14

Aerial Surveillance in the Digital Age

Drone-Related Privacy Concerns and the Protection of Other Human Rights

Skirgailė Žalimienė and Saulius Stonkus

14.1 INTRODUCTION

Innovation and digitalisation are perceived as an enabler of growth and a catalyst for the development of modern aviation in Europe.[1] In the view of the European Commission 'drones are a technology that is already bringing about radical changes, by creating opportunities for new services and applications, as well as new challenges'.[2] As it stated in the title of the Communication from the European Commission to the European Parliament and the Council, opening the aviation market to the civil use of drone technology marks '[a] new era for aviation'.[3] A similar view of drone technologies is shared by other countries.[4]

[1] For example, see European Commission, 'An aviation strategy for Europe', COM(2015) 598 final.

[2] The term 'drone' is often used to describe virtually any device that is able to fly without a pilot on board. A more technical term is unmanned aerial vehicle (UAV), which in conjunction with the equipment necessary to control it forms an unmanned aircraft system (UAS). The latter can be divided into remotely piloted aircraft systems (RPAS) or drones, which are piloted by remote pilots (humans), and autonomous aircraft, which do not require any human input during flight at all (with some exceptions, e.g., in accordance with Article 3 § 31 of Regulation (EU) 2018/1139 (commonly referred to as the 'Basic Regulation'), even when operating an autonomous aircraft, the remote pilot is still responsible for monitoring its course and remaining able to intervene and change the course at any time, whereas according to International Civil Aviation Organization (ICAO) terminology as autonomous aircraft are regarded as only those unmanned aircraft that do not allow pilot intervention in the management of the flight. Although the integration of fully autonomous aircraft into airspace is not expected to happen in the near future, the possibility for a remote pilot to intervene in a UAV flight and take over control is an important issue to discuss, as it is highly relevant when dealing with the liability for damage caused by autonomous aircraft (see International Civil Aviation Organization, *Unmanned Aircraft Systems* (2011), Cir 328, AN/190, ix, 3).

[3] See European Commission, 'A new era for aviation – opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner', COM(2014) 207 final.

[4] For example, the President of the US in his 2021 executive order acknowledged the 'great potential' of drones (White House, 'Executive Order on Promoting Competition in the American Economy', 9 July 2021, www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/) and the UK Regulatory Horizons Council pointed out in a 2021 exploratory study that 'drone technology, powered by advances in robotics,

Indeed, the commercial drone industry has flourished in recent years, and the technology, which a few decades ago was exclusively a part of modern military equipment, became available to the general public. The number of drone operations in Europe alone has already come close to manned aviation.[5] Drones are widely used by various state authorities, as well as commercial entities and private persons for purposes as diverse as policing, search and rescue, environment monitoring, film-making, mapping, agriculture, and entertainment.

Drones are undoubtedly very useful and represent tremendous opportunities. With evolving drone technologies various new business models emerge, such as parcel delivery by air, aerial photography, air taxis, and drone journalism. Drones offer new services and applications going far beyond traditional aviation and allow us to perform existing services in a more affordable and environmentally friendly way by increasing the efficiency of different activities. In addition, drones are hard to replace, especially in difficult situations; for example, when restoring communications or carrying out search and rescue missions after natural disasters. Even the pandemic caused by the COVID-19, when physical contact was restricted, became an opportunity to demonstrate the extremely wide range of possible drone applications and promote their use in everyday life, seeking a more positive public attitude towards the application of drone technology.[6] In principle, the capabilities of drones are almost limitless, making them applicable in any field.

However, among other reasons, to meet safety requirements, modern drones as a rule are equipped with high-end technologies, which can capture, store, and upload online or to other devices huge amounts of data, including private data. Drones can range in size from being big enough to carry a human to as small as a hummingbird, and very quiet, making them extremely hard to notice. In

battery power and artificial intelligence, is "on the cusp" of delivering new breakthrough capabilities' (Regulatory Horizons Council, 'The regulation of drones: an exploratory study' (2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1029834/rhc-drones-report.pdf).

[5] See ICAO, 'European Regional Aviation Safety Plan 2020–2022' (2020), www.icao.int/EURNAT/EUR%20and%20NAT%20Documents/EUR%20Documents/EUR%20RASP/Archive/EUR%20RASP%202020-2022_EN.pdf, 23.

[6] For example, in Lithuania, drones were used to monitor public places for possible violations of quarantine restrictions and to warn residents if such violations were observed (see Vilnius city website, 'Vilniuje karantino priežiūrai į dangų pakelti dronai' (2020), https://vilnius.lt/lt/2020/03/30/vilniuje-karantino-prieziurai-i-dangu-pakelti-dronai/); one man in Cyprus used a drone to take his dog for a walk while he was in lockdown because of COVID-19 (see L. Eadicicco, 'A man used a drone to take his dog for a walk while he was in lockdown because of the coronavirus' (2020), www.businessinsider.com/video-dog-being-walked-by-drone-cyprus-coronavirus-lockdown-2020-3?r=US&IR=T); in China and India drones were used to spray public areas with disinfectant – and such utilisation of drones was also considered in the UK (see Z. Kleinman, 'Coronavirus: should the UK use drones to disinfect public spaces?' (2020), www.bbc.com/news/health-52109824); even UNICEF prepared guidelines for how drones can be used to combat COVID-19 (see UNICEF, 'How drones can be used to combat COVID-19' (2020) www.unicef.org/supply/media/5286/file/%20Rapid-guidance-how-can-drones-help-in-COVID-19-response.pdf).

addition, drones are piloted remotely or, in some cases, using advanced artificial intelligence (AI) technology that is able to develop flight patterns with the only human input specifying the destination,[7] which makes it very hard to trace the actual drone users.[8] Therefore, with the use of drones private data can not only be easily accessed and collected in areas where people reasonably expect privacy, but it can also be achieved anonymously. Hence, along with all the new possibilities and benefits, the massive deployment of drones in public life also bring serious privacy issues, as drones like any other technology can be misused. According to Zuboff, in the absence of countervailing restrictions and sanctions, every digital application that *can* be used for surveillance and control *will* be used for surveillance and control, irrespective of its original intention.[9] Therefore, emerging drone technology requires an appropriate legal response, as it is impossible to disinvent the technology – drones are here to stay.

