aviation Authorities** should require applicants for aerial work permits to specify how they are meeting these transparency obligations.

Each of these measures would assist RPAS operators in gaining public acceptance of the use of RPAS for civil missions. Being transparent and clear about the purposes for which RPAS are being used, the operators and the organisations that members of the public can approach if they have questions or concerns is central to developing a trusting relationship between the public and the RPAS industry. Transparency tools are mandatory for any RPAS operation that may capture personal data of individuals (either purposely or inadvertently). The Commission, in association with Member State DPAs, CAAs and industry associations, should roll out such protocols to all RPAS operations now and make them mandatory, as most RPAS missions are currently focused on the collection of visual image data.

### 13.5 Impact assessment and soft law measures

The survey of RPAS industry representatives revealed that many responsible RPAS manufacturers and operators are conducting some assessment of the privacy and data protection issues raised by the operations they are undertaking. As Chapter 6 notes, these assessments consist of tools, including:

- Privacy impact assessments
- Risk assessments
- Surveillance impact assessments
- Social impact assessment
- Privacy by design
- Codes of conduct
- Privacy audits
- Data minimisation features
- Use logs and
- Other tools.

In addition, the proposed GDPR includes an article requiring the mandatory impact assessment of any operation involving the collection and processing of personal data. As such, the EC as well as many responsible industry representatives have already agreed that undertaking an assessment of these impacts, on a case-by-case basis, represents good practice

in the collection and processing of personal data. Such soft law measures are particularly suited to sectors such as civil RPAS operations, given that RPAS are multi-dimensional tools. The variety of operations, payloads and capabilities of RPAS mean that they must be assessed on a case-by-case basis, rather than using specific, overarching policy requirements. Furthermore, Chapters 9 and 10 find that the privacy and data protection laws are adequate to protect personal data in relation to civil RPAS; it is the education and enforcement elements that are lacking. As such, we recommend that **all RPAS operators be required to carry out an impact assessment of the potential privacy, data protection and ethical issues on operations that may raise such issues on a case-by-case basis**. Although the preferred method of impact assessment is a privacy or data protection impact assessment (discussed below), this subsection also outlines other soft-law measures that could be used to support good privacy and data protection practice.

**A properly completed privacy or data protection impact assessment<sup>3</sup> (DPIA) is the most robust mechanisms for ensuring that a proposed operation addresses privacy, data protection, ethical and other social considerations.** DPIAs can be tailored and expanded to include a consideration, not only of privacy and data protection issues, but also social and ethical impacts such as dignity, informed consent, protection from discrimination (e.g., profiling or social sorting), protection of freedom to assemble, communicate and move about public space.<sup>4</sup> There are already a number of existing resources to assist RPAS operators in designing and completing a PIA, and the EC would not necessarily have to provide any additional training materials and procedures (although this is recommended below). Such an impact assessment would enable operators to identify potential privacy, data protection and ethical issues early. This would, in turn, enable them to adjust their missions and data collection procedures before the operation and avoid costly retro-fixes (such as blurring unnecessary images) or liabilities (through breaching privacy or data protection laws). PIAs are particularly suited to the RPAS sector, given its heterogeneity. A PIA would encourage RPAS manufacturers and operators to avoid a checklist approach, and consequently, to consider the specificity of their individual operation, the capabilities of their RPAS, the payloads that it would carry and the data that would be collected, the stakeholders impacted, the potential privacy, ethical and reputational risks. In addition, it expands an existing, responsible and relatively common practice of risk or impact assessment, rather than introducing a new procedure. Many PIA experts advocate making the results of the PIA (or a summary of the PIA report) publicly available to assist in transparency and build public trust. This could also be of benefit to the RPAS sector. However, RPAS operators may not feel they have the necessary expertise to undertake such an assessment.

Furthermore, in other sectors – RFID and smart meters – industry representatives, Data Protection Authorities and the European Commission have worked together to develop PIA frameworks or templates for that particular sector. This has involved industry representatives drafting the initial framework, the Article 29 Working Party reviewing it and offering

---

<sup>3</sup> There is already a significant literature on privacy impact assessment, and it specifically includes a consideration of data protection as well as other issues. The GDPR uses the term data protection impact assessment and specifies that it should also include other fundamental rights such as privacy. For the purposes of this report, we use the term privacy impact assessment because it should address all issues associated, not only data protection.

<sup>4</sup> Wright, David, and Michael Friedewald, “Integrating privacy and ethical impact assessments”, *Science and Public Policy*, Vol. 40, No. 6, December 2013, pp. 755-766.  
[Http://spp.oxfordjournals.org/content/40/6/755.full](http://spp.oxfordjournals.org/content/40/6/755.full)

suggestions for improvement, and so on until they agreed on a workable approach. Given the complexity of RPAS technologies and missions, a similar undertaking, initiated by the European Commission, could be used and would offer clear guidance about good practice in assessing the potential impacts of RPAS missions. Furthermore, such a methodology would also result in a harmonisation of practices across Europe.

The **European Commission** should follow good practice in the RFID and smart meters sectors and commission or support the development of a PIA framework or template for RPAS. This would include issues specific to the current and likely future capabilities and applications associated with RPAS. The PIA framework should be devised in close consultation with industry representatives and Data Protection Authorities, and the Article 29 Working Party should endorse the framework before it is rolled out.

**Data Protection Authorities** should liaise with industry associations or other commissioned experts to assist in the creation of a PIA template and/or guidance. They should consider working within the Article 29 Working Party to consider what elements should be included in the PIA template and commit to evaluating the proposed framework and offering suggestions for improvement.

**Industry associations** should work with Data Protection Authorities and commissioned experts to ensure that the proposed PIA framework is relevant to their members. They should also commit to publicising and distributing the agreed-upon framework to their members and encouraging its adoption as best practice in meeting soon-to-be-implemented legal requirements.

Finally, as will be discussed in further detail below, because impact assessments will become legally required under the GDPR, **Civil Aviation Authorities** should not issue aerial work permits unless the operator has certified that a PIA has been conducted.

Additional tools, such as codes of conduct and privacy certification schemes, may assist in developing this necessary expertise. One benefit of devising codes of conduct is that they outline specific practices that are acceptable and unacceptable, based on previously gathered, expert information. **Developing codes of conduct for typical RPAS operations would enable RPAS industry representatives to build on existing knowledge and expertise in this area.** The benefits of such a tool would be that RPAS operators would not have to gain additional expertise and they could have clear-cut information about acceptable and unacceptable practices. The codes of conduct could build on existing resources, such as the *CCTV Code of Practice* developed by the UK Information Commissioner's Office.<sup>5</sup> The first drawback is such codes only provide basic information that RPAS operators would need to adapt to their individual technologies and operations. Second, such a tool would not address the heterogeneity and development of RPAS and their operations. Furthermore, a code of conduct would not necessarily encourage privacy-by-design approaches or other measures that requiring "thinking outside the box". Instead, they are quite static, rigid documents.

---

<sup>5</sup> Information Commissioner's Office, *CCTV Code of Practice*, Wilmslow, 2008. A draft, revised version is currently the subject of public consultation.

Finally, RPAS operators would have to manually communicate to the public that they are following such codes of conduct, which might entail complex communication.

**Industry associations** are the natural, centralised organisations to formulate such codes of practice, given that they have intimate and expert knowledge of RPAS capabilities and established and novel applications. Industry associations should liaise with their members and with Data Protection Authorities and other legal and policy experts to ensure that the code is relevant, and that it adequately addresses the ethical and legal obligations of their Member State and the European Commission.

As noted in the paragraph above, **Data Protection Authorities** should work with industry associations to ensure that the codes of conduct adequately address the likely privacy and data protection risks inherent in these typical scenarios.

**National policy-makers** should channel resources to Data Protection Authorities to enable them to adequately participate in these liaison activities.

A privacy impact assessment or other soft-law measures would specifically involve a consideration of all of the privacy, data protection and ethical issues raised in this report. PIAs, in particular, and the methodology already established in the RFID and smart meter sectors, offer an opportunity to establish a robust and harmonised framework for assessing these issues in this complex and dynamic sector. With specific relation to data protection as an exemplar, PIAs would address proportionality, data minimisation and purpose limitation because a PIA would encourage RPAS operators to be clear about the data they collect and they would have to justify this in relation to the stated purpose of the mission. It would also require them to describe their data management plans, including issues around data security and the potential transfer of data to third countries. Furthermore, a PIA would encourage operators to consider privacy by design, anonymisation or data minimisation features that could significantly reduce their risk in terms of their legal obligations. In addition, these instruments would address issues associated with transparency, consent, accountability and rights of data correction and erasure because RPAS operators would have to specify how they would meet these requirements. Finally, it would encourage RPAS operators to consider more complex privacy<sup>6</sup> and ethical issues. These assessments, and especially ensuring that the assessment is evaluated and endorsed by the Article 29 working party, would foster public trust in RPAS operations, and ultimately enable the expansion of their use for civil applications.

### 13.6 Monitoring good practice

Most of the policy recommendations outlined above focus primarily on improving civil RPAS operators' understanding and awareness of privacy, data protection and ethical obligations. However, the policy recommendations also need to deal with the second key issue associated with the legal framework – monitoring and enforcement. In particular, **CAAs and DPAs should be encouraged and supported to better communicate and co-operate in relation to the civil RPAS sector to check that these procedures are taking place and that RPAS**

---

<sup>6</sup> For example, privacy of behaviour, privacy of location, privacy of groups.

**operators are respecting privacy and data protection law.** Both CAAs and DPAs have a key stake in this issue, where CAAs act as gatekeepers that grant RPAS operators access to airspace, while DPAs already have the competence to identify, investigate and enforce privacy and data protection issues. As such, these two organisations have complementary strengths and powers in this sector, but they are not yet deploying these competencies as collaboratively as could be possible.

**Civil aviation authorities are the natural gatekeepers,** as they already certify RPAS operations in many Member States<sup>7</sup> and monitor safety and licensing issues for the aviation sector. Furthermore, although CAAs do not have the necessary competence in privacy and data protection, their role could be to ascertain that some sort of impact assessment has taken place (much as they ascertain that pilots have valid licences). The assessment could take the form of a PIA, or it could be a certification either that the mission has been assessed and/or that the pilot has adequate privacy and data protection training.

**Data Protection Authorities are the primary privacy and data protection enforcement authorities.** DPAs have the necessary skills and expertise, and they are already assessing data protection issues on a regular basis. They are centralised authorities, and already have powers to conduct investigations and issue sanctions. However, their powers might need to be clarified in relation to the assessment and enforcement of broader privacy or, more particularly, ethical infringements. This could be a significant stumbling block as some RPAS missions could breach privacy or ethical standards even though they do not collect personal data<sup>8</sup> Furthermore, DPAs are already stretched, and would require additional resources if they were to accept additional responsibilities.

The **European Commission** should liaise with JARUS, the EASA and other stakeholders to encourage Civil Aviation Authorities to accept responsibility for ensuring that a PIA has taken place before issuing permission to fly.

The **European Commission** should also work with CAAs to communicate and encourage all of them to follow good practice already established in the UK, Ireland, France, Belgium and other countries in terms of issuing aerial work permits and establishing some oversight over RPAS missions.

**National policy-makers** should clarify whether individual DPAs have the authority to address privacy and ethical issues related to RPAS alongside the data protection elements and, if so, provide resources to support this additional workload.

**Data protection authorities** should work to develop competency and authority in the assessment of privacy and ethical issues in relation to RPAS and should establish relationships with CAAs in order to enforce PIA requirements once they become a legal obligation.

**Civil Aviation Authorities** should enact oversight mechanisms for RPAS, including

---

<sup>7</sup> The UK, Ireland, Sweden, Germany, France and Italy.

<sup>8</sup> For example, one of the major privacy and ethical issues discussed in the chapters above is that members of the public often do not know that an RPAS is in operation and they do not know who is operating it and the purpose for which it is being used. Thus, even civil RPAS missions that do not collect personal data can breach privacy or ethical issues, particularly if they do not exercise good practice in transparency.

issuing aerial work permits that would include an assessment of adequate consideration of safety, licensing and liability issues as well as privacy and data protection.

These organisations clearly need to work closely together to ensure that the RPAS industry is aware of and properly addressing privacy, data protection and ethical issues in their operations. Each of these authorities are recognisable, centralised authorities that citizens can approach in order to ask questions or make complaints. In this analysis, the Civil Aviation Authorities are the most natural authorities to simply check that such an assessment has taken place, leaving the competence in privacy, data protection and ethical issues to the DPA. This recommendation also builds on the previous recommendations, in that the CAAs are also the natural holders of information on RPAS missions in order to meet transparency requirements and provide information to members of the public. The EC could support this necessary collaboration between CAAs and DPAs through workshops and training about each other's competencies and authorities. This could culminate in a series of national agreements about working together on issues related to civil RPAS.

### 13.7 Other recommendations

This study has also found that there are legal gaps with respect to the use of RPAS by private individuals or "natural persons" for household purposes and journalists. With regard to commercial operators, we find that many of the existing legal gaps would be addressed by the proposed General Data Protection Framework. As such, we recommend that the European Commission should **adopt the Parliament Proposal of the General Data Protection Regulation** to address these gaps.

All of the stakeholders consulted as part of this research have identified private users of RPAS as the most high-risk group as there are no specific privacy or data protection laws that apply to their use of RPAS for recreational or other purposes. However, these users are implicated in the RPAS stakeholder eco-system considered in the project. As such, **RPAS manufacturers who offer RPAS for private sale should include guidance on responsible use** of RPAS by private citizens and journalists. Furthermore, **national policy-makers should seriously consider how harassment laws and other instruments could be used to curtail irresponsible uses of RPAS or consider how these uses could be prevented.**

With regard to police or government use of RPAS for surveillance operations, this report finds that robust safeguards should be implemented to ensure that citizens' rights are protected. Specifically, RPAS capabilities mean that they can enter into spaces such as homes, buildings and other spaces not normally accessible and that they are likely to constitute close and targeted surveillance of individuals. As such, **RPAS operations by police should require a warrant issued by a judicial authority** and should be limited to situations where traditional surveillance tools are inadequate to meet the aims of the surveillance mission. Furthermore, **national policy-makers should implement strict controls on the seizure of RPAS footage taken by non-state actors in the investigations of crimes.** Finally, the European Commission should **revise the Proposed Police and Criminal Justice Data Protection Directive to better address the challenges posed by atypical intrusive surveillance technology like RPAS.**

Given that some Member States have linked their CCTV regulations to the use of RPAS, this offers a specific avenue through which they can offer specific advice. As such, **Member States should clarify the extent to which their CCTV regulations apply to the use of drones mounted with a visual surveillance camera in a commercial context.** However, not all RPAS applications rely upon the use of visual imaging, and Member States should also encourage RPAS operators to consider how these other technologies might impact privacy, data protection and ethics, preferably through a privacy impact assessment.

### 13.8 Summary

These policy recommendations are geared to the European Commission, national policy-makers, the RPAS industry, Data Protection Authorities and Civil Aviation Authorities. They specifically outline a set of key actions that should be undertaken to ensure adequate protection of citizens' privacy, personal data and ethical values. For each recommendation, we have outlined sub-recommendations or options to achieve these actions and the roles of different stakeholders in achieving them. While we believe that all of these recommendations offer an opportunity for improved practice, this summary section highlights a few, key recommendations for specific types of stakeholder.

First, we believe that the planned introduction of mandatory Data Protection Impact Assessments as part of the GDPR offers an opportunity for the European Commission to take the lead in ensuring that the RPAS industry takes their privacy and data protection obligations seriously. The RPAS industry must be supported to succeed in this endeavour. As such, we recommend that the European Commission support the development of a PIA framework for RPAS that can be evaluated by the Article 29 Working Party. This would follow established good practice in the RFID and smart meter sectors, and offer a robust and harmonised framework and methodology that would assist the RPAS industry in substantially meeting these obligations.

Second, this report reveals that there is a clear need for industry and Data Protection Authorities to establish an ongoing dialogue. This dialogue would protect citizens' fundamental rights, and protect the emerging RPAS industry from legal liabilities. As such, it offers an opportunity for both stakeholders to improve practice in this area. However, the resources of DPAs are stretched, and many RPAS industry representatives are SMEs with similarly stretched resources. The EC can support this collaboration by hosting regulator workshops or convening and funding a regular working group on this issue.

Third, the European Commission needs to support awareness-raising activities targeted at the RPAS industry that clarify privacy and data protection requirements as well as publicise privacy-by-design features and practices that could mitigate the privacy and data protection risks associated with RPAS missions. This could include working with Member States to develop training courses and high-quality information materials in multiple languages for industry representatives. It could also include commissioning an information portal and forum to share information about RPAS legal obligations and risk mitigation measures.

Fourth, different stakeholders within the civil RPAS sector should work together to develop a national or cross-national information resource to enable citizens to identify the missions and operators associated with individual RPAS. These tools will meet transparency requirements for those missions that are collecting personal data, and will build public trust in relation to missions that are not collecting such data.

Finally, the European Commission should work with EASA, JARUS and other organisations to deploy CAAs as a natural gatekeeper for the civil RPAS sector. CAAs should be encouraged to issue aerial work permits and to ensure that legal obligations such as transparency tools or DPIA requirements have been conducted. This will require closer collaboration between CAAs and DPAs to enable them to mobilise their complementary competencies in this area.

Each of these recommendations would promote better protection of privacy, data protection and fundamental ethical values. However, as a package, all of these recommendations would construct a robust system of protection for Europeans, and provide a predictable and consistent regulatory framework for the RPAS industry that would support innovation. Furthermore, many of these recommendations are intersecting and overlapping. For example, the conduct of PIAs would include transparency protocols. As such, when implementing these recommendations, the EC should consider how they might link together as a complete package for a healthy civil RPAS sector that protects European citizens' fundamental rights.

## 14 CONCLUSION

This analysis has made a significant contribution to an overall understanding of the RPAS landscape, including RPAS capabilities and applications, the potential privacy, data protection and ethical issues raised by RPAS and the European and Member State legal framework(s) associated with RPAS. This information was complemented with a number of consultation exercises and has resulted in a detailed analysis of the potential privacy, data protection and ethical risks raised by the use of RPAS with different capabilities in particular contexts and the extent to which existing legal frameworks are adequate to address the risks posed by RPAS. In summary, the report has found that the existing legal regime in Europe and Member States is adequate to address privacy, data protection and ethical risks associated with RPAS. However, we have also included a number of policy recommendations and “soft law” measures to raise awareness about these risks among the RPAS industry and to assist in the enforcement of the obligations of RPAS operators who are collecting, processing and storing data related to people and their property. In the following paragraphs, we summarise the main findings of the report.

First, RPAS are heterogeneous. They come in a number of sizes and have a range of flight capabilities. Additionally, the payloads with which they may be fitted, and the applications for which they may be used, are varied and differentiated. Consequently, the privacy, data protection and ethical issues they raise are often specific to the UAV, its payload, the operator, the context and the application. Each of the individual combinations and permutations of these factors raise specific privacy, data protection and ethical issues. In particular, the use of RPAS for aerial photography by commercial organisation and visual surveillance by law enforcement operators carry significant privacy, data protection and ethical risks. The report has found that RPAS operators are uninformed about these risks, as many applications only film “the tops of people’s heads”. However, when contextualised by particular landmarks, an individual’s private dwelling or other particular locations, these images may become personal data. Furthermore, the recording of number plates, GPS coordinates, biometrics or other details are certainly personal data. Whether the RPAS captures personal data or not, RPAS operation may raise privacy issues, such as a “chilling” effect, function creep or a dehumanisation of the surveilled among others, and may raise ethical issues such as safety and discrimination.

Furthermore, whether RPAS capture personal data or not, RPAS operators are subject to privacy legislation at a European level and the Member State level. These obligations prevent RPAS operators from interfering in the “privacy of home and family life” and the “privacy of communications” unless they can demonstrate that the interference is in accordance with the law, is necessary in a democratic society or is necessary for the protection of others. RPAS operations that record images in a systematic way, that disclose images of persons or that monitor public space through “sophisticated means” will interfere with this right and may be unlawful. If the images captured by RPAS are considered personal data, RPAS operators become subject to the European Data Protection Directive, as well as national instruments. This means that RPAS operators must adhere to certain principles when processing personal data, including:

- lawfulness and fairness principles
- purpose limitation principle;
- proportionality and data minimisation principles;
- data quality principle; and

- retention principle.<sup>1</sup>

Collecting personal information does not make the operation unlawful as such, but RPAS operators would need to comply with these principles and would need to respect citizens rights to access, correct and delete their personal information.

Given these issues, it is necessary to assist RPAS manufacturers and operators to meet these privacy and data protection obligations. However, as Finn and Wright argue, regulating RPAS in a comprehensive way will be challenging as “UASs are complex, multimodal [...] systems that integrate a range of technologies and capabilities”.<sup>2</sup> Addressing this complexity requires a unique set of expertise, including expertise related to the RPAS themselves, the payloads with which they are fitted and the European and national privacy and data protection regime under which they are operating. In short, it requires technical expertise *and* privacy and data protection expertise (as well as aviation safety). Very few stakeholders are likely to be able to adequately address both, and thus, effective oversight of RPAS would require cooperation between different stakeholders.

However, this cooperation is not yet occurring organically, and the EC must intervene to meet its goal that the regulation of RPAS also address “societal issues” alongside safety issues.<sup>3</sup> Some RPAS manufactures and operators are already addressing these issues using privacy impact assessments, privacy by design processes and other “fixes” such as blurring faces, persons or vehicles. These need to be encouraged and publicised for all RPAS operators that may be collecting personal data. Furthermore, the RPAS industry needs to be better informed about their legal obligations when collecting, processing and storing personal data. This can be accomplished by different stakeholders, especially Civil Aviation Authorities and Data Protection Authorities, working together to construct regulatory frameworks that will support RPAS operators and build expertise in these areas. It will also lead to better enforcement of these obligations and better protections for citizens. Finally, the RPAS industry needs, as far as possible, a harmonised regulatory framework in order to reduce complexity and provide clarity.

As such, this study makes five primary recommendations. Specifically:

- Industry should take specific actions to reduce their risk of collecting and processing personal data
- The EC, national policy-makers, Civil Aviation Authorities and Data Protection Authorities must work together to raise awareness of privacy and data protection requirements among the RPAS industry
- The RPAS industry should be required to meet information and transparency protocols
- Impact assessments of privacy and data protection issues (privacy impact assessments) should be conducted for each type of operation. The EC should support a harmonised framework by commissioning a PIA template for RPAS.

---

<sup>1</sup> European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, Article 6.

<sup>2</sup> Finn, Rachel, and David Wright, “Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications”, *Computer Law & Security Review*, Vol. 28, No. 2, 2012, pp. 184-194 [p. 185].

<sup>3</sup> European RPAS Steering Group, *Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System*, June 2013. <http://ec.europa.eu/enterprise/sectors/aerospace/uas/>

- Civil Aviation Authorities and Data Protection Authorities must work together to monitor good practice in privacy and data protection. The EC should support this collaboration.

These recommendations, and their associated sub-recommendations, represent a robust system of protection for Europeans, and would provide a predictable and consistent regulatory framework for the RPAS industry that would support innovation.

## **15 ANNEX A: RPAS CAPABILITIES AND APPLICATIONS**

### **15.1 Introduction**

This chapter provides an overview of the different types of remotely piloted aircraft systems (RPAS) that are currently in use or under development and which may one day be operated within the European Union. The purpose of this is to gain an understanding of how RPAS are being used, what payloads they may carry and what contexts within which they are operating, in order to provide a foundation for examining the privacy, data protection and ethical issues they may raise. This chapter concludes with a taxonomy of RPAS applications and contexts that will be used to map the privacy, data protection and ethical issues in Chapter 4.

Although it is widely assumed that RPAS are a quintessentially modern technology, their development can be traced all the way back to the late nineteenth century and the hydrogen-filled airships controlled by spark-emitting radio signals that were flown around theatre auditoriums to entertain music hall crowds. Subsequent attempts to create a “flying bomb” inspired by World War I produced the first remotely piloted aircraft flight – a modified “N9” U.S. Navy seaplane – in 1918.<sup>1</sup> For the next 75 years or so RPAS remained largely the preserve of the defence sector, which continued to develop the technology for missile guidance, target practice and surveillance purposes, and hobbyists and their suppliers, who developed the technology for the love of flight. The idea that RPAS could ultimately perform many if not all of the tasks currently performed by on-board-piloted aircraft gained currency in the 1990s and in particular after the NATO intervention in Kosovo, when UAS were used for real-time surveillance and target acquisition in the former Yugoslavia.<sup>2</sup> Today there are hundreds of different models and thousands of organisations engaged in their design, manufacture and use. According to UVS International, by 2011 the production of more than 400 different UAS was spread across at least 21 EU countries.<sup>3</sup>

This examination of civil applications is the first systematic attempt to outline the capabilities of RPAS, the payloads they may carry and the contexts in which they operate. It is based on an examination of research reports, academic journal articles and other publications, mass media materials, industry websites, policy documents and materials from civil society organisations. However, it is important to note that the RPAS sector is a quickly evolving industry, and due to its dynamic nature, this taxonomy may be quickly out-dated as miniaturisation of RPAS and payloads, technological development and the identification of novel applications continue.

The taxonomy is divided into three parts. The first examines the technical specifications that distinguish different types of UAS and RPAS from one another, notably the size and weight of the aircraft, the control systems used to pilot them and their flight capabilities. These are the considerations that typically inform national and intergovernmental regulations, although there is as yet no formally agreed international classification framework for unmanned

---

<sup>1</sup> See further the account of the historical development of unmanned aircraft systems in John Villasenor, “Observations From Above: Unmanned Aircraft Systems and Privacy”, *Harvard Journal of Law and Public Policy*, Vol. 36, No. 2, 2013, pp. 462-464.

<sup>2</sup> European Advisory Group on Aerospace, “STAR 21: Strategic Aerospace Review for the 21st Century”, Brussels, 2002.

<sup>3</sup> Van Blyenburgh, Peter, “UAS Industry and Market Issues”, *European Commission UAS Panel, 1st Workshop*, 12 July 2011.

systems. The second part of the taxonomy examines the capabilities of UAS and RPAS with a view to introducing the technological and operational issues that must be considered from a data protection and broader ethical perspective. The third part examines the different sectors in which UAS and RPAS may be used, now and in the future. The final part of the taxonomy provides a matrix summarising the possible proliferation of different classes of UAS and RPAS and the data protection and ethical concerns raised by different applications.

## 15.2 Technical specifications

The acronyms UAV (Unmanned Aerial Vehicle) and RPA (Remotely Piloted Aircraft) are commonly used as generic shorthand for the wide and varied range of unmanned and remotely controlled aircraft that now exist. The terms UAS and RPAS refer to the complete systems required to fly UAVs and RPAs, which include a vast array of sensors, processors and data links that facilitate flight and communication between the ground-station and the aircraft. Although there is no formal, internationally agreed classification framework for UAS/RPAS, the UK's Civil Aviation Authority (UK CAA) "is widely regarded globally as the standard-setter", notably in connection with its regularly updated publication, *Unmanned Aircraft System Operations in UK Airspace – Guidance*.<sup>4</sup> The UK CAA uses "a combination of the emerging International Civil Aviation Organisation definitions, other 'common use' terms which are considered to be acceptable alternatives, and a number of 'legacy' terms".<sup>5</sup> *Circular 328*, published in 2011 by the United Nations' International Civil Aviation Authority is another authoritative source.<sup>6</sup> The North Atlantic Treaty Organization (NATO) also has a classification standard.<sup>7</sup> Work on common terminological standards in UAS/RPA advisory bodies in the EU and USA is also underway but not yet complete. In order to introduce the different types of RPAS in operation or under development the following subsections describe the different weight classes of RPAS set out in the UK CAA regulations. Some EU Member States use slightly different weight ranges and classes (see further 9on regulations).

### 15.2.1 Size and weight

#### *Large (over 150 kg)*

The key threshold for UAVs and RPAs as far as the European Union is concerned is whether the operating mass, or Maximum Take-Off Mass (MTOM), exceeds 150 kilograms. If so, it is subject to the basic European Aviation Safety Agency (EASA) Regulation of 2008 and will

---

<sup>4</sup> Goldberg, David, "Remote Control: Remotely Piloted Air Systems – Current and Future UK Use", *House of Commons Select Committee on defence 10th Report, Vol. II*, March 2014.

<sup>5</sup> UK Civil Aviation Authority, *Unmanned Aircraft System Operations in UK Airspace – Guidance (Fifth Edition)*, CAP 722, 2012.

<sup>6</sup> International Civil Aviation Organization, *Unmanned Aircraft Systems (UAS)*, ICAO Cir 328, 2011.

<sup>7</sup> In 2006 the three NATO UAV working groups (navy, land and air) were merged into a single Joint Capability Group on UAVs. In 2008 a UAV Classification guide was adopted to assist in the process of developing a common language for deliberating, planning and operation of UAV/UAS in a coalition environment. The Classification Guide is available in Ministry of Defence, *Unmanned Aircraft Systems: Terminology, Definitions and Classification*, Joint Doctrine Note (JDN) 3/10, 2012, pp. 2-3.

be required to have an EASA airworthiness certificate – unless it is operated by a state agency.<sup>8</sup>

In the 150kg plus category – or Weight Classification Control Group 3 as defined by the UK CAA – NATO distinguishes between Class II (150-600 kg) and Class III (over 600kg). Class II includes “tactical” UAVs” such as the “Sperwer”, “Hermes 450”, and “Watchkeeper”. Class III UAS include three subcategories: (i) Medium Altitude, Long Endurance (MALE), (ii) High Altitude, Long Endurance (HALE) and (iii) strike or combat UAVs (or UACVs).

The development of UAVs and RPAs in these weight classes has been driven by the defence sector, where MALE UAS include the “Predator”, “Heron” and “Hermes 900” and HALE UAS such as the “Global Hawk”, which has the wingspan of a 737 airliner and can climb to 65,000 feet on non-stop, 35-hour missions.<sup>9</sup> Strike UAS (or UCAV) are currently limited to weaponised MALE models such as the “MQ9-Reaper” (or “Predator B”) but a host of dedicated combat models are currently under development by the world’s militaries.<sup>10</sup>

Compared to the vast potential for civil applications using smaller RPAS, the development of civil applications using class II and III RPAS appears limited as compared to smaller craft. According to UVS International, the development of aircraft with a MTOM of less than 150kg outnumbered their larger (more than 150kg) counterparts by a ratio of almost five to one in 2011.<sup>11</sup> Those areas where the use of large RPAS for commercial purposes is widely envisaged include very high-altitude, long-endurance applications, where VHALE drones could act as proxy satellites and provide services such as communications networks and earth observation, at a fraction of the cost. MALE drones are already used for law enforcement and surveillance purposes including for border controls by the US government and similar applications are envisaged in the European Union.<sup>12</sup> Large RPAS could also one day provide cargo and even passenger transport services but investments to date have been relatively small because of the restrictive regulatory framework, immaturity in the market and doubts as to take-up in the short term.

#### *Light (20-150 kg)*

Light RPAS, with an operating mass of between 20 to 150 kilograms – or Weight Classification Control Group 2 as defined by the UK Civil Aviation Authority – are exempt from the EASA airworthiness requirements but must obtain approval and operating permission from national civil aviation authorities if used for commercial purposes (see further Chapter 9 on safety regulations). Light RPAS are typically longer-range, fixed-wing aircraft capable of flying hundreds of miles on what are known as “beyond the line of sight” missions at altitudes of around 10,000 feet. These smaller aircraft offer exceptional endurance but require a skilled crew comprising several persons to operate and a dedicated support

---

<sup>8</sup> European Commission Regulation 216/2008/EC on common rules in the field of civil aviation and the establishment of the European Aviation Safety Agency, OJ L 79/1, 19.3.2008. Amended by Regulation 1108/2009/EC.