Privacy is a constitutional value recognised in the vast majority of countries. According to Privacy International, one of the world's major watchdogs on surveillance and privacy, over 130 countries in every region of the world have constitutional statements regarding the protection of privacy.[10] The right to privacy is also enshrined in major international and regional human rights documents (conventions, declarations, charters, etc).[11] Although legal scholars often acknowledge that drones pose a serious threat to privacy, in making such a conclusion they simply presume the potential dangers, usually limiting themselves to a few examples, but

[7] Such autonomous drones are already available on the market (see the Skydio Autonomy website at www.skydio.com/skydio-autonomy).

[8] Owing to the issue of identifying the actual pilot of a drone, a new type of profession – drone detectives (forensics) – has evolved in recent years (e.g., see P. Marks, 'How police catch drone-flying criminals' (2017), www.bbc.com/future/article/20170731-how-cops-catch-drone-flying-criminals).

[9] S. Zuboff, *In the Age of the Smart Machine: The Future of Work and Power* (New York: Basic Books, 1988); S. Zuboff, 'The surveillance paradigm: be the friction – our response to the new Lords of the Ring' (2013), *Frankfurter Allgemeine Zeitung*, www.faz.net/aktuell/feuilleton/the-surveillance-paradigm-be-the-friction-our-response-to-the-new-lords-of-the-ring-12241996.html.

[10] For more information see Privacy International, 'What is privacy?', 23 October 2017, https://privacyinternational.org/explainer/56/what-privacy.

[11] For example, Article 5 of the American Declaration of the Rights and Duties of Man, Bogotá, 2 May 1948, 1 Annals of the OAS. 130 (1949); Article 12 of the United Nations Declaration of Human Rights, GA Res. 217A (III), UN Doc. A/810, at 71 (1948); Article 8 of the European Convention on Human Rights, Rome, 4 November 1950, Council of Europe, European Treaty Series No. 5; Article 17 of the International Covenant on Civil and Political Rights, New York, 16 December 1966; Article 11 of the American Convention on Human Rights, San Jose, 22 November 1969, 1144 UNTS 123; Article 16 of the Convention on the Rights of the Child, New York, 20 November 1989, 1577 UNTS 3; Article 10 of the African Charter on the Rights and Welfare of the Child, Addis Ababa, 11 July 1990, 29 ILM 1458; Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, New York, 18 December 1990, 2220 UNTS 3; Article 7 of the Charter of Fundamental Rights of the European Union, Nice, 7 December 2000, Official Journal of the European Union (OJ), 2000/C 364/01; Articles 16 and 21 of the Arab Charter on Human Rights, Tunis, 22 May 2004, 12 ILM 307); Article 21 of the Association of Southeast Asian Nations Human Rights Declaration, Phnom Penh, 18 November 2012, 52 ILM 1010, etc.

do not discuss in more detail the privacy violations that the use of drone technology can cause.

A deep understanding of drone related threats to privacy, the diverse ways that drone technology can affect privacy, the way it can interfere with other human rights, the various restrictions to drone use that may be implicated, and the need to mitigate these tensions by maintaining the right balance together form the cornerstone to ensuring the successful integration of drones in modern society. Therefore, the aim of Section 14.2 is to present a broader discussion of the major privacy concerns arising from the mass introduction of drones into everyday life,[12] provide a more detailed description of the relevant threats, as well as to highlight possible clashes between privacy and other human rights invoked by the use of drone technology, emphasising the need to strike a fair balance between these conflicting values. In Section 14.3, the current regulatory developments on drone technologies in relation to identified human rights concerns are analysed, focusing primarily on the European context and seeking to determine the main shortcomings that must be rectified in order to effectively manage the threats associated with the use of drones.

14.2 DRONES AND THEIR USE: MAJOR PRIVACY CONCERNS AND OTHER HUMAN RIGHTS ISSUES

Article 7 of the Charter of Fundamental Rights of the European Union (the Charter) holds that everyone has the right to respect for his or her private and family life, home, and communications. While Article 8 of the Charter enshrines protection of personal data, stating in its first paragraph that everyone has the right to the protection of personal data concerning him or her. The Court of Justice of the European Union (CJEU) when applying Articles 7 and 8 of the Charter has noted on numerous occasions that Article 7 of the Charter, regarding the right to respect for private and family life, contains rights corresponding to those guaranteed in Article 8(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), and that 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 of the ECHR. In accordance with Article 52(3) of the Charter, Article 7 of the Charter is thus to be given the same meaning and the same scope as Article 8(1) ECHR, as interpreted by the case law of the European Court of Human Rights (ECtHR).[13] The same is true for other rights protected by the Charter which correspond to rights guaranteed by the ECHR. Therefore, the CJEU

[12] For the purposes of this chapter, the right to privacy is regarded as including the right to protection of personal data (except if stated otherwise).

[13] See, for instance, Case C-345/17, *Sergejs Buivids v Datu valsts inspekcija* [2019], ECLI:EU:C:2019:122, para. 65; Case C-460/20, *TU, RE v Google LLC* [2022], ECLI:EU:C:2022:962, para. 59.

often relies on the jurisprudence of the ECtHR when interpreting the meaning and the scope of the rights recognised by the Charter. Nevertheless, this provision does not prevent EU law providing more extensive protection.

The ECtHR has emphasised in its case law that the concept of private life extends to aspects relating to personal identity, such as pictures of a person.[14] A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development.[15] It primarily presupposes the individual's right to control the use of that image, including the right to refuse its publication, which is also relevant for publications online.[16] And namely in the light of drone technology, the most evident threat to privacy is when using a drone equipped with a camera, which usually comes as a standard element of drone equipment and is able to capture images (photographs and videos).

The right to one's image is recognised virtually worldwide as a part of the right to private life or regarded as a separate right with a special provision in national laws to protect it; nevertheless, it is closely related to the right to respect for private life.[17] Therefore, the unlawful surveillance of a person and recording, collecting, processing, or using that data may lead to the violation of his or her right to privacy. As evident from the jurisprudence of the ECtHR, everyone, including people known to the public, has a legitimate expectation that his or her private life will be protected.[18] However, a person's reasonable expectation of privacy is a significant though not necessarily conclusive factor, since there are occasions when people knowingly or intentionally involve themselves in activities that are or may be recorded or reported

[14] See *Schüssel v. Austria* (dec.), Application no. 42409/98, Decision of 21 February 2002; *Von Hannover v. Germany*, Application no. 59320/00, Judgment of 24 June 2004, para. 50; *von Hannover v. Germany (no. 2)* [GC], Applications nos. 40660/08 and 60641/08, Judgment of 7 February 2012, para. 95.

[15] See *López Ribalda and Others v. Spain* [GC], Applications nos. 1874/13 and 8567/13, Judgment of 17 October 2019, paras. 87–91 and the references cited therein.

[16] See *Reklos and Davourlis v. Greece*, Application no. 1234/05, Judgment of 15 January 2009, para. 40; *von Hannover v. Germany (no. 2)* [GC], Applications nos. 40660/08 and 60641/08, Judgment of 7 February 2012, para. 96.

[17] For example, see S. R. Barnett, 'The right to one's own image: publicity and privacy rights in the United States and Spain' (1999) 47 *The American Journal of Comparative Law* 4, 555–81; E. H. Reiter, 'Personality and patrimony: comparative perspectives on the right to one's image' (2002) 76 *Tulane Law Review* 3, 673–726; H. Trouille, 'Private life and public image: privacy legislation in France' (2000) 49 *International and Comparative Law Quarterly* 1, 199–208.

[18] See *von Hannover v. Germany (no. 2)* [GC], Applications nos. 40660/08 and 60641/08, Judgment of 7 February 2012, para. 97; *Sciacca v. Italy*, Application no. 50774/99, Judgment of 11 January 2005, para. 29; *Reklos and Davourlis v. Greece*, Application no. 1234/05, Judgment of 15 January 2009, para. 40; *Von Hannover v. Germany*, Application no. 59320/00, Judgment of 24 June 2004, para. 51; *Leempoel & S.A. ED. Ciné Revue v. Belgium*, Application no. 64772/01, Judgment of 9 November 2006, para. 78; *Standard Verlags GmbH v. Austria (no. 2)*, Application no. 21277/05, Judgment of 4 June 2009, para. 48; *Hachette Filipacchi Associés (ICI PARIS) v. France*, Application no. 12268/03, Judgment of 23 July 2009, para. 53.

in a public manner.[19] Therefore, there are a number of elements relevant to the consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises.[20] As a result, according to the ECtHR, it is relevant if the surveillance exceeded an extent of exposure possible to a passer-by or to security observation and beyond a degree surpassing that which the individual could possibly have foreseen.[21]

In this sense the use of drones in the light of the right to privacy is quite problematic. Drones can be very small and quiet, and so hard to detect, and the ever-decreasing size of various drone components constantly leads to less detectable devices. Owing to these features, people may often not be aware of being surveilled; among other issues, it creates opportunities for more frequent voyeuristic attacks. Drones can also be very light and easy to carry, they can take off quickly and almost from anywhere, usually there is no need for lengthy preparation and/or special take-off and landing sites. In addition, they are relatively cheap. These are definitely the advantages of drones in comparison with conventional aircraft, as they make aerial surveillance, which was previously quite expensive and usually available only to state authorities, easily accessible to everyone. However, this poses a serious challenge to ensuring adequate protection of the right to privacy because it may lead to systematic mass surveillance, which can in turn cause serious negative psychological consequences in society by making people feel less free and force a sort of self-censorship by restricting their behaviour.

Private life, in the ECtHR's view, includes a person's physical and psychological integrity; the guarantee afforded by Article 8 of the ECHR is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings.[22] There is therefore a zone of interaction with others, even in public contexts, which may fall within the scope of private life.[23] The ECtHR, for example, has found video surveillance of public places where the visual data are recorded, stored, and disclosed to the public as falling under Article 8 of the ECHR.[24] According to the ECtHR, although monitoring the

[19] See *Bărbulescu v. Romania* [GC], Application no. 61496/08, Judgment of 5 September 2017, para. 73; *Köpke v. Germany* (dec.), Application no. 420/07, Decision of 5 October 2010.

[20] See *P. G. and J. H. v. the United Kingdom*, Application no. 44787/98, Judgment of 25 September 2001, para. 57.

[21] See, for instance, *Peck v. United Kingdom*, Application no. 44647/98, Judgment of 28 January 2003, para. 62.

[22] See *Von Hannover v. Germany*, Application no. 59320/00, Judgment of 24 June 2004, para. 50; also, mutatis mutandis, *Niemietz v. Germany*, Application no. 13710/88, Judgment of 16 December 1992, para. 29; *Botta v. Italy*, Application no. 21439/93, Judgment of 24 February 1998, para. 32.

[23] See, mutatis mutandis, *P. G. and J. H. v. the United Kingdom*, Application no. 44787/98, Judgment of 25 September 2001, para. 56; *Peck v. United Kingdom*, Application no. 44647/98, Judgment of 28 January 2003, para. 57.

[24] In particular, the disclosure to the media for the broadcast use of video footage of an applicant whose suicide attempt was caught on surveillance television cameras was found to be a serious interference with the applicant's private life, notwithstanding that he was in a public place at the time (see *Peck*

actions of an individual in a public place using photographic equipment that does not record the visual data does not, as such, give rise to an interference with the individual's private life,[25] the recording of the data and the systematic or permanent nature of the record may give rise to such considerations, regardless of whether the surveillance is covert or overt.[26] Therefore, the ECtHR has concluded that the compilation of data by security services on particular individuals, even without the use of covert surveillance methods, constitutes an interference with the applicants' private lives.[27] This comes in line with 'mosaic theory', developed in light of the Fourth Amendment to the US Constitution.[28] According to this theory, a certain amount of data as an aggregated whole can implicate reasonable expectations of privacy even though the separate constituent parts of such data do not.[29] Hence, it is evident that private life is a broad term 'not susceptible to exhaustive definition'.[30]

Threats posed by drones equipped only with sound recorders and no ability to capture video or images should also not be neglected, as they can secretly listen to and record private conversations. Moreover, modern technologies make it possible to perform a sort of human profiling based on timbre and other voice characteristics and/or identify a particular person (i.e., a speaker) using voice recognition technology.[31] Accordingly, voice recordings, as well as images in the case of facial recognition, can be further processed into biometric data using advanced technologies, which makes it possible to relate real people with their profiles in the digital domain. Such unforeseen use of photographs, videos, and sound recordings can constitute an interference with the right to private life.[32] In the ECtHR's view, the rapid development of increasingly sophisticated techniques allowing, among

v. United Kingdom, Application no. 44647/98, Judgment of 28 January 2003, paras. 57–63, 87). For example, video surveillance in a supermarket by an employer (see *López Ribalda and Others v. Spain* [GC], Applications nos. 1874/13 and 8567/13, Judgment of 17 October 2019, para. 93) and in a university amphitheatre (see *Antović and Mirković v. Montenegro*, Application no. 70838/13, Judgment of 28 November 2017) also fall within the scope of Article 8 of the ECHR.