<sup>9</sup> “Aviation first for robotic spy plane”, *BBC news*, 24 April 2001.  
<http://news.bbc.co.uk/1/hi/world/americas/1294014.stm>

<sup>10</sup> See for examples, MilitaryFactory staff writer, “Unmanned Combat Air Vehicles (UCAVs)”, *MilitaryFactory.com*, 3 December 2014. <http://www.militaryfactory.com/aircraft/unmanned-combat-air-vehicle-ucav.asp>

<sup>11</sup> Blyenburgh, op. cit. 2013.

<sup>12</sup> See for example the EU-funded PERSEUS, SEABILL, OPARUS and CLOSEYE projects.

infrastructure, making them relatively expensive as compared to the smaller models described below. Examples of light RPAS include the “Luna” and “Hermes 90”. Civil applications for light RPAS include geospatial surveying and wide-area surveillance.

#### *Small (2-20kg)*

Small RPAS or “mini-UAVs” with an operating mass of less than 20 kilograms may be exempt from national airworthiness requirements but are still subject to various regulations and guidelines, including demonstrable pilot competence if used for commercial purposes (the threshold for small RPAS is 25 kg in several EU Member States). Within this category, RPAS with an operating mass of less than seven kilograms may be exempt from these requirements if used for non-commercial purposes (see further Chapter 9 on safety regulations). Hobbyists and non-commercial operators are advised to “only fly Small UAV (under 7Kg)” at less than 400 feet (122 metres) and maintain both visual line of sight and “pilot in control” for these reasons.<sup>13</sup>

Within the small RPAS category there are hundreds of different types of small, cheap multi-rotor and fixed wing UAVs that resemble traditional radio-controlled model aircraft. Their capabilities include “automated flight, GPS guidance, live video streaming cameras (connected to First Person View FPV goggles, enabling the craft to be flown via camera, out of sight, over the horizon), all sold in a compact flying package, available online in components or assembled, or from the local hobby shop for the price of a smart phone”.<sup>14</sup> According to the US Federal Aviation Authority This category of RPAS is expected to “grow most quickly in civil and commercial operations because of their versatility and relatively low initial cost and operating expenses”.<sup>15</sup>

#### *Micro (less than 2kg)*

UAVs with an operating mass of less than 2kg are known as “micro UAVs”, “micro drones” or “MAVs” (Micro Air Vehicles), with the smallest of these models known as “insect drones” or “nano-drones”. California-based AeroVironment’s “RQ-11 Raven”, a 1.9kg fixed-wing, hand-launched UAV first developed for the US military has a range of 10 kilometres and is cited as the “most widely adopted UAV system in the world today”, with 19,000 units shipped by 2012.<sup>16</sup> However, the toy “Parrot AR Drone”, which weighs around 400 grams is now claimed to have sold more than half a million units.<sup>17</sup>

The video-capable “Nano Hummingbird”, also developed by AeroVironment for the USA’s Defense Advanced Research Projects Agency (DARPA), weighs only 19 grams and in 2011 reportedly completed a successful demonstration of “controlled precision hovering and fast-forward flight of a two-wing, flapping wing aircraft that carries its own energy source, and

---

<sup>13</sup> UnmannedTech staff writer, “Are UAV's Legal?”, *UnmannedTech.co.uk*, no date. <http://www.unmannedtech.co.uk/regulations.html>

<sup>14</sup> Corcoran, Mark, *Drone Journalism: Newsgathering applications of Unmanned Aerial Vehicles (UAVs) in covering conflict, civil unrest and disaster*, 2014, p. 10. <http://cryptome.org/2014/03/drone-journalism.pdf>

<sup>15</sup> Federal Aviation Authority, “Fact Sheet – Unmanned Aircraft Systems (UAS)”, 6 January 2014. [http://www.faa.gov/news/fact\\_sheets/news\\_story.cfm?newsId=14153](http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14153)

<sup>16</sup> Alex, Dan, “AeroVironment RQ-11 Raven Small Unmanned Aerial Vehicle (SUAV)”, *MilitaryFactory.com*, 7 February 2014. [http://www.militaryfactory.com/aircraft/detail.asp?aircraft\\_id=888](http://www.militaryfactory.com/aircraft/detail.asp?aircraft_id=888)

<sup>17</sup> Laxague, Fabien, Vanessa Loury and Megan Soule, “Parrot Establishes Itself on the Civil Drones Market”, *Parrot Press Release*, June 2013. <http://www.parrot.com/paris-air-show-2013/usa/bg-press-release.pdf>

uses only the flapping wings for propulsion and control”.<sup>18</sup> In 2013 Techjet unveiled the “Dragonfly” MAV, which has a six-inch wingspan, weighs only 5.5 grams and costs just \$119.<sup>19</sup> The unit comes equipped with cameras and can be piloted by a device as common as an iPhone or tablet. In 2006 Harvard University’s “RoboBees” or “coordinated agile robotic insects” project achieved its first successful MAV take-off.<sup>20</sup>

In sum, the operating weight of RPAS is critical both in terms of the regulations governing their use and their likely proliferation in the civil sector, with smaller and lighter RPAS set likely to be much more widely used in the civil sector. These factors – regulation and take-up – are also dependant on the ways in which RPAS are controlled and piloted.

### 15.2.2 Control systems

Much of the debate around the terminology and classification of RPAS centres on how they are controlled. This requires clear distinctions between the aerial component and the control and communication system components that are necessary for operation. The term Unmanned Aerial Vehicles refers simply to the fact that there is no pilot *on-board the aircraft*. The term Remotely Piloted Aircraft refers simply to the fact that flight and operation are controlled by someone outside the aircraft. RPAs may be controlled by an “adjacent pilot” with “visual line of sight” of the aircraft, or by a “remote pilot” able to fly the aircraft “beyond the line of sight” using a “first person view” of live images streamed to the ground station.

UAVs may also fly autonomously, or with a significant degree of autonomy in respect not just to flight but the determination of destinations, flight-path planning, working of on-board equipment and delivery of payload. All of these operations are monitored and may be controlled by ground crew. The UK Ministry of Defence defines an “automated system” as “one that, in response to inputs from one or more sensors, is programmed to logically follow a pre-defined set of rules in order to provide an outcome”. An “autonomous System” is further defined as “capable of deciding a course of action, from a number of alternatives, without depending on human oversight and control, although these may still be present”.<sup>21</sup>

As the technology develops it is likely that RPAS will increasingly include more and more automated and autonomous features to help them fly more efficiently and operate with a maximum level of safety. This includes elements such as predefined flight-paths using GPS, “sense-and-avoid” systems, and safety mechanisms that are activated automatically in the event of pilot or communications failure. Figure 1, over, provides a snapshot of these and other processes at work in RPAS.

---

<sup>18</sup> Gitlin, Steven and Mark Boyer “AeroVironment Develops World’s First Fully Operational Life-Size Hummingbird-Like Unmanned Aircraft for DARPA”, *Reuters*, 17 February 2011.  
<http://uk.reuters.com/article/2011/02/17/idUS155387+17-Feb-2011+BW20110217>

<sup>19</sup> Plafke, James, “This tiny robotic dragonfly drone only costs \$119”, *Geek.com*, 20 February 2012.  
<http://www.geek.com/news/this-tiny-robotic-dragonfly-drone-only-costs-119-1533241/>

<sup>20</sup> Harvard’s School of Engineering and Applied Sciences, “Robobees”, *Harvard University*, no date.  
<http://robobees.seas.harvard.edu/>

<sup>21</sup> Ministry of Defence, *Unmanned Aircraft Systems: Terminology, Definitions and Classification*, Joint Doctrine Note (JDN) 3/10, 2012, pp. 1-5.

An optionally piloted vehicle (OPV) is a hybrid between a conventional aircraft and a UAV that maybe piloted remotely or autonomously with on-board crew able to take conventional control. FRONTEX, the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the EU, is reportedly considering the purchase of OPVs for wide area maritime surveillance before switching to UAVs when the regulatory framework allows.<sup>22</sup>

Evidence of remote pilot competency or certification may be required by national civil aviation authorities responsible for licensing RPAS (see further Chapter 9 on safety regulations). Matters of liability and mandatory insurance in the event of damage caused by accident or negligence are a matter of EU law and national regulations.<sup>23</sup> Separation distances and other safety requirements including sense-and-avoid and ballistic recovery systems (i.e. parachutes) may also be mandated by civil aviation authorities.<sup>24</sup>

---

<sup>22</sup> Hayes, Ben, Chris Jones and Eric Töpfer, *Eurodrones Inc.*, Statewatch/Transnational Institute, Amsterdam, 2014, p. 65.

<sup>23</sup> European Commission Regulation 785/2004/EC of 21.04.2004 on insurance requirements for air carriers and aircraft operators, OJ L 138/1, 30.4.2004, requires most operators of aircraft, including many UAVs, irrespective of the purposes for which they fly, to hold adequate levels of insurance in order to meet their liabilities in the event of an accident. In applying the regulation domestically some national civil aviation authorities may specify additional rules. See for example UK Civil Aviation (Insurance) Regulations 2005.

<sup>24</sup> See for example the UK Civil Aviation Authority, op cit., 2012.

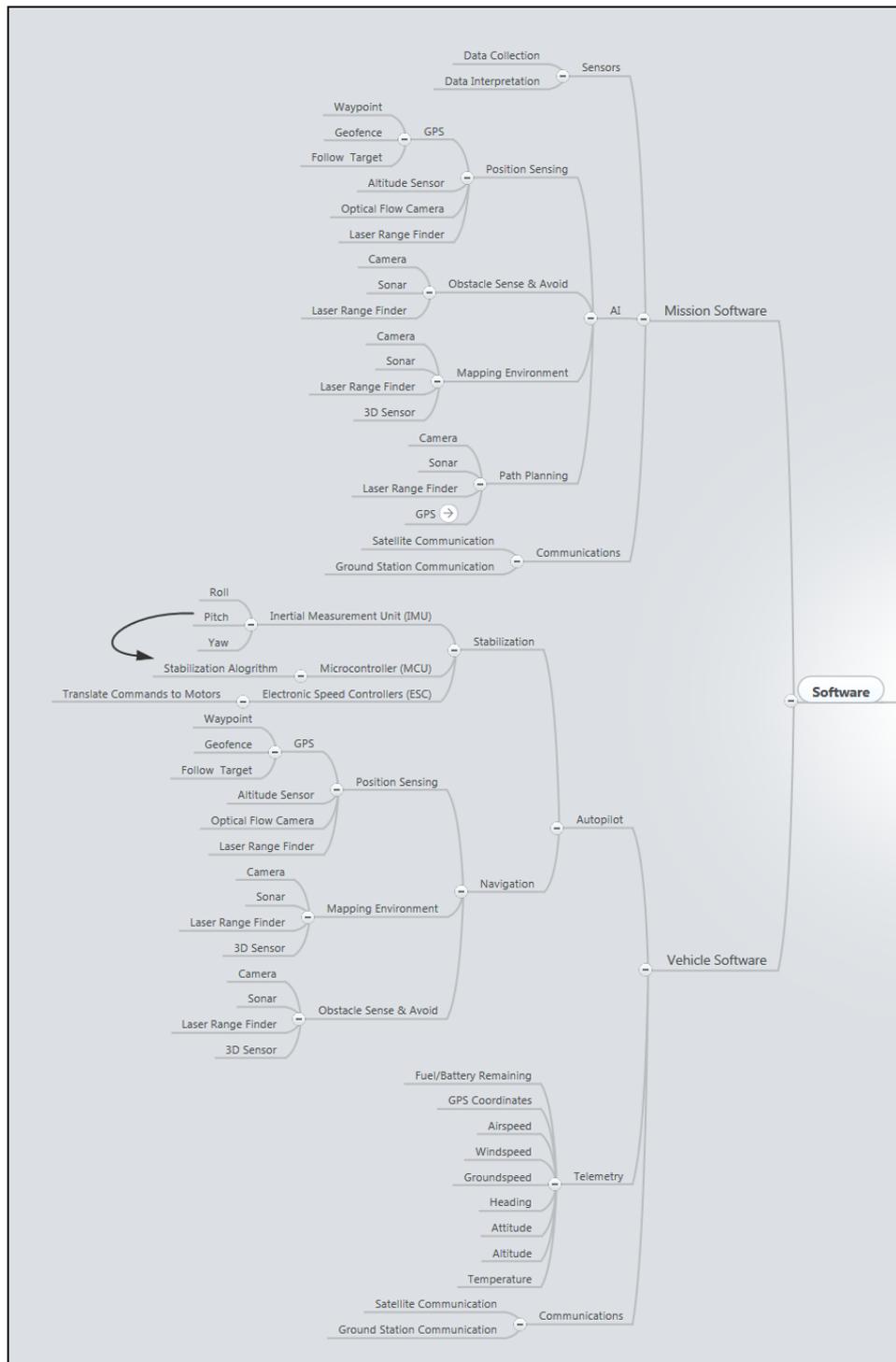


Figure 5: RPAS control systems<sup>25</sup>

<sup>25</sup> Klein, David, "UAV Mind Map", *Mindmeister.com*, February 2014.  
<http://www.mindmeister.com/309657737/uav>

### 15.2.3 Flight

In addition to the way that UAS are piloted and controlled, factors determining the performance of different types of RPAS include launch requirements, speed, range and endurance. The various components affecting the capabilities of RPAS are shown in Figure 2, below.

“Fixed wing” RPAS resemble traditional aeroplanes and are capable of taking-off and landing in the same way. Larger RPAS may also be launched by rocket or catapult, smaller models by hand. Gun-launched “surveillance projectiles” and “parasite UAVs” have also been developed, primarily for military use, but as with other mini-UAVs, numerous civilian uses are envisaged.

Multiple rotor and helicopter-style RPAS are capable of vertical take-off. This includes small “helicopter-like ‘multi-rotors’ weighing less than 2kg” – like the aforementioned the “Parrot AR Drone” – and “larger multi-rotor, 2-7kg” models. The former are now very cheaply available and can be controlled via standard wireless networks using a smart phone or tablet device over a range of a few hundred metres. The latter are capable of carrying heavier payloads such as broadcast quality HD live streaming cameras. These larger multi-rotor craft typically have a line of sight operating radius of about 2,000m and are capable of speeds of up to 70 km per hour. They are more difficult to fly and may require a trained UAV pilot supported by a systems or camera operator.<sup>26</sup>

The fastest UAVs have been developed for the US military. Northrop Grumman’s “RQ-4 Global Hawk” surveillance drone has a cruising speed of 575 km/h and can survey as much as 40,000 square miles per day.<sup>27</sup> The UK Ministry of Defence hopes the “Tarans” UCAV it is developing will be the world’s first supersonic drone, capable of exceeding the speed of sound (approximately 1,234 km/h or Mach 1).<sup>28</sup> The US Air Force has even greater ambitions with its “Falcon HTV-2”, an experimental hypersonic drone that flies at sub-orbital altitudes (of 100 km plus) at speeds of Mach 20 (twenty times the speed of sound).<sup>29</sup>

The range of RPAS is limited by payload and power unit. Medium-altitude long-endurance (MALE) UAVs can fly at up to 30,000 feet for as long as two days. Small fixed wing craft (18-25kg), resembling large model aircraft, are capable of 24 hours continuous flight, while smaller hand-launched RPAS capable of beyond the line of sight flight can fly as much as 50 km over 90 minutes.

---

<sup>26</sup> Corcoran, op. cit., 2014, p. 11.