[25] See, for instance, *Herbecq and the association 'Ligue des droits de l'homme' v. Belgium*, Applications no. 32200/96 and 32201/96, Decision of 14 January 1998.

[26] See *P. G. and J. H. v. the United Kingdom*, Application no. 44787/98, Judgment of 25 September 2001, para. 57; *Peck v. United Kingdom*, Application no. 44647/98, Judgment of 28 January 2003, para. 59.

[27] See, for instance, *Rotaru v. Romania* [GC], Application no. 28341/95, Judgment of 4 May 2000, paras. 43–4; *Amann v. Switzerland* [GC], Application no. 27798/95, Judgment of 16 February 2000, paras. 65–7.

[28] See, e.g., O. S. Kerr, 'The mosaic theory of the Fourth Amendment' (2012) 111 *Michigan Law Review* 3, 311–54; D. C. Gray and K. D. Citron, 'A shattered looking glass: the pitfalls and potential of the mosaic theory of Fourth Amendment privacy' (2013) 14 *North Carolina Journal of Law & Technology* 2, 381–429.

[29] See Kerr, 'The mosaic theory of the Fourth Amendment', 311–54.

[30] See, for instance, *P. G. and J. H. v. the United Kingdom*, Application no. 44787/98, Judgment of 25 September 2001, para. 56; *Peck v. United Kingdom*, Application no. 44647/98, Judgment of 28 January 2003, para. 57.

[31] See, e.g., R. Singh, *Profiling Humans from their Voice* (Singapore: Springer, 2019).

[32] See, for instance *Peck v. United Kingdom*, Application no. 44647/98, Judgment of 28 January 2003.

other things, facial recognition and facial mapping techniques to be applied to individuals' photographs without a doubt amounts to interference with his or her right to private life within the meaning of Article 8 § 1 of the ECHR, which makes the taking of their photographs and the storage and possible dissemination of the resulting data problematic.[33] Therefore, recording and storing voices may also in itself constitute an interference with the right to private life. As the ECtHR has ruled in the case *P. G. and J. H. v. the United Kingdom* (§ 59–60), the recordings taken for use as voice samples cannot be regarded as falling outside the scope of the protection afforded by Article 8 of the ECHR.

The risk of interference with the right to privacy may arise not only when photographing and/or filming individuals but also their private property.[34] Even when such images (e.g., of an enclosed courtyard) are not related to an identified or identifiable natural person, it may still infringe one's privacy, as the right to respect for private life also includes the inviolability of the home. While drones can easily overcome fences of any size and construction or even fly inside buildings,[35] where persons reasonably expect to maintain their privacy, the inviolability of the home gains even more significance.[36] In addition to this, cameras used in

[33] See *Gaughran v. the United Kingdom*, Application no. 45245/15, Judgment of 13 February 2020, para. 70.

[34] E.g., Article 29 of the Data Protection Working Party in Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones (01673/15/EN, WP 231), adopted on 16 June 2015, has concluded that the processing of images (including images of houses, vehicles, driving licence plates, etc.) related to an identified or identifiable natural person carried out by the data processing equipment on-board a drone may have an impact on privacy and data protection, and therefore trigger the application of data protection legislation.

[35] E.g., an indoor security camera drone was recently introduced to the market (see J. Siminoff, 'Introducing Ring always home cam: an innovative new approach to always being home' (2020), https://blog.ring.com/products-innovation/introducing-ring-always-home-cam-an-innovative-new-approach-to-always-being-home/).

[36] Even legal entities (corporations) can rely on the right to privacy, although, e.g., CJEU has excluded legal persons from data protection (see Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [2010] ECR I-11063, paras. 52, 53 and 87). In this regard, the ECtHR has emphasised in the case *Bernh Larsen Holding AS and others v. Norway*, that the word 'home', appearing in the English text of Article 8 of the ECHR (the word '*domicile*' in the French text has a broader connotation) covers residential premises and may extend also to certain professional or business premises. It includes not only the registered office of a company owned and run by a private individual, but also that of a legal person and its branches and other business premises. Accordingly, in certain cases concerning complaints under Article 8 of the ECHR related to the search of business premises and the search and seizure of electronic data, the ECtHR found an interference with 'the right to respect for home' and 'correspondence'. Nevertheless, according to the jurisprudence of ECtHR, in such cases the Contracting States retain their entitlement to 'interfere' to the extent permitted by paragraph 2 of Article 8 of the ECHR, and that entitlement might well be more far-reaching where professional or business activities or premises were involved than would otherwise be the case (see *Bernh Larsen Holding AS and others v. Norway*, Application no. 24117/08, Judgment of 14 March 2013, paras. 104–5 and the references cited therein). The corporate right to privacy is acknowledged in US legal doctrine as well, yet this topic is still controversial (see, e.g., E. Pollman, 'A corporate right to privacy' (2014) 99 *Minnesota Law Review* 1, 27–88; also K. Robinson, 'Corporate rights and individual

modern drones have advanced optical and digital zoom capabilities, which make it possible to capture high resolution images from a long distance.[37] Combined with advanced infra-red, radar, laser, holographic, computer, and other technologies and theoretical scientific knowledge, drones equipped with high zoom cameras enable to form a detailed spatial (3D) projection from captured data, revealing in detail the geometric, physical, and other properties of objects and their interrelationships.[38] Furthermore, this feature (high zoom capability) is also an issue in relation to privacy concerns as far as it helps to maintain the secrecy of surveillance by facilitating a large distance from the subject of interest, in addition to the anonymity of the drone pilot owing to remote control. In turn, the individual not being aware of ongoing surveillance is one of the most significant challenges to privacy in relation to drones, when either way the actual transgressor (pilot) may remain anonymous.

Drones can capture and store a great variety of data – beside sound recordings and standard images (photos or videos), drones can also capture thermal images, geo-location and geo-spatial data, which poses no less threat to privacy than the former. For example, thermal image technology makes it possible to see through walls, obtaining an image of people and objects inside buildings without even entering.[39] In this respect, for example, the Supreme Court of the United States in the case *Kyllo v. US* (2001) has ruled that the use of such technology to capture the internal thermal image of a person's home constitutes a search within the meaning of the Fourth Amendment to the United States Constitution.[40] It may also be concluded from ECtHR jurisprudence that sophisticated surveillance methods with enhanced video monitoring capabilities, such as thermal imaging, infra-red, or night vision, will likely interfere with Article 8 of the ECHR, as they surpass the ordinary surveillance measures available to the general public and thus exceed reasonable expectations of privacy in certain circumstances (making individuals exposed in an unforeseen way).[41]

Most basic modern drones also have Global Positioning System (GPS) functionality, accelerometers, inclinometers, and other sensors necessary for safe drone operation and the functioning of such features as 'return home', 'follow me', and

interests: the corporate right to privacy as a bulwark against warrantless government surveillance' (2015) 36 *Cardozo Law Review* 6, 2283–320).

37 E.g., one of the largest drone manufacturers DJI offers drones with the integrated aerial zoom camera Zenmuse Z30, which has a 30x optical zoom and 6x digital zoom with a total magnification up to 180x (see DJI website at www.dji.com/lt/zenmuse-z30/info).

38 See B. Jiang, J. Yang, and H. Song, 'Protecting privacy from aerial photography: state of the art, opportunities, and challenges' (2020) *IEEE Conference on Computer Communications Workshops*, 799–804.

39 See J. Celso, 'Droning on about the Fourth Amendment: adopting a reasonable Fourth Amendment jurisprudence to prevent unreasonable searches by unmanned aircraft systems' (2014) 43 *University of Baltimore Law Review* 3, 461–94.

40 *Kyllo v. US*, 533 US 27 (2001).

41 See, for instance, *Peck v. United Kingdom*, Application no. 44647/98, Judgment of 28 January 2003, para. 62.

so on.[42] Meanwhile recording the GPS data makes it possible to track a person's movement and can interfere with the right to private life, especially in conjunction with other captured data (e.g., images).[43] In fact, GPS coordinates are often automatically assigned to images (photos and videos) taken by drones as metadata, making it possible to identify the specific location they were captured. This is a clear example of how new data (in a qualitative sense) can be created by combining various pieces of data, especially with the use of AI-driven data mining and data harvesting techniques, which make it possible to unearth new interesting and unexpected patterns and relationships between existing, at first sight completely unrelated, data by discovering the missing details of the information and linking such data in a logical way, creating a detailed picture of the subject under study. As Gray and Citron have noticed, 'technological advances have made it possible for public and private actors to watch us and to know us in ways that once seemed like science fiction'.[44] In this regard, the aforementioned mosaic theory becomes significant. The CJEU also shares this view and emphasises that various data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as their everyday life habits, permanent or temporary places of residence, daily or other movements, activities, their social relationships, and the social environments they frequent.[45]

With advanced computer programs and AI technology, besides providing such functions as face recognition or identification of vehicle licence plate numbers or autonomously tracking the target, drones can also perform many other tasks; for example, intercept or block mobile communications,[46] recognise and scan radio-frequency identification (RFID) tags (i.e., information stored in them), which form the basis of various identification methods (identity cards, pass cards, etc.),[47] and much more. However,

[42] The 'follow me' function can also enable a drone to autonomously track a specified 'target' (person of interest), without any input from the pilot.

[43] See, for instance, *Uzun v. Germany*, Application no. 35623/05, Judgment of 2 September 2010, paras. 49–53.

[44] See Gray and Citron, 'A shattered looking glass', 386–7.

[45] See, for instance, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238, para. 27.

[46] Tapping and other forms of the interception of communications represent a serious interference with private life and correspondence (see, for instance *Dragojević v. Croatia*, Application no. 68955/11, Judgment of 15 January 2015).

[47] RFID is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal, or person; it is often used in passports, for access control (e.g., key cards), tap-and-go credit card payments, and tracking various assets. RFID systems are becoming increasingly used to support internet of things deployments. Combining the technology with smart sensors and/or GPS technology enables sensor data including temperature, movement, and location to be wirelessly transmitted (see S. Amsler and S. Shea, 'RFID (radio frequency identification)', www.techtarget.com/iotagenda/definition/RFID-radio-frequency-identification). At the same time, RFID technology can be used to transmit information about the drone and its pilot (e.g., registration number, pilot's

drones can be hacked and intercepted themselves, making it not only possible to use them for the unlawful collection of private data by taking over their control, but also to retrieve the data already stored in the drone's internal memory. Therefore, despite the fact that personal data may sometimes be gathered by drones lawfully, it is necessary to subsequently ensure adequate protection of such data. However, the cybersecurity of drones is questionable,[48] especially if even state-of-the-art military drones can be hacked.[49] This low level of cybersecurity poses a threat to drone technology itself, as it can erode public confidence in such technology, and drones, which are now rapidly gaining popularity among modern society, may no longer look so attractive.[50]

By using a well-established wireless (mobile) network, drones are able to transmit captured data directly to other devices (including other drones), upload the data online, or simply broadcast publicly over the internet, including through popular social networks and other platforms. Similarly, drones connected to a mobile network can download data from various databases and combine it with real time surveillance data. Notwithstanding, storing and processing personal data relating to the private life of an individual also falls within the right to privacy.[51] This raises another issue regarding the cross-border exchange of data,[52] while at the same time ensuring adequate protection of personal data.[53]

location) to devices on the ground; e.g., passers-by, smartphones. This is an example of how a technology that is seen as posing threat to privacy can also be employed to help protect it.

[48] Several studies have showed the vulnerability of drone cybersecurity. E.g., see R. Altawy and A. M. Youssef, 'Security, privacy, and safety aspects of civilian drones: a survey' (2016) 1 *ACM Transactions on Cyber-Physical Systems* 2, 1–25; B. Siddappaji and K. B. Akhilesh, 'Role of cyber security in drone technology', in K. B. Akhilesh and D. P. F. Möller (eds.), *Smart Technologies* (Singapore: Springer, 2020), pp. 169–78.

[49] E.g., see L. Mungin, 'Iran claims released footage is from downed U.S. drone' (2013), CNN World, https://edition.cnn.com/2013/02/07/world/meast/iran-drone-video/.