<sup>27</sup> Spyflight writer (anonymous), “Northrop Grumman RQ-4A Global Hawk”, *Spyflight.co.uk*, no date.  
<http://www.spyflight.co.uk/global%20hawk.htm>

<sup>28</sup> Tarantola, Andrew, “The World’s First Supersonic UAV Is Ready for Takeoff”, *Gizmodo*, 19 June 2013.  
<http://gizmodo.com/the-worlds-first-supersonic-uav-is-ready-for-takeoff-514058742>

<sup>29</sup> Plummer, Mary and Ned Potter, “Falcon HTV-2 Hypersonic Plane Loses Control in Mach 20 Test”, *ABC News*, 11 August 2011. <http://abcnews.go.com/Technology/hypersonic-flight-darpa-launches-htv-plane-test-loses-contact/story?id=14280849>

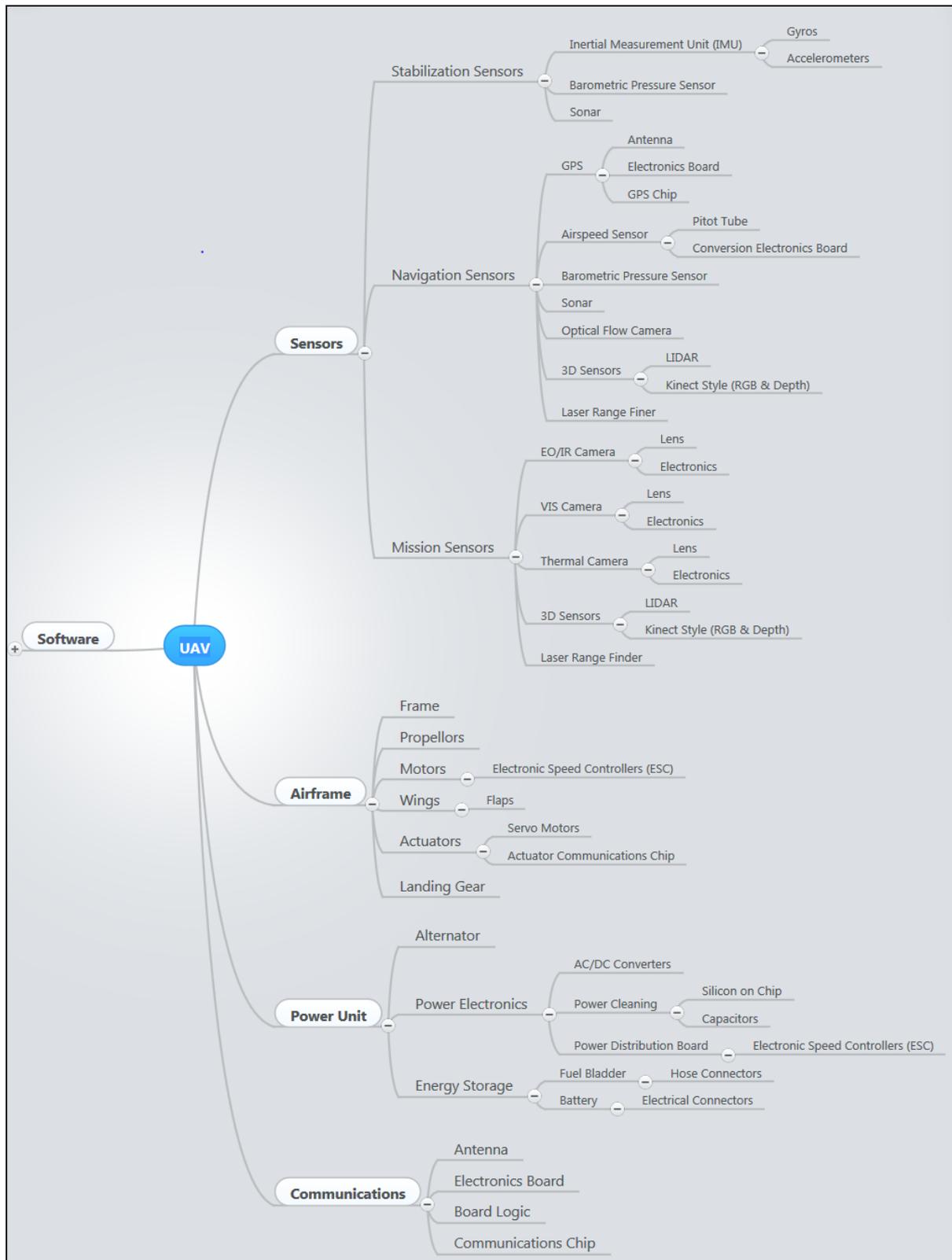


Figure 6: RPAS components<sup>30</sup>

<sup>30</sup> Klein, op. cit., 2014.

As with larger RPAS the trend is toward much greater endurance and in future years the small, low-altitude UAS – which are more widely available – are likely to be able to stay in the air for much longer.<sup>31</sup> In July 2012 UAV Factory’s “Penguin B”, with a total take-off weight of just 22.3 kg, flew for more than 54 hours, beating the previous record of 38 hours for a mini-class RPA.<sup>32</sup> The biggest advances in endurance are promised by solar-power. QinetiQ’s “Zephyr”, which weighs just 53 kg despite having a wingspan of 22.5 metres, stayed aloft for more than two weeks in 2010.<sup>33</sup> Boeing’s “SolarEagle”, which is being developed for the US military, promises up to five years continuous flight from altitudes above 60,000 feet.<sup>34</sup> Test flights are scheduled to begin in 2014. Long endurance, hydrogen-powered UAVs are also in development.<sup>35</sup>

Having introduced the technical specifications and basic characteristics of RPAS, and considered some of the ways in which the enabling technologies may be developed and used, the following sections examine their current and future capabilities and applications.

### 15.3 Capabilities

The recent development of RPAS owes as much to the rapid expansion of computational power, digital imaging and data transmission capabilities as advances in aeronautical technology. Real-time video streaming is a standard feature of beyond the line of sight RPAS, enabling pilots and controllers to fly the aircraft using a “first person view” of live images streamed to the ground station. Many models carry additional surveillance equipment to provide operators with aerial imagery, geospatial analysis and other types of data that can be captured using dedicated on-board equipment. This is why many RPAS raise so many data protection concerns, even when operated by private actors for purposes other than “surveillance”. In the sub-sections that follow, we provide more information about the potential capabilities and applications of civil RPAS.

#### 15.3.1 Aerial photography and video streaming

Depending on payload capacity, the entire range of video camera technology can be fitted to a RPA. In addition to the first-person-view cameras that ground controllers use to pilot the aircraft, everything from basic ‘webcam’ style video streaming to the very high resolution cameras used in film-making can be mounted on RPAs. The cameras may be controlled by a dedicated operator on the ground. Thanks to continuing innovations in airframe design and flight control algorithms, the cameras are effectively becoming more agile. The simplest RPAS are low altitude and line of sight controlled and equipped with one or more cameras and capable of streaming or storing still (photographic) or moving (video) images. The vast

---

<sup>31</sup> Villasenor, John, “Observations From Above: Unmanned Aircraft Systems and Privacy”, *Harvard Journal of Law and Public Policy*, Vol.36. No. 2, 2013, p. 497.

<sup>32</sup> Menaker, Joseph, “New endurance record for small unmanned aircraft”, *UAV Factory Press Release*, 7 July 2012. [http://www.uavfactory.com/info/press\\_releases/pressrelease002.pdf](http://www.uavfactory.com/info/press_releases/pressrelease002.pdf)

<sup>33</sup> Chuter, Andrew, “Solar UAV Lands After Record 2 Weeks Aloft”, *Defensenews.com*, 23 July 2010. <http://www.defensenews.com/article/20100723/DEFSECT01/7230304/Solar-UAV-Lands-After-Record-2-Weeks-Aloft>

<sup>34</sup> Boeing Co., “Boeing Wins DARPA Vulture II Program”, *Boeing Press Release*, 15 Sept 2010. <http://boeing.mediaroom.com/index.php?s=43&item=1425>

<sup>35</sup> “NRL’s liquid hydrogen-fuelled Ion Tiger UAV sets new endurance record”, *Naval-technology.com*, 13 May 2013. <http://www.naval-technology.com/news/newsnrls-liquid-hydrogen-fuelled-ion-tiger-uav-sets-new-endurance-record>

majority of RPAS already licensed for development and use in Europe fall into this category: light and small drones used for activities such as photography, filming, site inspection and infrastructure monitoring. According to lobby group UVS International, “practically all cases” of authorised UAS are visual line-of-sight (VLOS) controlled aircraft flown at an altitude of less than 500 feet with MTOM [Maximum Take Off Mass] of less than 25 kilograms.<sup>36</sup>

### 15.3.2 Wide area surveillance

Higher altitude UAVs and RPAs are capable of conducting surveillance (via aerial photography) of much wider areas due to a combination of the height at which they fly, which gives them a much wider frame of vision, and the resolution of the cameras they carry, which continues to increase exponentially. Their mobility also gives them a great advantage over satellites in lower orbits that can acquire very detailed images but not on a continuous basis.<sup>37</sup> “Predator” drones, which are capable of operating at 18-25,000 feet above sea level, are fitted with daytime and infrared camera and a synthetic aperture radar capable of providing photographic-like images through clouds, rain or fog, and in daytime or night-time conditions, all in real-time. “Global Hawks” are reportedly capable of mapping areas of up to 100,000 km<sup>2</sup> on a single flight.<sup>38</sup> At much lower altitudes even small, hand-launched RPAS can cover relatively large areas. Mavinci’s auto-piloted “Sirius Pro”, for example, claims to be able map up to 8.5 km<sup>2</sup> on a single 45-minute flight.<sup>39</sup>

The EU has funded several research and development projects examining the use of UAS and RPAS for wide area coastal and maritime surveillance including the OPARUS and 3i projects. In the commercial sector a whole host of uses for UAS and RPAS that can cover larger areas are envisaged, particularly applications using mapping and surveying equipment. In the future is possible that high-altitude UAVs capable of continuous, high-resolution earth observation could be deployed and networked to provide “persistent wide area surveillance”.

BAE Systems has developed this kind of system for the USA’s defence agency (DARPA). ARGUS (Autonomous Real-Time Ground Ubiquitous Surveillance) System produces high-resolution video image that covers up to 15 square miles from an altitude of 17,500 ft. This data is streamed to the ground and stored, and operators can zoom in upon any small area and watch the footage of that exact spot.<sup>40</sup> The video camera is reported to have a combined resolution of 1.8 gigapixels – the equivalent to having 100 “Predator” Drones hover over a medium-sized city at once – and is capable of capturing objects as small as six inches wide as well as tracking vehicles and people. Although the deployment of such a system would face tremendous privacy and data protection hurdles, the establishment of permanent earth

---

<sup>36</sup> UVS International Org., “Civil RPAS in the European Union”, *UVS International*, 17 February 2014. [http://uvs-international.org/phocadownload/03\\_11\\_articles\\_and\\_opinions/RPAS-in-the-EU\\_UVSI\\_140217.pdf](http://uvs-international.org/phocadownload/03_11_articles_and_opinions/RPAS-in-the-EU_UVSI_140217.pdf)

<sup>37</sup> See further Villasenor, op. cit., 2013, p. 495.

<sup>38</sup> DARC, “Robots”, *Drones and Aerial Robotics Conference*, no date. <https://droneconference.org/robots/>

<sup>39</sup> Claussen, Johanna, “MAVinci’s next generation aerial image UAS: From flight planning to professional orthofoto and DEM”, *DIY Drones*, 18 April 2011. [http://diydrone.com/profiles/blog/show?id=705844%3ABlogPost%3A339917&commentId=705844%3AComment%3A342268&xg\\_source=activity](http://diydrone.com/profiles/blog/show?id=705844%3ABlogPost%3A339917&commentId=705844%3AComment%3A342268&xg_source=activity)

<sup>40</sup> Stanley, Jay, “Drone ‘Nightmare Scenario’ Now Has A Name: ARGUS”, *American Civil Liberties Union*, 21 February 2013. <https://www.aclu.org/blog/technology-and-liberty-free-speech-national-security/drone-nightmare-scenariow-has-physical>

observation capabilities using networks of UAVs may become attractive to governments as the costs fall, providing an infrastructure that could have a variety of commercial applications. It has also been suggested that “because they fly at such high altitudes, HALE UAS could potentially track every car trip in a city, or the times when lights in residences were turned on and off”.<sup>41</sup>

### 15.3.3 Geospatial analytics

RPAS are also being inserted into systems used for geospatial analysis and the capture of geographical information, supplementing or replacing functions traditionally performed by manned aircraft or satellites. This includes aerial photography, mapping, overlaying, 3D rendering techniques, spectral and hyper-spectral imaging, and remote sensing. Traditional cameras can be augmented with data provided by electromagnetic sensors such as visual spectrum, infrared and radar. UAVs can also carry photogrammetric equipment that promises faster and cheaper 3D-imaging (digital elevations and surface maps etc.) than traditional LiDAR remote sensing techniques.<sup>42</sup> These applications appear particularly promising from a commercial point of view, with a growing number of dedicated providers – for example Isis Geomatics, Orbit GeoSpatial Technologies and Swissdrones – offering a geospatial analytics and geographical information service using small and light RPAs.

### 15.3.4 Artificial intelligence and “smart drones”

Artificial intelligence already allows RPAS to communicate and coordinate with one another and carry out certain tasks autonomously. Developed for the military under the banner of “intelligence, surveillance, target acquisition and reconnaissance” (ISTAR), smart UAVs and RPAs are likely to prove no less attractive to the commercial sector as applications capable of identifying, tracking or delivering items autonomously are developed. “Smart surveillance” systems that are already in use include the detection of abnormal or suspicious behaviour using CCTV cameras, profiling and data mining techniques.<sup>43</sup> The Japanese company Secom is already marketing a “private security drone” that can “take to the air if there’s a break in and record what’s happening” and “track moving subjects with a laser sensor”.<sup>44</sup> Increasing autonomy in both the flight and vision capability of RPAS effectively merges some of these applications with the geospatial mapping techniques described above. These functionalities will enable commercial drones to search for and identify items, to track targets and deliver payloads autonomously.

Researchers are already adding facial recognition technology to UAS, causing alarm among civil liberties organisations.<sup>45</sup> The same technology could also be used, for example, by farmers to target certain crops with fertiliser or pesticide. Although they carry a heightened

---

<sup>41</sup> Villasenor, op. cit., 2013, p. 495

<sup>42</sup> LiDAR is a remote sensing technology that measures distance by illuminating a target with a laser and analysing the reflected light.

<sup>43</sup> See Wright, David, Michael Friedewald, Serge Gutwirth, Marc Langheinrich, Emilio Mordini, Rocco Bellanova, Paul De Hert, Kush Whadwa and Didier Bigo, “Sorting out smart surveillance”, *Computer Law & Security Review*, Vol. 26, 2010, pp. 343-354.

<sup>44</sup> Fingas, Jon, “Secom offers a private security drone, serves as our eyes when we’re away”, *Engadget*, 27 December 2012. <http://www.engadget.com/2012/12/27/secom-offers-a-private-security-drone/>

<sup>45</sup> Conte, Andrew, “Drones With Facial Recognition Technology Will End Anonymity, Everywhere”, *Business Insider*, 27 May 2013. <http://www.businessinsider.com/facial-recognition-technology-and-drones-2013-5>; “Domestic Unmanned Aerial Vehicles (UAVs) and Drones”, *Electronic Privacy Information Centre*, no date. <http://epic.org/privacy/drones/>

risk in terms of their impact on data protection and fundamental rights, the development of “smart surveillance” technologies also has the potential to minimise the amount of data that is collected by employing triggers and filters (or “artificial vision technologies”) that block out certain data or relay limited pictures – in much the same way as the new generation of body scanners.<sup>46</sup>

### 15.3.5 Sampling and detection technologies

A range of detection technologies including infrared sensors and microphones are already mounted on RPAs. As noted above, many are equipped with night-vision cameras or forward-looking infrared (FLIR) cameras that detect radiation emitted heat sources. RPAS may also be fitted with infrared search and track (IRST) systems capable of detecting and tracking objects that give off infrared radiation.<sup>47</sup>

The audio devices that can be fitted to RPAS range from the simple microphones that accompany basic video recording systems – for example the on board USB sound recorder or iPhone Voice Memo sound file that can be fitted to the mass-produced “Parrot AR drone” – to much more complex acoustic systems including passive radar for detecting noise emitting objects.<sup>48</sup> The former are limited because of the noise created by the engines and motors used to propel RPAS; the latter have been deployed in military UAS to “acoustically map” battlefield situations by locating and classifying all sources that are below a UAV in order to detect gunshots, armoured vehicles and other assets.

RPAs can also be mounted with biological sensors capable of detecting the airborne presence of various microorganisms and chemical sensors that use laser spectroscopy to analyse the concentrations of airborne elements.<sup>49</sup> The use of RPAS equipped with sampling and detection technologies by the commercial and public sectors is likely to grow significantly where they provide a safer or more cost-effective way of gathering samples in places that are difficult or dangerous to reach.

### 15.3.6 Telecommunications

RPAS can also be used as proxy satellites to carry communications systems and provide broadband services. Interest in this sector piqued recently with the announcement that Facebook is in advanced talks to buy Titan Aerospace, a producer of solar-powered UAVs.<sup>50</sup> Its “Solara 50” and “Solara 60” models can be launched at night using power from internal battery packs, then, when the sun rises, can store enough energy to ascend to 20 kilometres

---

<sup>46</sup> The aforementioned 3i project, for example, is using UAS equipped with “[A]utomated triggers and filters in the vision software that can filter images before they are recorded. So that any privacy sensitive images that are not of interest to the mission can be filtered out. The triggers can also be used to start recording only when an anomaly has been detected, e.g. a fire or an oil spill on the surface of the water”. See 3i project website, <http://www.2seas-uav.com/>

<sup>47</sup> Axe, David, “The Pentagon Has Figured Out How to Hunt Enemy Stealth Fighters”, *Medium.com*, 27 February 2014. <https://medium.com/war-is-boring/3acf9d25cd44>

<sup>48</sup> Adams Technology Pvt. Ltd., *Battlefield Acoustics – Microflown*”, *Adams Technology*, no date. <http://adams-tech.net/battlefield-acoustic.html>

<sup>49</sup> Omara, David, “Deploying Ruggedized Systems in Unmanned Military Vehicles for Advanced Air-Sea-Land Applications”, *Kontron Whitepaper*, no date. [http://www.kontron.com/resources/collateral/white\\_papers/whitepaper-aplabs-part1\\_en.pdf](http://www.kontron.com/resources/collateral/white_papers/whitepaper-aplabs-part1_en.pdf)

<sup>50</sup> Perez, Sarah, “Facebook Looking Into Buying Drone Maker Titan Aerospace”, *Techcrunch.com*, 3 March 2014. <http://techcrunch.com/2014/03/03/facebook-in-talks-to-acquire-drone-maker-titan-aerospace/>

above sea level where they can remain for five years without needing to land or refuel. As a communications relay, one Solara UAV can provide coverage for a radius of around 18 miles with a “constellation” of the craft able to create a persistent communications network.<sup>51</sup> Facebook is partnering with six telecommunications partners in a project called *Internet.org*, which aims to provide affordable Internet access to the five billion people for whom it is currently out of reach.<sup>52</sup> Google is involved in a similar initiative using a network of unmanned hot air balloons (a type of UAS) at the same altitude.<sup>53</sup> As noted above, these initiatives are expected to provide broadband telecommunications services at a fraction of the cost of their satellite-based counterparts. In addition to providing telecommunications services over small or wide areas, RPAS can also be fitted with equipment that enables the local interception of telecommunications.<sup>54</sup>

### 15.3.7 Non-lethal weapons

Despite or perhaps because of the controversy surrounding the use of armed drones for counter-terrorism purposes a variety of “less-lethal” or “non-lethal” payloads may one day be fitted to RPAs. Drones carrying “non-lethal weapons designed to immobilise [targets of interest]” have reportedly been considered for use along the US-Mexico border, and one police force in Texas has purchased a drone that the authorities have considered equipping with “a 12 gauge delivery system with lethal and less-lethal deliveries”.<sup>55</sup> The EU-funded AEROCEPTOR project is testing a UAS capable of stopping stolen vehicles.<sup>56</sup> BAE Systems has already successfully tested a drone that fires high-powered microwaves, also known as electromagnetic pulse weapons, capable of rendering all electrical systems in their path useless.<sup>57</sup> Similar weapons are being tested by NATO to paralyse the engines of moving vehicles.<sup>58</sup> A Texas-based company recently unveiled the “Chaotic Unmanned Personal Intercept Drone”, which is equipped with a “stun gun”.<sup>59</sup>

---

<sup>51</sup> Gallagher, Sean, “Almost orbital, solar-powered drone offered as ‘atmospheric satellite’”, *Ars Technica*, 18 August 2013. <http://arstechnica.com/information-technology/2013/08/almost-orbital-solar-powered-drone-offered-as-atmospheric-satellite/>

<sup>52</sup> See <http://internet.org/>

<sup>53</sup> Its project is called ‘Project Loon’, see <http://www.google.com/loon/>

<sup>54</sup> The technology that these UAVs are equipped with are known as ‘IMSI catchers’ or ‘stingrays’: essentially a false cell phone tower used for the interception and tracking of mobile phones that is virtually undetectable by the targets of surveillance (IMSI stands for International Mobile Subscriber Identity and is the unique identifier found in all ‘SIM cards’). IMSI catchers can be produced at very low cost and pocket-sized models are now available. See Robinson, Clarence. A. Jr., “Petite Cyber Drone Packs Punch”, *Defense Media Network*, 24 September 2011. <http://www.defensemedianetwork.com/stories/petite-cyber-drone-packs-punch/>

<sup>55</sup> Newsdesk, “Non lethal weapons on UAS along the U.S borders?”, *i-HLS*, 8.7.2013. <http://i-hls.com/2013/07/non-lethalweapons-on-uas-along-the-u-s-borders/>

<sup>10</sup> Geer, David, “Vanguard Shadowhawk”, *Tactical-Life*, 1 February 2012. <http://www.tacticalife.com/magazines/special-weapons/vanguard-shadowhawk/>

<sup>56</sup> See <http://www.aeroceptor.eu/>

<sup>57</sup> Military Technology, “A Look at the Future UAV Battlespace”, *Miltechmag.com*, 8 August 2012. <http://www.miltechmag.com/2012/08/a-look-at-future-uav-battlespace.html>

<sup>58</sup> Whitwam, Ryan, “NATO developing EMP beam that can stop suicide bombers”, *Geek.com*, 14 September 2013. <http://www.geek.com/science/nato-developing-emp-beam-that-can-stop-suicide-bombers-1570743/>

<sup>59</sup> “Why a drone called Cupid is fitted with a stun gun”, *BBC News*, 9 April 2014. <http://www.bbc.co.uk/news/technology-26930644>

The capabilities of UAS and RPAS are already wide-ranging and the amount of interest and investment suggests that they will continue to grow apace. The following section considers the ways in which these features are being used and may be used in the future.

## 15.4 Operators and applications

At least 16 of the 27 EU Member States are believed to own drones for military (combat and reconnaissance) or non-military (surveillance and detection) purposes. It is not known how many RPAS are in commercial or private ownership but according to lobby group UVS International “there are currently more than 1,000 approved and authorised civil operators in the European Union”.<sup>60</sup> As noted above, almost all of these are visual line-of-sight UAS flown at an altitude of less than 500 feet and weighing less than 25 kilograms.

As noted in the previous section, the capabilities of RPAS are already wide and varied and new capacities are continually being devised. It is also important to note that for all the concern about the use of RPAS by governments, there are already more drones being flown by hobbyists than there are by the military. Thanks to the “smartphone revolution” and other rapid advances in consumer electronics, private individuals have all the necessary elements to create their own RPAS.<sup>61</sup> These technological developments underpinned the emergence of “personal drone” communities dedicated to open-source drone research and development that are in turn creating commercial spin-offs and accelerating the already dynamic pace of innovation. In 2013 “DIY Drones”, an online social network, boasted more than 36,000 members worldwide.<sup>62</sup>

### 15.4.1 Classifying RPAS applications

There is no single accepted taxonomy for RPAS applications with different actors tending to adopt one of three approaches. The first is a “mission-based” taxonomy in which RPAS are classified according to the practical tasks they perform. Figure 3, below, for example, identifies seven core missions and a range of sub-missions<sup>63</sup>:

- Intelligence/Reconnaissance;
- Drones (in the classic sense of the meaning – as decoy or target practice);
- Transport;
- Extraction;
- Insertion (payload delivery);
- Communication;
- Surveillance.

---

<sup>60</sup> UVS International org., op. cit., 2014.

<sup>61</sup> Corcoran, Mark, “Drone journalism takes off”, *ABC News Online - Foreign Correspondent Special Report*, 21 February 2012. <http://www.abc.net.au/news/2012-02-21/drone-journalism-takes-off/3840616>

<sup>62</sup> See *DIY Drones* <http://diydrone.com/>

<sup>63</sup> Nehme, Carl, Jacob W. Crandall and M. L. Cummings, “An Operator Function Taxonomy for Unmanned Aerial Vehicle Missions”, *Twelfth International Command and Control Research and Technology Symposium*, Massachusetts Institute of Technology, 2007. [http://dodccrp.org/events/12th\\_ICCRTS/CD/html/papers/171.pdf](http://dodccrp.org/events/12th_ICCRTS/CD/html/papers/171.pdf)

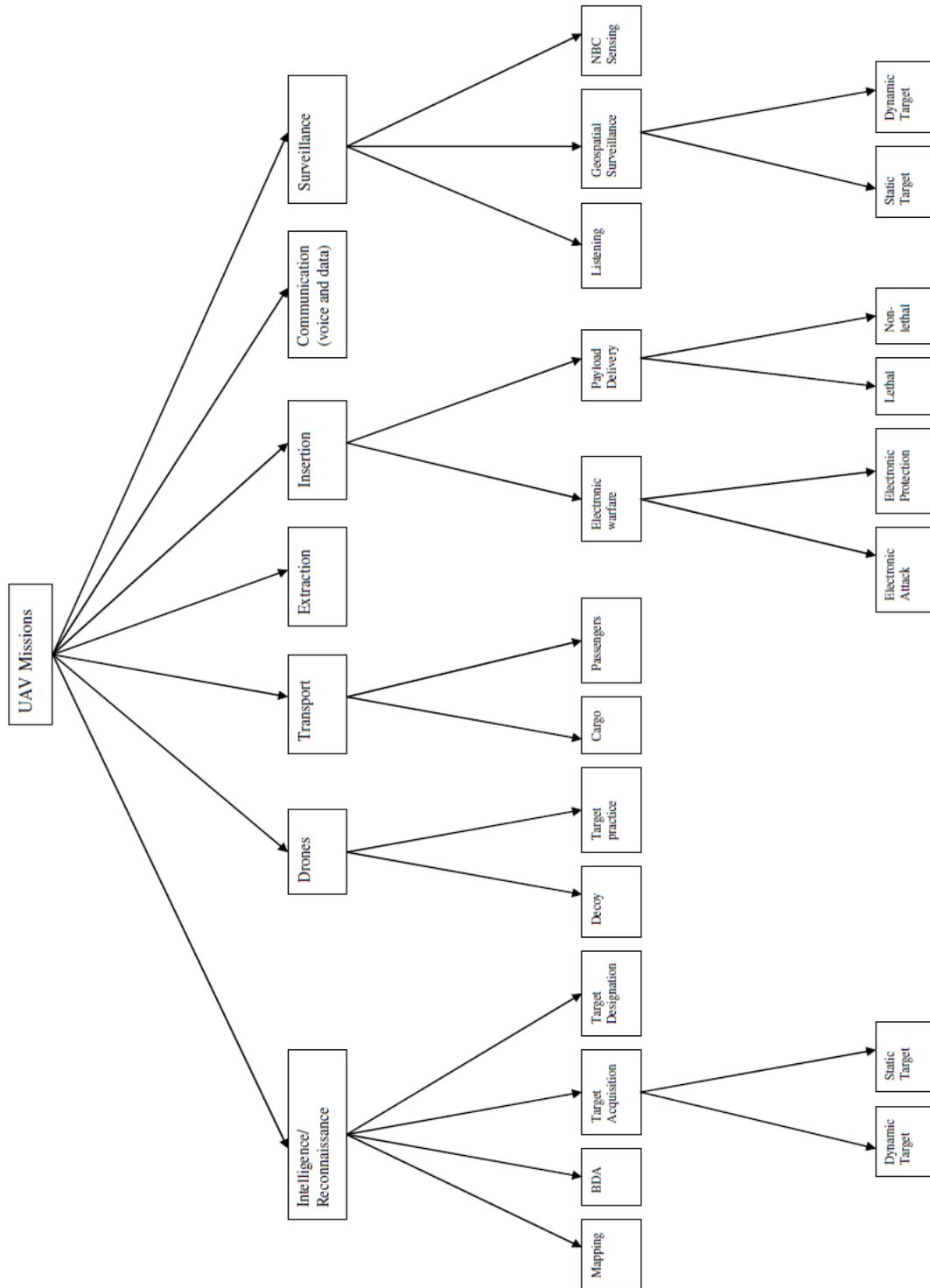


Figure 7: Taxonomy of RPAS missions

The second approach is user-based, with RPAS grouped according to who the aircraft is being used by. This is the approach taken by the International Civil Aviation Authority (ICAO) which regulates scheduled air passenger services, general aviation and commercial aerial work (agriculture, construction, photography, surveying, observation and patrol, search and rescue, aerial advertisement, etc.). The ICAO assumes that RPAS will be regulated in the same way as conventional aircraft as far as possible.

The third and most common approach is to group the applications into clusters of applications in different sectors.<sup>64</sup> This is the approach taken in the following subsections.

### *Civil contingencies*

Civil protection and contingencies includes emergency planning and response and the monitoring of critical infrastructure. It involves a wide range of public services and private actors and the sector is expected to see a strong take-up of RPAS. One of the most common current uses of RPAS is to monitor critical infrastructure (e.g. bridges, nuclear facilities, pipelines, ports and key buildings) and assets for routine checks and specific threats. After natural or manmade disasters the aircraft can also be used to monitor and assess damage, to deliver supplies and equipment, or to detect chemical, nuclear or biological hazards. In China the authorities have even developed a “smog clearing drone” in an attempt to tackle the chronic air pollution in that country.<sup>65</sup>

In relation to disaster relief, fire and rescue services are already using pilotless aircraft to ascertain the spread and extent of fires and to map the surrounding areas for hazardous materials. Agencies responsible for search and rescue and emergency response are using UAS and RPAS for navigating areas too dangerous or remote for them to reach using conventional equipment. For example in Japan RPAS are being used to prevent crews being exposed to harmful levels of radiation at the Fukushima Daiichi nuclear plant which was damaged by an earthquake and tsunami in March 2011.<sup>66</sup>

### *Energy*

The use of RPAS by the energy industry is also expected to grow significantly in the areas of infrastructure monitoring, servicing and exploration. The aircraft can be employed in those aspects of oil, gas and mineral exploration requiring aerial reconnaissance and geographical surveying and to remotely monitor existing production facilities. Oil refineries, chemical plants, nuclear plants, electricity plants, dams, pipelines and renewable energy may all one day employ RPAS for monitoring and safety purposes.<sup>67</sup> In the event of oil spills or the accidental discharge of other hazardous materials, RPAS may also be used to map contamination or the spread of pollutants.

### *Agriculture, forestry and fisheries*

The potential use of RPAS in agriculture, forestry and fisheries includes a range of resource management and monitoring applications.<sup>68</sup> Close-up surveillance of farm plots can provide high-resolution data capable of identifying invasive species, drought and blight, and other diseases. For remote sites or terrain that is difficult to cover by land vehicle, RPAS can

---

<sup>64</sup> See for example Frost & Sullivan, *Study Analysing the Current Activities in the Field of UAV – First Element: Status*, European Commission, 2007.