[50] Public acceptance of UAV technology is recognised as key to the growth of drone services. E.g., see Riga declaration on remotely piloted aircraft (drones) 'Framing the future of aviation', Riga, 6 March 2015, https://eu2015.lv/images/news/2016_03_06_RPAS_Riga_Declaration.pdf; also European Parliament resolution of 29 October 2015 on safe use of RPAS, commonly known as UAVs, in the field of civil aviation (2014/2243(INI)), OJ J C 355.

[51] See, for instance, *Amann v. Switzerland* [GC], Application no. 27798/95, Judgment of 16 February 2000, paras. 65; *Copland v. United Kingdom*, Application no. 62617/00, Judgment of 3 April 2007, para. 43.

[52] In recent decades, information, including personal data, has been rapidly exchanged in both private and public sectors, and personal data is being transferred beyond national territories (see S. Žaltauskaitė-Žalimienė et al., *Europos Sąjungos Pagrindinių teisių chartijos taikymas supra- ir nacionaliniu lygmenimis* (Vilnius: Vilnius University Press, 2019), p. 237). Such growing cross-border movement of personal data owing to the ongoing economic and social integration in the world caused by globalisation will inevitably pose greater threats to privacy in the future, as national regulations in this area differ in many respects and the practice has already shown the shortcomings of existing protection mechanisms (see, for instance, Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, ECLI:EU:C:2015:650; Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, ECLI:EU:C:2020:559).

[53] E.g., despite various legislative attempts, there is still legal uncertainty in relation to data exchange between the EU and US, which led to announcements by Meta, the parent company of Facebook

The ability of drones to communicate (interact) with each other makes it possible to form an interoperable drone *swarm*, making it possible to monitor multiple targets at the same time and/or maintain continuous long-term aerial surveillance using different drones in shifts. This kind of communication, as part of the Internet of Things, has led to the emergence of the terms Internet of Drones or Internet of Drone Things.[54] As the President of the European Commission, Ursula von der Leyen, has stressed in her political guidelines for 2019–24, the Internet of Things (thus, also the Internet of Drones) is connecting the world in new ways, as physical devices and sensors are now linking up with each other so that huge and increasing amounts of data are being collected; although data and AI are ingredients for innovation, in order to release that potential it is crucial to balance the flow and wide use of data while preserving high privacy standards, as well as ensuring safety and security.[55] This is a serious issue because combining drones with huge databases and aggregation software controlled by private entities may lead to significant shifts in the distribution of power in society, creating powerful private entities that can tend to abuse the available data. The AI technology used to manage such data can also lead to discrimination by misinterpreting individual behaviour and creating prejudices.

Technological development in recent decades has been notably moving towards higher levels of automation in various areas, including air transport.[56] Automation plays an ever-increasing role in aviation, where many processes are in fact already entrusted to technologies capable, for example, of keeping an aircraft on course, identifying conflicting traffic, proving resolution advisories to avoid potential mid-air collisions, plotting and executing optimal descent profiles, and in some cases even controlling aircraft take-off or landing, with the pilot becoming a simple observer of these high-end systems.[57] Accordingly, aviation is increasingly focusing on the application of AI technology in the air transport sector,[58] including, for

and Instagram, that it may be forced to shut down its two popular social media platforms in Europe as a result of the strict EU data protection regulation (see S. Shead, 'Meta says it may shut down Facebook and Instagram in Europe over data-sharing dispute', 7 February 2022, CNBC, www.cnbc.com/2022/02/07/meta-threatens-to-shut-down-facebook-and-instagram-in-europe.html).

[54] See, e.g., Z. Lv, 'The security of Internet of drones' (2019) 148 *Computer Communications*, 208–14; A. Nayyar, B.-L. Nguyen, and N. G. Nguyen, 'The Internet of drone things (IoDT): future envision of smart drones', in A. Luhach et al. (eds.), *First International Conference on Sustainable Technologies for Computational Intelligence. Advances in Intelligent Systems and Computing* (Singapore: Springer, 2020), pp. 563–80; R. Krishnamurthi, A. Nayyar, and A.E. Hassanien (eds.), *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead* (Cham: Springer International Publishing, 2021).

[55] See U. von der Leyen, *Political Guidelines for the Next European Commission 2019–2024* (Luxembourg: Publications Office of the European Union, 2019), p. 13.

[56] As one of the laws formulated by Zuboff states, in *In the Age of the Smart Machine*, everything that can be automated will be automated.

[57] See ICAO, *Unmanned Aircraft Systems* (2011), Cir 328, AN/190, at 5.

[58] The progress of the whole aviation sector is based on AI technology (see European Organisation for the Safety of Air Navigation, *The FLY AI Report – Demystifying and Accelerating AI in Aviation / ATM* (2020)).

example, the use of passenger face recognition technology at airports to speed up the boarding process,[59] or the automation of air traffic control to increase aviation safety, inter alia by safely integrating drones into the non-segregated airspace.[60] As already mentioned, AI technology is widely used in drones themselves, with drones being regarded as high-risk AI systems.[61] This aspect of the digital transformation reflects the fourth industrial revolution, which is 'characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres' and will change society in unpredictable ways.[62] In this regard the European Commission predicts that the use of drones is likely to grow significantly, as automation enables them to fly further, and declares that 'European rules promote the sustainable growth of drone operations, paving the way for a digital future.'[63]

Unmanned aerial vehicles are exceptional in the sense that they are able to integrate many different modern technologies into a single whole, acting like a platform (base) that additionally gives wings to these technologies. Drones are essentially flying robots capable of capturing and processing extremely large amounts of various types of data, and this process can be more or less automated, which makes them perfect surveillance tools. Despite the fact that the majority of the technologies used in drones (e.g., cameras, sound recorders, GPS sensors) are not so new, and that therefore they are quite well known (including the threats they pose to privacy), drone technology (specifically, their ability to fly and the remote control option) brings these to the next level of danger, making private data, which is so valuable and often regarded as the new currency, more vulnerable than ever.[64] Just as the emergence of instantaneous photographs in the gutter press was once seen as a game changer, requiring us to re-estimate the protection of the right to privacy

[59] E.g., such technology is already implemented in practice at Narita International Airport in Tokyo (see K. Ishihara et al., 'Introducing Face Express, a new boarding procedure using face recognition (One ID at Narita Airport)' (2021) 16 *NEC Technical Journal* 1, 49–53.