<sup>65</sup> Badkar, Mamta, “China May Use Drones To Kill The Smog Problem”, *Business Insider*, 5 March 2014. <http://www.businessinsider.com/china-is-testing-smog-clearing-drones-2014-3>

<sup>66</sup> For examples of the use of UAVs for civil contingencies see AUVSI, “Disaster Response” Increasing Human Potential, 30 April 2014. <http://increasinghumanpotential.org/category/news/spotlight/disaster/>

<sup>67</sup> Snider, Annie, “Drones fly into nascent civilian market ripe with energy, environmental applications”, *E&E Publishing*, 25 February 2012. <http://www.eenews.net/stories/1059958938>

<sup>68</sup> For example of these applications see Farmingdrones.com, “Farming Drones: UAVs in the Agriculture Industry”, 2013. <http://farmingdrones.com/>

provide quick and effective monitoring of food crops and livestock. Spraying fertilizers, pesticides and fungicides could also be done by RPAS with increasing autonomy capable of minimising human input. Surveying equipment mounted on RPAs can be used to plan planting and drainage and to map and estimate crop yields. Similar applications can be used for forestry and fisheries monitoring which also require cost efficient, wide area surveillance.

#### *Earth observation and remote sensing*

Earth observation and remote sensing currently carried out using imagery provided by satellites or samples collected by conventional aircraft will also be enhanced by the availability of low-cost RPAS. Much of the data used to monitor climate change and atmospheric pollution or to produce environmental impact assessments may be collected much more efficiently using unmanned systems. Environmental organisations and governments are already using unmanned systems to monitor forests for illegal logging, protect green space, track wildlife and prevent soil erosion.<sup>69</sup> These systems are particularly useful for covering large areas of land, particularly when ground operations are difficult or dangerous. Archaeology, geology, meteorology, oceanography and seismology are among the sectors that could benefit from novel surveying and remote sensing payloads mounted to RPAS.

#### *Communications and media*

As noted above, communications service providers are already investing in VHALE (very high-altitude long-endurance) UAS platforms that can be used as proxy satellites to provide communications networks. At lower altitudes RPAS may also be used to provide short-term, local communications networks. The film industry has already added mounted high-resolution cameras on RPAs to provide aerial footage and commercial broadcasters are using UAS for newsgathering. While many are excited about the prospect of “drone journalism”,<sup>70</sup> others are worried that UAS and RPAS will be used irresponsibly by “paparazzi” prepared to ignore any privacy and aviation regulations.<sup>71</sup> The use of RPAS for media and private photography purposes could also breach some national laws on trespass, stalking/harassment and commercial secrecy.

#### *Transport*

The retailer *Amazon* made headlines recently when it suggested that UAS could one day be used to deliver its products to consumers in an exercise widely regarded as a publicity stunt.<sup>72</sup> But while commercial passenger transport using UAS may be a long way off – despite the

---

<sup>69</sup> AUVSI “The Benefits of Unmanned Aircraft Systems: Saving Time, Saving Money, Saving Lives”, *Association for Unmanned Vehicle Systems International (AUVSI)*, no date. <http://epic.org/events/UAS-Uses-Saving-Time-Saving-Money-Saving-Lives.pdf>

<sup>70</sup> Goldberg, David, Mark Corcoran and Robert G. Picard, *Remotely Piloted Aircraft Systems and Journalism: Opportunities and Challenges of Drones in News Gathering*, Reuters Institute for the Study of Journalism, University of Oxford, 2013.

<sup>71</sup> According to Villasenor, “it would be optimistic to the point of naïveté to expect them to always operate UAS in a manner respectful of privacy considerations and in compliance with FAA safety regulations”. Villasenor, op. cit., 2013, p. 499.

<sup>72</sup> See for example, “Amazon testing drones for deliveries”, *BBC News*, 2 December 2013. <http://www.bbc.co.uk/news/technology-25180906>

level of automation in existing scheduled air services – the use of RPAS for some cargo transport and parcel delivery is a more realistic prospect. The United Arab Emirates, for example, says it plans to use unmanned aerial drones to deliver official documents and packages to its citizens as part of efforts to upgrade government services.<sup>73</sup>

### *Law enforcement*

The use of RPAS for policing and law enforcement purposes has provoked widespread criticism and concern from non-governmental organisations. However, police drones may be the exception rather than the rule, at least in the short term. The use of UAS for public order purposes is still controversial and typical police operations have been limited to obtaining after-the-fact crime scene images, search and rescue, and providing imagery for structure fire suppression and arson investigations.<sup>74</sup> Nevertheless a much wider range of applications for surveillance, tracking and public order purposes has been envisaged, although their use remains subject to the resolution of the regulatory and considerable data protection and human rights issues at stake. Police helicopters are very expensive to keep in the air and it is widely expected that UAVs could provide the same kind of aerial surveillance for a fraction of a cost. The European Commission has funded various research and development projects examining the police use of RPAS and UAS including for counter-terrorism (ARGUS 3D), non-cooperative vehicles (AEROCEPTOR), search-and-rescue (DARIUS, ICARUS, HELI4RESCUE) and situation awareness (AIRBEAM). In addition to domestic law enforcement, RPAS and UAS are also likely to play some role in EU maritime security policy, whether as part of the EUROSUR (border surveillance) system or for common EU security and defence operations, such as the on-going international anti-piracy mission of the Somali coast.

## **15.5 Summary and conclusions**

This chapter has examined the different capabilities and applications by examining their technical specifications, their capabilities and the operators and applications with which they may be associated. In addition to offering these details, the chapter also identifies alternative ways to classify RPAS. The examination as used to organise the size, capabilities and contexts in which RPAS may operate into a matrix that identifies contexts where different sized RPAS, with different flight heights, time airborne and payloads may be useful, and where RPAS with different capabilities (e.g., aerial photography, environmental sensing, etc.) may be useful. This analysis demonstrates the wide and varied current and potential applications of RPAS, which may significantly impact privacy, data protection and ethical obligations in Europe. Chapters 7 and 8 specify these issues and examine their applicability to these uses of RPAS.

---

<sup>73</sup> “UAE to use drones for citizen services”, *Al Jazeera*, 12 February 2014.  
<http://www.aljazeera.com/news/middleeast/2014/02/uae-use-drones-government-services-20142121717319272.html>

<sup>74</sup> Villasenor, op. cit., 2013, p. 467.

## 16 ANNEX B: REVIEW OF EUROPEAN AND NATIONAL RPAS SAFETY REGULATIONS

### 16.1 Introduction

This section examines the rules governing the use of RPAS in the European Union. The use of UAVs with a maximum take-off weight of 150 kg or more is subject to “*Regulation 216/2008/EC on common rules in the field of civil aviation and the establishment of the European Aviation Safety Agency*” (hereafter the “basic EASA Regulation”) under which UAS in this class are subject to the broadly the same requirements as conventional manned aircraft when using controlled (or “non-segregated”) airspace. The features of the basic EASA Regulation, which does not to apply to the use of aircraft by military, customs, police or similar national government agencies, are further examined in the following section.

Eleven EU Member States have already adopted national regulations on the commercial use of UAVs under 150 kg: Austria, the Czech Republic, Denmark, France, Germany, Ireland, Italy, Poland, Romania, Sweden and the United Kingdom. Belgium, Finland, Lithuania, the Netherlands and Slovenia do not yet have regulations that explicitly provide for the commercial use of UAVs but do permit some UAS flights on a case-by-case basis, as does Norway, which is not a Member States but is formally associated with EU policy development in many areas. Some of these states plan new laws or Directives to regulate the commercial use of UAS. An overview of the situation in these Member States is provided in the sub-sections below. The information was gathered through desk research and is derived in part from the data provided by the EU-funded ULTRA (Unmanned Aerial Systems in European Airspace) consortium.<sup>1140</sup> Where no publicly available information could be located, the information was requested from the civil aviation authority of the Member State. Reliable data was obtained for 15 of the 18 aforementioned countries (see Section 7.3, below).

The research examined the national regulations that apply to commercial operators of RPAS with a maximum take-off weight of up to 150 kg. The summaries that follow do not therefore refer to the rules that apply to private individuals who wish to use UAS for non-commercial purposes. In some cases, particularly for smaller classes of UAV, these activities are subject to dedicated rules covering the use of model aircraft. Some Member States also have accredited national associations of model aircraft users that provide guidance, training, permits or insurance for their members (for example the Austrian and Italian “Aeroclubs”, “Modelflyvning” in Denmark and the “Air Sports Federation” of Norway).

Among the key features of national laws regulating the commercial use of RPAS are pilot qualification and training, airworthiness and certification requirements, the provision of operating licences and aerial work permits, liability, insurance and operational (in-flight) rules. Most national laws place much greater restrictions on beyond the line of sight flights or prohibit them altogether. While there may be exceptions for the smallest classes of RPA (typically those with a maximum take-off mass of less than two, five or seven kilograms),

---

<sup>1140</sup> See in particular ULTRA Consortium, “Identification of gaps and new/modified regulations within the existing regulatory framework”, 2013.

<http://ultraconsortium.eu/index.php/deliverable?download=33:ultra-wp1-indra-d1-1-reg-gaps-pu-v3-0>

most national regulations require commercial operators to apply for a permit from the Civil Aviation Authority; the majority also require a dedicated aerial work permit if applicable. National UAS regulations usually place greater requirements or restrictions with regard to flights over or close to built-up or densely populated areas, gatherings of people, airports and other critical infrastructure; some states prohibit such flights altogether. The regulations also typically impose a minimum pilot age of 16 or 18 years and require pilots of larger classes of RPAS (those with a maximum take-off mass of greater than 20 or 25 kilograms) to have a professional pilot licence or RPAS qualification, though some states prohibit the use of these UAS altogether. In respect to the data protection rules that must be followed by RPAS operators, only the French, German, Norwegian and UK regulations appear to contain dedicated provisions, though other regimes refer to data protection legislation when listing the rules that must be respected by RPAS operators or recipients of aerial work permits. The following table provides a basic summary of how national RPAS regulations address key issues and, where data is available, the number of RPAS permits issued by national authorities to date.<sup>1141</sup> More detailed information is provided in the summaries of national regulations in the subsections below.

*Table 5: Overview of national RPAS regulations*

Country	Regulations allowing commercial use in place	RPAS qualification or pilot license	Operator or RPAS registration (# to date)	Permit to fly required	Aerial work allowed	BLOS allowed
Austria	Yes	> 5 kg	Yes	Yes	With permit	With permit
Belgium	No	No	Yes (10)	Yes	No	No
Czech Republic	Yes	> 7 kg	Yes (15)	Yes	With permit	No
Denmark	Yes	> 7 kg	Yes (12)	Yes	With permit	With permit
Finland	No	No	Yes	Yes	No	No
France	Yes	> 5 kg	Yes (431)	Yes	With permit	With permit
Germany	Yes (< 20 kg)	> 5 kg	Yes (est. 300)	Yes	With permit	No
Ireland	Yes	Yes	Yes (12)	Yes	Yes	No
Italy	Yes	> 25 kg	Yes	> 25 kg	With permit	Yes
Lithuania	Yes	Not known	Not known	Yes	With	Yes

<sup>1141</sup> UVS International Org., “Civil RPAS in the European Union”, *UVS International*, 17 February 2014. [http://uvs-international.org/phocadownload/03\\_11\\_articles\\_and\\_opinions/RPAS-in-the-EU\\_UVSI\\_140217.pdf](http://uvs-international.org/phocadownload/03_11_articles_and_opinions/RPAS-in-the-EU_UVSI_140217.pdf)

	(< 25 kg)				permit	
Netherlands	No	No	Yes (10)	Yes	With permit	No
Norway	No	No	Yes (43)	Yes	With permit	Segregated airspace
Poland	Yes	TBC	TBC	TBC	TBC	TBC
Spain	No	No	No	Yes	No	No
Sweden	Yes	> 7 kg	Yes (216)	Yes	With permit	With permit
UK	Yes	All	> 20 kg (250 est.)	Yes	Yes	Segregated airspace

## 16.2 EU Aviation Safety requirements

The basic EASA Regulation (216/2008/EC) extended EU competence in civil aviation from airworthiness and environmental standards to air operations, flight crew licencing and third-country permissions. Subsequent regulations have been adopted in each area and these have been codified into the “*European Civil Aviation Handbook*”.<sup>1142</sup> As noted above, these rules apply to RPAS with a maximum take-off mass greater than 150 kg with the exception of those UAVs used for military, policing or similar purposes. Despite these exemptions some of the rules set out in the basic EASA Regulation and implementing legislation extend by default to smaller and lighter classes of RPAS. Primarily, national regulations for light UAS (with a maximum take-off weight of between 20 and 150 kg) must be consistent with the basic Regulation so that safety is not arbitrarily compromised. This is so that the same standards apply, for example, to UAS weighing 140 kg and 160 kg (which would otherwise be subject to different regulations). A working group of “Joint Authorities for Rulemaking on Unmanned Systems” (JARUS) comprised of the EASA, EUROCONTROL and national CAAs working on harmonised regulations for RPAS has been established for this purpose. The extension of EU aviation safety requirements to the use of small and light UAS in the Member States is also happening in respect to insurance requirements as states apply the obligations on the operators of most aircraft to hold adequate levels of insurance in order to meet their liabilities in the event of an accident (under Regulation 785/2004/EC) to RPAS operators. Finally, RPAS operating in non-segregated airspace are subject to the same flight and air traffic control rules as manned aircraft regardless of weight. Thus from an operational perspective the 150 kg threshold does not apply where RPAS are flown in controlled European airspace. In the coming decade it is expected (following the current European RPAS Steering Group “Roadmap”) that the basic EASA Regulation will ultimately be extended in scope to all RPAS in the light class. The following subsections summarise the current national rules where applicable.

---

<sup>1142</sup> European Commission, “European Civil Aviation Handbook”, 9 October 2012.  
[http://ec.europa.eu/transport/modes/air/internal\\_market/handbook/part1\\_en.htm](http://ec.europa.eu/transport/modes/air/internal_market/handbook/part1_en.htm)

## 16.3 Requirements in European Member States

### Austria

**Overview:** New rules governing the use of UAS in Austria entered into force on 1 January 2014. Commercial operators must apply for permission to use RPAS from the Austrian Civil Aviation Authority (Austrocontrol).

**Commercial operations:** There are different requirements for UAS operating approval according to the weight of the aircraft and the area of operation and there are different rules for visual and beyond the line of sight RPAS. The weight classes (maximum take-off mass) are (a) up to 5 kg, (b) 5-25 kg and (c) 25-150 kg; the areas of operation are (i) undeveloped (no buildings), (ii) unpopulated, (iii) populated and (iv) densely populated (gatherings prohibited). The categories of UAS use are as follows, with different rules applicable in each scenario.



	UAS Class 1 (VLOS) – Area of Operation			
	I undeveloped (no buildings)	II unpopulated	III populated	IV densely populated (except crowds)
MTOW up to and including 5 kg	A	A	B	C
MTOW up to and including 25 kg	A	B	C	D
MTOW above 25 kg and up to and including 150 kg	B	C	D	D

Figure 8: Categories of RPAS operation in Austria<sup>1143</sup>

UAS flown beyond the line of sight are to be subject to the same requirements as civil aircraft and as determined by Austrocontrol.

**Pilot qualification:** Category B operations require a pilot qualification; category C and D operations require a pilot license.

**Additional rules:** Commercial operators for all operations (categories A-D) must be registered and insured and must keep flight logs. Models above 25 kg must be certified for category B, C and D operations. Flights are authorised to a maximum distance of 150 metres from the pilot. UAS operators must comply with all other relevant regulations including privacy, trade law and nature conservation.

<sup>1143</sup> AAI UAS Working Group, “NEW Austrian regulation for UAS Class 1 (VLOS): AAI Fact Sheet”, no date. [https://www.aai.at/wp-content/uploads/2014AAI\\_Factsheet\\_UAS\\_Class1\\_VLOS\\_AustrianRegulation\\_OverviewEnglish.pdf](https://www.aai.at/wp-content/uploads/2014AAI_Factsheet_UAS_Class1_VLOS_AustrianRegulation_OverviewEnglish.pdf)

## *Belgium*

**Overview:** There are no specific legal instruments governing the commercial use of light RPAS in Belgium, but Circular CIR/GDF-01 of 01 June 2005 on the use of model aircraft provides some guidance for RPAS. The “Belgian Certification Specification for UAV Systems” issued by the Belgian Civil Aviation Authority (CAA) in 2007 in accordance with its obligations under the basic EASA Regulation also provides for UAS with a maximum take-off mass of up to 150 kg to be used within visual of sight, subject to CAA.

**Commercial operations:** The commercial use of RPAS for aerial work as defined by the ICAO is not technically permitted but will be addressed by the new regulations that are expected in 2014.

**Pilot qualification:** Belgium does not have a remote pilot licensing procedure for RPAS but under the current rules the CAA verifies that the RPAS operator has received sufficient training. However, the forthcoming 2014 Royal Decree will likely stipulate that RPAS operators must have a remote pilot license or applicable certificate.<sup>1144</sup>

**Additional rules:** Flights have to be within the visual line of sight and not more than 400 meters from the pilot with a maximum authorized altitude of 120 meters. In addition, a distance of minimum 200 meters has to be maintained at all times between the UAV or RPA and any residential area. Derogations are possible with the permission of the CAA. The 2014 Royal Decree will also likely include provisions that RPAS must be registered with the CAA.<sup>1145</sup>

## *Czech Republic*

**Overview:** The use of RPAS in the Czech Republic is governed by Aviation Regulations adopted by the Civil Aviation Authority (CAA) in August 2011 and supplementary rules adopted in March 2012 setting out the procedures for issuing permits to fly.<sup>1146</sup> The regulations also contain national requirements for design, production, maintenance, modifications and operation of RPAS not covered by the basic EC Regulation.

**Commercial operations:** All commercial UAVs and pilots must be registered and authorised to fly by the CAA with an additional permit required for aerial work. Beyond the line of sight operations are generally prohibited though permission may be granted by the CAA in special circumstances. *RPAS must also have an identity label or registration mark that identifies the aircraft.*

**Pilot qualification:** UAVs with a maximum mass of less than 20 kg used for recreational or non-profit purposes are exempt from many of the requirements, including pilot qualifications and registration. Pilots of all UAVs used for commercial purposes must be registered and where the maximum operating mass is greater than 7 kg must also demonstrate competence. All pilots of UAVs with a maximum operating mass of more

---

<sup>1144</sup> Billen, Erika, “Belgian approach related to remotely piloted aircraft systems (RPAS) and their insertion into non-segregated airspace”, *Belgian Civil Aviation Authority*, Feluy, 20 November 2013.  
[http://eo.belspo.be/Docs/Resources/Presentations/beodays2013/402\\_Belgian\\_Approach\\_UAV.pdf](http://eo.belspo.be/Docs/Resources/Presentations/beodays2013/402_Belgian_Approach_UAV.pdf)

<sup>1145</sup> Ibid.

<sup>1146</sup> Czech Civil Aviation Authority, “L2 – Rules of the Air (National Implementation of ICAO Annex 2): Unmanned Aircraft Systems”, 25 August 2011; Czech Civil Aviation Authority, “Postupy Pro Vydání Povolení k Létání Letadla Bez Pilota na Palubě (Procedures for issuing RPAS permit to fly)”, CAA/S-SLS-010-1/2012, 1 March 2012.

than 20 kg must be qualified regardless of the purpose for which the aircraft is used. These and other requirements are shown in the following figure.

line	maximum mass	> 0,91 kg		< 7 kg		7 – 20 kg		> 20 kg		UAS BLOS
		recreational competition	commercial experimental research	recreational competition	commercial experimental research	recreational competition	commercial experimental research	recreational competition	commercial experimental research	
1	aircraft registration	no	yes	no	yes	no	yes	yes	yes	yes
2	pilot registration	no	yes	no	yes	no	yes	yes	yes	yes
3	pilot competence test	no	no	no	no	no	yes	yes	yes	yes
4	special authorization to flight	no	yes	no	yes	no	yes	yes	yes	yes
5	aerial work or private aviation activities permission	N/A	yes	N/A	yes	N/A	yes	N/A	yes	N/A
6	identification label only/ ID label and registration mark	no / no	yes / no	yes / no	yes / yes	yes / no	yes / yes	yes / no	yes / yes	yes / yes
7	min. distance T/O-LDG / persons / populated area	safe	safe	safe	safe	minimum 50/100/150	minimum 50/100/150	minimum 50/100/150	minimum 50/100/150	minimum 50/100/150
8	liability insurance: regular operation / airshow (millions CZK)	no / 0,25	acc. to EC Regulation Nr. 785/2004	no / 1	acc. to EC Regulation Nr. 785/2004	no / 3	acc. to EC Regulation Nr. 785/2004			
9	supervision	no	no	no	no	no	no	yes	yes	no
10	failsafe system	no	no	yes	yes	yes	yes	yes	yes	yes

Figure 9: Overview of regulatory requirements for the use of RPAS in the Czech Republic<sup>1147</sup>

**Additional rules:** UAV pilots must be stationary and must maintain visual control. Flights can only take place a safe distance from persons and densely populated areas (at least 150 metres). The use of UAVs with reactive engines (jet, rocket etc.) is prohibited.

### Denmark

**Overview:** Regulations on the use of UAVs weighing less than 25 kg in were adopted by the Danish Civil Aviation Administration (CAA) in January 2004, restricting the use of aircraft with an operating mass of 7 kg or more to model aircraft fields (BL 9-4, 9.1.2004). Supplementary regulations on the use of UAVs by approved organisations were adopted in 2012 (AIC B 22/12). RPAS operated beyond the line of sight of the pilot are subject to the same airworthiness and certification requirements as manned aircraft.

---

<sup>1147</sup> ULTRA Consortium, op. cit., 2013, p. 39.

**Commercial operations:** The 2012 regulations, modelled on the 2009 Swedish rules (see further below), set out four categories of RPAS classification: (i) models with a maximum take-off weight equal or less than 1.5 kg (Category 1A); (ii) models with a maximum take-off weight between 1.5 kg, and 7 kg (Category 1B); (iii) models with a maximum take-off weight between 7 kg, and 150 kg flying within sight of the pilot (Category 2); models equipped to be flown beyond the line of sight from the pilot and with a maximum weight of 150 kg (Category 3). *An approval from the CAA is required for all civil RPAS operations in Denmark.* Applications for Category 1A and 1B operations must include an insurance certificate, a description of the pilot's experience of flying the UAV in question and in the case of 1B UAVs a description of critical safety functions. Applications for Category 2 permits must also include a description of the UAV's intended activities as well as operation and maintenance manuals.

**Pilot qualification:** All RPAS pilots must be familiar with the aircraft's performance and control and must determine that the planned flight can be performed in a safe manner. Formal Pilot qualifications and dedicated training programmes are required for Category 2 and 3 RPAS and only holders of a Commercial Pilot License (CPL) can use RPAS in residential areas.

**Additional rules:** All RPAS operations must be conducted within the line of sight of the pilot at a maximum altitude of 100 metres above ground level in a manner that does not endanger the life or health of any living thing. RPAS must not be flown within 150 metres of built-up areas, main roads or gatherings of people, or within 5 kilometres of civilian airports or 8 kilometres of military airports. Any exception to these rules requires explicit permission from the CAA.

### *Finland*

**Overview:** The use of RPAS in Finnish airspace is regulated by article 6 of the Aviation Act, which sets out a derogations that provide for the operation of UAS with an operating mass of less than 150 kg. RPAS fulfilling the aforementioned condition are exempted from the Aviation Act provisions regarding aircraft registration, nationality and markings, airworthiness and emission restrictions, as well as pilot licence and qualification requirements. The Finnish Transport Safety Agency (TRAFI) is expected to introduce amendments in the near future to the national aviation regulation on aerial work with a view to regulating the commercial use of RPAS in non-segregated airspace.

**Commercial use:** No express permission but "An unmanned aircraft used for experimental or research purposes may deviate from the Rules of the Air in an area prohibited from other aviation or temporarily segregated for the purpose, provided that the exceptional procedure has been planned and is conducted so as not to compromise flight safety." In such cases the operator must obtain prior permission from TRAFI.

### *France*

**Overview:** The use of UAVs in France is regulated by a legislative Decree of 11 April 2002 (DEVA1207595A) on the use of French airspace by unmanned aerial vehicles and requires commercial UAS operators to be registered with the Directorate General for Civil Aviation (DGAC). A second Decree (DEVA1206042A, also 11 April 2002) contains standards for the design, use and pilot competence requirements for UAVs. Further rules are contained in a code developed under the auspices of the Ministry of Defence (Direction Générale de l'Armement, DGA) and NATO standards.

**Commercial operations:** Four scenarios for UAV use are defined in the French regulations with various operational constraints according to the category of the aircraft. These are:

- (i) direct line of sight operations outside populated areas with a maximum horizontal distance of 100 meters;
- (ii) beyond the line of sight operations outside populated areas with a maximum horizontal dimension of one kilometre and a height less than 50 m above the ground or obstacles;
- (iii) operations in urban areas or near gatherings of people or animals, in direct view of the remote pilot at a maximum horizontal distance of 100 meters;
- (iv) operations where activities are recorded including photography, observation and aerial surveys occurring outside populated areas not meeting the criteria of S-2 and with a flying height of less than 150 m above the ground or obstacles.

The following table shows the permissible operations, with specific authorisation from the DGAC required in most cases.

Operational Scenario	RPA Category				
	C (captive, Mass < 150 kg)	D (Mass < 2 kg)	E (2 Kg ≤ Mass < 25 kg)	F (25 Kg ≤ Mass < 150 kg)	G (Mass ≥ 150 kg)
S-1	✓	✓	✓	(1)	(1)
S-2	(1)	✓	✓	(1)	(1)
S-3	✓(2)	✓	(3)	(1)	(1)
S-4	(1)	✓	(1)	(1)	(1)

NOTES (1) Further evaluation required (authorisation on a "case by case" basis)  
 (2) For LTA RPA with mass < 25 Kg or heavier than air RPA with mass < 4 Kg  
 (3) For RPA with mass < 4 Kg

Figure 10: Summary of RPAS licensing requirements in France<sup>1148</sup>

**Pilot qualification:** The French regulations include dedicated rules on the competencies and responsibilities of RPAS pilots requiring them to have received practical training and a declaration of competence from the operator based on at least one demonstration flight. The requisite level of competence varies across seven different categories of UAV, and for visual and beyond the line of sight operations. The requisite competence for each category is set out in the Annex to the Decree. Theoretical knowledge and practical skills are required for all operators. For RPAS weighing more than 25 kg, pilots must be certified by the DGAC. For the most complex scenario (S-4, above), the pilot must hold a private aeroplane, helicopter or glider licence (PPL(A) or PPL(H)) and have 100 hours flying experience. They must also have 20 hours of practical experience of flying their RPAS in direct line of sight.

<sup>1148</sup> ULTRA Consortium, op. cit., 2013, p. 40.

**Additional rules:** A dedicated airworthiness certificate is required for all UAV's with an operating mass greater than 25kg. Operators of other UAV's must meet specific airworthiness requirements as applicable to the aircraft, including strength, performance, navigation, command and control requirements, testing and flight safety.

**Data protection:** If a commercial RPAS is equipped with a device capable of recording any type of visual data (e.g., photographs and videos taken from an image/video recording device/camera), then a declaration must be made to the DGAC at least two weeks before the operations take place. For UAVs equipped with a device capable of recording any type of data from outside the visible spectrum (e.g. radar, thermograph, infrared), a general authorisation is required.

### *Germany*

**Overview:** Germany has some of the most restrictive rules among European states that have regulated UAV flights. The regulations were adopted in May 2012 and stipulate that all flights must be within the line of sight of the pilot and that the operation of a UAV with a maximum take-off weight of more than 25 kg is prohibited unless the Länder (regional) aviation authority grants an exemption (Amendment No. 14 of the Aviation Act (LuftVG) dated 8 May 2012).

**Commercial operations:** Permission from a federal administrative body (Landesluftfahrtbehörden) is required to operate all RPAS, with models under 5 kg subject to a general permit and systems weighing 5 kg to 25 kg requiring individual permits for every flight. Applications must include a brief description of the planned operations, a certificate of insurance, written consent of the landowner or the local Council, a sketch of the flight area and the estimated time of flight including maximum height of ascent intended.

**Pilot qualification:** Permission to operate a UAV is dependent upon pilot competence and training. Permission for smaller (< 5 kg) models is usually granted where the pilot holds a model aircraft flying licence issued by the Federal Aviation Authority. Permits to fly larger models (5-25 kg) may include additional requirements in respect to training and licensing of the pilot and ground crew members.

**Additional rules:** Operations of RPA outside segregated airspace are only allowed in visual line of sight and at an altitude of no more than 100 metres above ground level. Permits to fly may also prohibit UAV operations above urban areas and gatherings of people. Larger UAVs with a maximum take-off mass greater than 25 kg may only be permitted to fly in the traffic circuit of an airfield or in segregated airspace.

**Data protection:** Permits to operate UAVs must be accompanied by declaration that the operations will not violate the individual rights of persons in Germany. Flights using photography or surveillance equipment must therefore demonstrate they will not violate German data protection law.

### *Ireland*

**Overview:** The Irish Aviation Authority (IAA) issued regulations covering the operation of Unmanned Aerial Systems in Ireland in May 2012 and updated them in September

2013.<sup>1149</sup> Registration requirements were introduced in November 2012. With the exception of model aircraft used for recreational purposes, RPAS may not be operated in Irish Airspace without a written permission from the IAA. Anyone wishing to use UAS for commercial operations must also hold an Aerial Work Permission issued by the IAA for that purpose. RPAs with an operating mass greater than 20kg must be registered unless an exemption is issued by the IAA and all RPAS with an operating mass greater than 150kg must be registered unless the operator has received an exemption.

**Commercial operations:** Where RPAS are to be used for commercial purposes such as filming, photography, survey, surveillance, etc., the operator must apply to the Authority for an Aerial Work Permission to cover such activity. Although there are no national regulations in force addressing certification or airworthiness, RPAS operators must ensure that the system is safe to use prior to the flight.

**Pilot qualification:** There are no recognised UAS qualifications but pilots and operators are expected to have “completed thorough ground instruction equivalent to that undertaken by aircrew for manned flights”, “through practical training in the operation and control of a RPAS in flight” and “periodical theoretical and practical examination” of proficiency.

**Additional rules:** RPAS must comply with Ireland’s visual flight rules in the same way as manned aircraft and must not be operated other than under the direct, unaided visual contact of the operator. RPAS with a mass of less than 20kg shall not be operated: beyond Visual Line of Sight (VLOS), further than 500 metres from the point of operation or at a height of more than 120 metres (400 feet) above ground level; within the confines of a congested area or within controlled airspace except with the written permission of the IAA; within an aerodrome traffic zone or closer than 8 kilometres (5 nautical miles) from an aerodrome boundary except with the written permission of the IAA; within 150 metres of any person, vessel, vehicle or structure not under the control of the aircraft operator or over any assembly of persons on the ground nor closer than 150 metres laterally from such an assembly (except during take-off or landing, when the aircraft must not be flown within 50 metres of any person, unless that person is under the control of the aircraft operator); closer than 2 kilometres from an aircraft in flight; unless there is in place a third party liability insurance policy covering the operation of the system which is acceptable to the Authority.

### *Italy*

**Overview:** The Italian National Authority for Civil Aviation (Ente Nazionale per l’Aviazione Civile; ENAC) adopted new regulations governing the operation of RPAS on 16 December 2013. The regulations will enter into force on 30 April 2014 and cover all UAV’s with a maximum take-off weight (MTOW) below 150kg. The regulation contains different sets of rules for model aircraft, UAVs with a MTOW of below 25kg and UAVs with a MOTW of between 25 and 150kg. UAVs in the larger category operating within Italian airspace must be registered by ENAC in the Remote Piloted Aircraft Register.