[60] E.g., the U-space initiative in Europe, aimed at ensuring safe and secure management and integration of drones in airspace, is largely based on AI and machine learning (see SESAR, 'Smart ATM: U-space and urban air mobility', www.sesarju.eu/U-space). It is estimated that over time U-space services will evolve as the level of automation of drones increases and advanced forms of interaction with the environment are enabled (including manned and unmanned aircraft) (see SESAR, *U-space Blueprint* (Luxembourg; Publications Office of the European Union, 2017)).

[61] See draft report of the European Parliament Committee on Legal Affairs with recommendations to the Commission on a Civil liability regime for AI, 2020/2014(INL), 27 April 2020, 24. Also see B. C. Stahl, *Artificial Intelligence for a Better Future. An Ecosystem Perspective on the Ethics of AI and Emerging Digital Technologies* (Cham: Springer, 2021), p. 63.

[62] K. Schwab, *The Fourth Industrial Revolution* (Geneva: World Economic Forum, 2016).

[63] See European Commission, 'Aviation safety', https://transport.ec.europa.eu/transport-modes/air/aviation-safety-policy-europe_en.

[64] See G. Clayton, 'Safeguarding the world's new currency' (2002) 36 *Information Management Journal* 3, 18–24; C. Gates and P. Matthews, 'Data is the new currency' (2014) *Proceedings of the 2014 New Security Paradigms Workshop*, 105–16.

in order to meet the demands of society,[65] today drones invoke the same necessity owing to the increased scope of aerial surveillance they afford.[66]

Along with the mass introduction of drones in everyday life, sophisticated surveillance techniques emerge.[67] Traditionally, the state was seen as the source of such surveillance concerns,[68] but increased usage of modern technologies in public life (including the commercial drone industry) has created what Zuboff calls 'surveillance capitalism', which stems from the exploitation and control of human nature as private entities control most of the data.[69] The immense deployment of drones in public life may lead to the so-called chilling effect on the fundamental right to privacy, creating a Panopticon environment, where individuals feel less free and may resort to self-preservation (self-censorship) by restricting their behaviour to avoid being watched even when no drones are in operation.[70] This requires an appropriate legal response, especially in light of increasing public concerns regarding bulk interception.

However, some data is captured and processed by drones for safety and security reasons – modern drones inevitably must capture, store, and process some specific data in order to ensure their safe and secure integration into the non-segregated airspace and our everyday life. For example, it would be hard (if not impossible) to safely use a long-distance drone without a camera, gyroscope, GPS, and other modern sensors, especially when performing BVLOS flights.[71] Such sensors are also necessary for the proper functioning of Detect and Avoid technology, which can automatically avoid obstacles (including humans); therefore, requiring the drone to constantly monitor the surrounding environment and process that data in real time. GPS data is also crucial for the proper operation of the return home function, which can safely return a drone to its take-off or other pre-arranged location; for example, in case of the loss of the remote control or when the drone battery is

[65] See S. D. Warren and L. D. Brandeis, 'The right to privacy' (1890) 4 *Harvard Law Review* 5, 193–220.

[66] It has to be noted that all of the aforementioned features of modern drones are just the tip of the iceberg. Owing to the extremely rapid progress in technological development and the wide range of possible uses of drones, it is difficult to foresee all the challenges that may arise to privacy from the use of drones. Therefore, this chapter does not aim to provide an exhaustive list of these challenges, essentially limiting them to the main threats that best illustrate the issues in the area in question.

[67] Now drones are widely used by state authorities, commercial entities, and private persons for various purposes, examples being mapping, agriculture, environment monitoring, filmmaking, policing, search and rescue, and entertainment.

[68] See D. Lyon, *Surveillance Society: Monitoring Everyday Life* (Buckingham: Open University Press, 2001).

[69] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Public Affairs, 2019).

[70] See, e.g., R. Clarke, 'The regulation of civilian drones' impacts on behavioural privacy' (2014) 30 *Computer Law and Security Review* 3, 286–305; R. L. Finn, D. Wright, and M. Friedewald, 'Seven types of privacy', in D. Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (Dordrecht: Springer, 2013), pp. 3–32; P. McBride, 'Beyond Orwell: the application of unmanned aircraft systems in domestic surveillance operations' (2009) 74 *Journal of Air Law and Commerce* 3, 627–62.

[71] Beyond Visual Line of Sight.

running low. This is also necessary for the geo-fencing technology used in restricted areas for security reasons (e.g., above nuclear plants, military bases, government buildings, airports).[72] Therefore, aviation safety and security implications must also be taken into account when analysing the privacy concerns raised by the use of drones because the collection, processing, storage, and use of certain (private) data may inevitably be necessary.

Moreover, although increasing drone usage primarily raises privacy concerns, at the same time, drone technology creates new opportunities for diverse applications and services. Therefore, the restrictions imposed on their use in order to protect the right to privacy may interfere with other human rights, necessitating a fair balance to be struck between these conflicting values.

As already stated, evolving drone technologies have led to the emergence of new business models, such as parcel delivery by air and aerial photography. Accordingly, drones are now widely used in various professions, including estate agents, photographers, cinematographers, advertisers, and others. In this regard, Articles 15 and 16 of the Charter enshrine that everyone has the right to engage in work and to pursue a freely chosen or accepted occupation, and the freedom to conduct a business in accordance with the law is recognised. Freedom to choose an occupation and the right to engage in work is also recognised by other international human rights documents.[73] Therefore, any restrictions on drone usage that affect professions dependent on this technology may be regarded as interfering with the freedom to choose an occupation, the right to engage in work, and the freedom to conduct a business.

Such restrictions may also interfere with the right to property, as protected by Article 17 of the Charter, Article 1 of Protocol No. 1 of the ECHR, among others. This is not only the case in the meaning of the use and peaceful enjoyment of drones themselves as physical possessions, but also in a broader sense. For example, the ECtHR has concluded in its case law that the economic interests connected with running a business include 'possessions' for the purposes of Article 1 of Protocol No. 1 of the ECHR, and maintenance of the licence can be regarded as one of the principal conditions for carrying on a business; thus its withdrawal could constitute interference with the right to the 'peaceful enjoyment of [one's] possessions'.[74] This

[72] Accordingly, Regulation (EU) 2018/1139, whose principal objective is to establish and maintain a high uniform level of civil aviation safety in the EU (Article 1), states that in order to ensure safety for people on the ground and other airspace users during the operation of unmanned aircraft, unmanned aircraft must be safely controllable and manoeuvrable, as necessary under all anticipated operating conditions including following the failure of one or, if appropriate, more systems, and must be operated only if it is in airworthy condition and where the equipment and the other components and services necessary for the intended operation are available and serviceable (see Annex IX to Regulation (EU) 2018/1139, establishing the essential requirements for unmanned aircraft).