**Commercial operations:** For RPAS with a MTOW of below 25kg the regulations distinguish between “non-critical” and “critical” operations. The former are those operations that do not involve flights over congested areas, gatherings of people, urban areas, infrastructure, restricted areas, railway lines and stations, highways and industrial plants, and must be conducted in daylight conditions, in uncontrolled airspace, and at a

---

<sup>1149</sup> See Irish Aviation Authority. <https://www.iaa.ie/unmanned-air-systems>

minimum distance of 8 km from the perimeter of an airport and from the paths of approach/take-off to/from an airport. Any operations that do not meet these criteria are deemed “critical”. Those undertaking non-critical operations must submit a declaration to ENAC; those undertaking critical operations must apply for authorisation from ENAC. Simplified procedures exist for RPAS with MTOW less than or equal to 2 kg. Users of RPAS with a MOTW of between 25 and 150kg must obtain a Permit to Fly or Restricted Certificate of Airworthiness and an Operating Authorisation from ENAC.

**Pilot qualification:** All RPAS pilots are required to know the applicable rules of the air and be medically fit to fly. Knowledge can be demonstrated by the possession of a civil pilot’s license or of an Italian VDS (pleasure flying) pilot license. All pilots must have attended a specific training program for the RPAS. For RPAS with MTOW of less than 25 kg and used in non-critical operations, a declaration that the pilot is qualified for the system must be provided to ENAC. For RPAS in the 25-150kg category the pilot qualification must be recognised and verified by ENAC.

**Additional rules:** Operations in uncontrolled airspace must be conducted under VLOS conditions at a maximum distance of 70 metres for UAVs under 25kg and 150 metres for larger models. Operators wishing to use controlled airspace must submit an application to ENAC which may establish restrictions and conditions. Upon request ENAC may authorise operations for the pilot has no direct visual contact with the RPA or at greater distances (Extended Visual Line Of Sight). UAVs cannot be operated without valid, adequate third party insurance that complies with the minimum standards of EC Regulation 785/2004.

### *Netherlands*

**Overview:** In The Netherlands the use of RPAS is provided for in derogations and amendments to civil aviation law that have steadily extended the scope of operations that may be permitted. These provide, inter alia, for the remote piloting of aircraft, for directives from the Ministries of Transport and Defence on the use of light unmanned aircraft (with a maximum take-off mass of up to 150 kg). Separate regulations exist for fixed-wing UAS and “rotorcraft”. In 2011 the Dutch government published a new “Vision on Airspace” (Luchtruimvisie) promising new regulations on the commercial use of light UAS.

**Commercial operations:** There are currently three categories of UAS operation in the Netherlands as shown in the following table.

Parameter	Class 1	Class 2	Class 3
Visual Line Of Sight (VLOS)	yes	yes	yes
Radius	500 m	500 m	
Flying Height AGL	400 ft	400 ft	
Airspace	Rural, non-segregated	Urban, non-segregated or segregated	Rural, segregated

Figure 11: Categories of RPAS operations in the Netherlands<sup>1150</sup>

In principle only Class 1 operations will be permitted by the Dutch authorities although Class 2 operations are possible where there is a demonstrable public interest.

**Pilot qualification:** there are no recognised UAS pilot qualifications but all operators must demonstrate that the pilot and a mandatory observer are competent to ensure that the operation will be executed in a safe manner.

**Additional rules:** A risk analysis must be prepared for each flight. Third party insurance must be in place. RPAS operators must contact their local authority to obtain authorisation for the temporary use of terrain as an airfield (Terrein Uitzonderlijk Gebruik).

#### Norway

**Overview:** There are no dedicated rules on the use of UAS in Norway, though the Civil Aviation Authority has published a circular AIC-N 25/09 (29 June 2009) clarifying that permission for UAV operations can be granted through a specific application to the CAA.

**Commercial operations:** Each application is dealt with individually and there are no firm criteria or guidance for obtaining permission. Operations must be justified and appear safe before the CAA will grant permission.

**Data protection:** Norwegian law includes restrictions on aerial photography adopted in 1997 that apply to RPAS. Those wishing to engage in aerial photography must apply for permission to the National Security Authority.

#### Poland

**Overview:** Amendments to the Polish Aviation Act of 2002 allowing the use of civil UAVs in controlled airspace for the first time – subject to permission from the Civil Aviation Office – entered into force on 18 September 2011 (Dz. Urz. Nr 100, item 696). Flight safety features must be equivalent to manned aircraft and operations must follow

<sup>1150</sup> Haarbrinkhttp, R. B., “UAS for Geo-Information: Current Status and Perspectives”, *International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, Vol. 38-1/C22, 2011, p. 4. [http://www.geometh.ethz.ch/uav\\_g/proceedings/haarbrink](http://www.geometh.ethz.ch/uav_g/proceedings/haarbrink)

flight paths stipulated in the permit. The Aviation Act amendment provides for detailed regulations to be drawn-up jointly by the Polish Ministry of Transport and the Ministry of Defence but these have not yet been issued. Specific regulations covering RPAS with an operating mass of less than 30 kg are also expected.

### *Spain*

**Overview:** On 8 April 2014 the Spanish Air Navigation Safety Agency ("AESA") published a note stating commercial RPAS operations are not permitted in Spain. With the exception of military and experimental licenses, which may be granted subject to very restrictive conditions, only recreational flights in specific areas are permitted. AESA is currently drafting new rules that will enable the commercial use of light RPAS subject to safety and certification criteria.<sup>1151</sup>

### *Sweden*

**Overview:** The Swedish Board of Transportation (Transportstyrelsens författningssamling) regulations on UAVs were adopted in 2009 (TSFS 2009:88) and apply to the design, manufacture, modification, maintenance and use of unmanned aerial systems within Sweden, which are not covered by the basic EASA Regulation. Permission is required for all RPAS operations.

**Commercial operations:** There are four categories of UAV classification in the Swedish regulation:

- (i) models with a maximum take-off weight equal or less than 1.5 kg (Category 1A);
- (ii) models with a maximum take-off weight between 1.5 kg, and 7 kg (Category 1B);
- (iii) models with a maximum take-off weight between 7 kg, and 150 kg flying within sight of the pilot (Category 2);
- (iv) models equipped to be flown beyond the line of sight from the pilot and with a maximum weight of 150 kg (Category 3).

An approval from the Swedish Transport Agency is required for all civil RPAS operations. Applications for Category 1A and 1B operations must include an insurance certificate, a description of the pilot's experience of flying the UAV in question and in the case of 1B RPAS a description of critical safety functions. Applications for Category 2 permits must also include a description of the RPAS intended activities as well as operation and maintenance manuals. Category 3 permits are further dependent on a description of the organisation and management structures (including the CV's of the general, flight operations and technical managers).

---

<sup>1151</sup> Howell, Luis Lorente, "Spain: Authorities Working on Future Unmanned Aerial Vehicle (UAV) Regulation", *Bird & Bird News Centre*, 25 April 2014.  
<http://www.twobirds.com/en/news/articles/2014/spain/spain-authorities-working-on-future-unmanned-aerial-vehicle-regulation>

#	RPAS Category			Airworthiness Approval?	Operations Approval?	Operator Approval?	Pilot Qualification?
	MTOM (Kg)	Max. Kinetic Energy (J)	VLOS/BVLOS				
1A	≤ 1.5	150	VLOS	No	Yes	Yes	No
1B	1.5 < M ≤ 7	1000	VLOS	No	Yes	Yes	No
2	> 7	Any	VLOS	No	Yes	Yes	Yes
3	Any	Any	BVLOS	Yes	Yes	Yes	Yes

Figure 12: Overview of regulatory requirements for RPAS in Sweden<sup>1152</sup>

**Pilot qualification:** All UAV pilots must be familiar with their aircraft's performance and control and must determine that the planned flight can be performed in a safe manner. Formal pilot qualifications and dedicated training programmes are required for Category 2 and 3 UAVs (the former to the standard of a Private Pilot License (PPL), latter to the standard of a Commercial Pilot License (CPL)).

**Additional rules:** Category 1A UAVs may not be flown at night. For Categories 1A, 1B and 1C the RPAS must be operated well within sight of the pilot without aids and the within the operational range of the aircraft; any operation in controlled airspace requires permission from Air Traffic Controllers. All RPAS flights must be carried out at least 50m from humans, animals, vehicles and other property not involved in the operation.

#### United Kingdom

**Overview:** The UK Civil Aviation Authority (CAA) is widely recognised as having the most mature rules on RPAS operations in the world. Guidance was first issued in June 2002 and has subsequently been revised five times, most recently in August 2012.<sup>1153</sup> The Guidance sets out the safety requirements that have to be met, including airworthiness and operational standards, before an RPAS is allowed to operate in the UK. The guidance is also intended to assist those who are involved in the development of RPAS in order to ensure that the required standards and practices are met by all operators. It guidance covers both civilian and military RPAS activities. In January 2010 the CAA introduced new regulations that require operators of small unmanned aircraft used for aerial work purposes and those equipped for data acquisition and/or surveillance to obtain permission from the CAA before commencing a flight within a congested area or in proximity to people or property.

**Commercial operations:** All commercial RPAV pilots must have a Basic National UAS Certificate (BNUC) and operators must have appropriate insurance and permission to operate from the CAA. UAVs with operating mass of more than 20kg must also be registered and obtain airworthiness approval; those over 150kg must obtain a European Air Safety Agency permit as well as a UK Permit to Fly. These requirements are summarised in the following table.

<sup>1152</sup> ULTRA Consortium, op. cit., 2013, p. 38.

<sup>1153</sup> UK Civil Aviation Authority, *Unmanned Aircraft System Operations in UK Airspace – Guidance (Fifth Edition)*, CAP 722, 2012. <http://www.caa.co.uk/docs/33/CAP722.pdf>

Aircraft Mass	Airworthiness Approval?	Registration?	Operating Permission?	Pilot Qualification
20 kg and less	No	No	Yes (Note 1)	Yes (Note 1) BNUC-S™ or equivalent (Note 2)
More than 20 kg, up to and including 150 kg	Yes (Note 3)	Yes (Note 3)	Yes	Yes, BNUC™ or equivalent (Note 2)
More than 150 kg	EASA Permit to Fly or UK Permit to Fly in accordance with 'B conditions' (Note 3)	Yes	Yes	Yes, BNUC™, CPL(A) or equivalent (Note 2)

Figure 13: Summary of RPAS licensing requirements in the UK<sup>1154</sup>

*Note 1: Applicable for aircraft used for Aerial Work purposes or if flown within a congested area or close to people or property; Note 2: Equivalent pilot experience will be considered on a case-by-case basis during application for an operating permission; Note 3: It may be possible to obtain certain exemptions from the airworthiness and registration requirements.*

**Pilot qualification:** The Regulations and Guidance set out two use cases: “Case 0”, where one or more risk mitigating factors apply and the licensing regime is relaxed, and “Case 1”, where there are no risk mitigating factors and UAS pilot and commander qualifications apply (see further below). The risk mitigating factors are airspace segregation (separation from other users); visual line-of-sight operation (500 metres horizontally and 400 feet (122 metres) vertically); low aircraft mass. Depending on the mass and use case, operators may require a Basic National UAS Certificate (BNUC, or BNUC-S for small RPAS), Unmanned Commercial Pilot Licence (CPL(U)), Unmanned Airline Transport Pilot Licence (ATPL(U)). These requirements are summarised in the following table.

<sup>1154</sup> “Are UAV's Legal?”, *UnmannedTech.co.uk*, no date. <http://www.unmannedtech.co.uk/regulations.html>

Operating Mass (maximum)	Case 0	Case 1
7 kg or less	None, or BNUC-S™ or equivalent	BNUC-S™ or equivalent
More than 7 kg to 20 kg	None, or BNUC-S™ or equivalent	CPL(U) or equivalent
More than 20 kg to 150 kg	BNUC™ or equivalent	CPL(U) or equivalent
More than 150 kg	Industry Code of Practice, CPL(U) or ATPL(U) or equivalent	CPL(U) or ATPL(U) or equivalent

Figure 14: Overview of pilot qualification for the use of RPAS in the UK<sup>1155</sup>

**Additional rules:** With respect to “Small unmanned aircraft”, defined as having an operating mass of 20 kg or less, a person must not cause or permit any article or animal (whether or not attached to a parachute) to be dropped from a small unmanned aircraft so as to endanger persons or property; the person in charge of a small unmanned aircraft may only fly the aircraft if reasonably satisfied that the flight can safely be made and must maintain direct, unaided visual contact with the aircraft sufficient to monitor its flight path in relation to other aircraft, persons, vehicles, vessels and structures for the purpose of avoiding collisions. Small unmanned aircraft with a mass of more than 7kg must not be flown at a height of more than 400 feet or in Class A, C, D or E airspace or within an aerodrome traffic zone during the notified hours of watch of the air traffic control unit (if any) at that aerodrome unless the permission of any such air traffic control unit has been obtained.

**Data protection:** In respect to “Small unmanned surveillance aircraft”, defined as small RPAS which are equipped to undertake any form of surveillance or data acquisition, permission is required from the CAA to fly over or within 150 metres of any congested area; over or within 150 metres of an organised open-air assembly of more than 1,000 persons; within 50 metres of any vessel, vehicle or structure which is not under the control of the person in charge of the aircraft; or within 50 metres of any person.

## 16.4 Summary and conclusions

These guidelines suggest some key commonalities between different RPAS regulatory regimes as well as some key areas where considerations related to privacy, data protection and ethical issues can be inserted. With specific regard to key commonalities, many regulations relevant to RPAS include prohibitions against flying over people, animals or key infrastructure, as well as over populated or urban areas. Furthermore, almost all regulations require the operator to keep the RPAS in their line of sight at all times. Finally, most regulations also limit the height at which RPAS may fly. These limitations significantly diminish the potential privacy, data protection and ethical issues relevant to

<sup>1155</sup> Ibid.

RPAS. For example, restrictions on flying over people or populated areas diminishes the amount of information that can be collected about individuals on the ground, their property or their surroundings. The policy push at the EC level specifically intends to relax these restrictions and enable the use of RPAS for additional purposes and in additional contexts. However, these restrictions do provide some information about how responsible RPAS operators can limit the amount of data they collect about people, and subsequently limit their liabilities in terms of privacy and data protection. For example, they specifically encourage RPAS operators to consider how RPAS flights over people or infrastructure may impact those on the ground.

Furthermore, some RPAS regulations also seek to have, or offer an opportunity to introduce, specific controls associated with potential privacy, data protection or ethical impacts. Ireland, Italy and Sweden all require operators to obtain authorisation or aerial work permission before flying RPAS for civil purposes. Furthermore, the French and German systems require that operators declare that they will not breach privacy rules, data protection rules or fundamental rights. Authorisations could be used to check whether operators have carried out any privacy impact assessments or other risk assessments or to certify whether they have taken a specific course related to privacy, data protection and ethics. While the French requirement that RPAS operators using visual surveillance payloads must make a declaration to their national CAA is helpful, this could be extended to other payloads and could be combined with requirements to conduct an impact assessment. This extension to other payloads is important as the discussion in Chapter 4 demonstrates it is not only visual surveillance payloads that may have such impacts. Finally, the Czech, British and Irish requirements that larger RPAS have an identifying mark could assist in ensuring that RPAS are identifiable and transparent by enabling individuals on the ground to find out who is operating the RPAS and the purpose for which it is being used.



## HOW TO OBTAIN EU PUBLICATIONS

### Free publications:

- one copy:  
via EU Bookshop (<http://bookshop.europa.eu>);
- more than one copy or posters/maps:  
from the European Union's representations ([http://ec.europa.eu/represent\\_en.htm](http://ec.europa.eu/represent_en.htm));  
from the delegations in non-EU countries  
([http://eeas.europa.eu/delegations/index\\_en.htm](http://eeas.europa.eu/delegations/index_en.htm));  
by contacting the Europe Direct service ([http://europa.eu/europedirect/index\\_en.htm](http://europa.eu/europedirect/index_en.htm))  
or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (\*).

(\*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

### Priced publications:

- via EU Bookshop (<http://bookshop.europa.eu>).

### Priced subscriptions:

- via one of the sales agents of the Publications Office of the European Union  
([http://publications.europa.eu/others/agents/index\\_en.htm](http://publications.europa.eu/others/agents/index_en.htm)).