[73] See, e.g., Article 23(1) of the Universal Declaration of Human Rights.

[74] See, for instance, *Traktörer Aktiebolag v. Sweden*, Application no. 10873/84, Judgment of 7 July 1989, para. 53; *Capital Bank AD v. Bulgaria*, Application no. 49429/99, Judgment of 24 November 2005, para. 130.

means that any legal regulation that may restrict the use of drones for business purposes in favour of the protection of the right to privacy, as a general (public) interest, must be reasonably proportionate to the aim sought. In other words, a fair balance must be struck between these conflicting values, and the requisite balance will not be found if the person or persons concerned have to bear an individual and excessive burden.

One profession that immediately took advantage of the emergence of drone technology is journalism, which is also closely related to the freedom of expression and the right to information.[75] Article 11 of the Charter, Article 10 of the ECHR, and other human rights instruments protect the right to receive information without interference by a public authority regardless of frontiers.[76] In light of this right, drone journalism becomes highly important, as drones allow reporters to access information in difficult and dangerous situations while maintaining a safe distance, such as in violent demonstrations, flooded areas, and the sites of other environmental disasters, where they could not otherwise be present or their presence would be of a very limited scope. Such an opportunity, besides helping to gather information, could also help promote human rights protection by documenting possible human rights violations (e.g., in war zones, during riots). Therefore, policies regarding the use of drones can be linked to the World Press Freedom Index and can be seen as a test of the freedom of expression, with top-ranked countries being the least restrictive about the use of drones and authoritarian countries completely prohibiting the journalistic use of this technology.[77]

Drone technology, as an instrument for remote observation, may also be relevant in the sense of the integration of persons with disabilities. Article 26 of the Charter states that the EU recognises and respects the right of persons with disabilities to benefit from measures designed to ensure their independence, social and occupational integration, and participation in the life of the community. Article 27 § 1 of the Universal Declaration of Human Rights also recognises, that everyone has the right freely to participate in the cultural life of the community and to share in scientific advancement and its benefits. Meanwhile, drones equipped with cameras, microphones, and speakers in some cases may be regarded as one way (if not the only way) for people with movement disabilities to engage in public life (at least remotely) and interact with others.

However, the intrusive nature of drone surveillance discussed in Section 14.1 could also affect the freedom of movement of others protected by Article 45 of the Charter, Article 2 of Protocol No. 4 of the ECHR, Article 13 of the Universal

[75] E.g., see P. Chamberlain, *Drones and Journalism – How the Media is Making Use of Unmanned Aerial Vehicles* (London: Routledge, 2016).

[76] E.g., see Article 19 of the Universal Declaration of Human Rights.

[77] E.g., see E. Lauk et al., 'Drone journalism: the newest global test of press freedom', in U. Carlsson (ed.), *Freedom of Expression and Media in Transition: Studies and Reflections in the Digital Age* (Gothenburg: Nordicom, 2016), pp. 117–25.

Declaration of Human Rights, among others. In this regard it must be noted that constant surveillance caused by such digital interaction, could damage freedom of movement in the sense that it may lead to a chilling effect, when individuals feel less free and resort to a form of self-preservation (self-censorship) by restricting their behaviour and feeling forced to avoid such drone-filled public places.

Another important issue is the right to life:[78] as already mentioned, drones inevitably must capture, store and process certain data owing to aviation safety and security considerations (see Section 14.1). The main aim of such aviation safety and security-based measures is not only to protect people in the air (e.g., crews and passengers of manned aircraft, against a collision with a drone), but also people on the ground (e.g., passers-by who may be injured by flying drones), as well as their property, which could be damaged or destroyed. A slightly more distant implication in this regard is related to drone usage during natural disasters and other difficult situations, when drone technology can be crucial in restoring communications and carrying out search and rescue missions, thereby saving lives.[79]

14.3 DEVELOPMENTS OF DRONE REGULATIONS: MAINTAINING THE BALANCE BETWEEN CONFLICTING HUMAN RIGHTS FROM A EUROPEAN PERSPECTIVE

In recent years, the vast development of drone technology has led to the important evolution of legal regulation worldwide. However, standards set by individual countries could lead to a significant weakening of the protection of the right to privacy, given the possible diversity of views in relation to it. Hence, it is worth looking into EU drone regulation in more detail, as the EU is characterised by its integrative nature and declares the expressed aim of becoming a world leader in international aviation, a global model for the development of next-generation aviation technologies in full respect of fundamental human rights.[80] It is clear from the jurisprudence of the ECtHR that when it comes to balancing competing values in relation to the use of modern technologies (e.g., in this case, drones), any state claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.[81] Accordingly, with drones

[78] Enshrined, e.g., in Article 2 of the Charter, Article 2 of the ECHR, Article 3 of the Universal Declaration of Human Rights.

[79] E.g., see the white paper by Alliance for Telecommunications Industry Solutions (ATIS) on the use of UAVs for restoring communications in emergency situations, ATIS-I-000071, December 2018; also see J. N. McRae et al., 'Utilizing drones to restore and maintain radio communication during search and rescue operations' (2021) 32 *Wilderness and Environmental Medicine* 1, 41–6.

[80] See European Commission, 'An aviation strategy for Europe', COM(2015) 598 final.

[81] See, for instance, *S. and Marper v. the United Kingdom* [GC], Applications nos. 30562/04 and 30566/04, Judgment of 4 December 2008, para. 112.

considered to be the future of aviation,[82] there have been important developments in EU regulation in recent years.

In particular, the new Regulation (EU) 2018/1139 on common rules in the field of civil aviation was adopted (commonly referred to as the Basic Regulation), thereby also establishing an EU Aviation Safety Agency. It brought all aircraft, regardless of their operating mass, into EU competence. In other words, since the adoption of the Basic Regulation, all drones fell within the scope of EU regulation.[83] This comes in line with the opinion of the European Commission, expressed earlier in its Communication to the European Parliament and the Council COM(2014)207 'A new era for aviation', that rules allowing civil drone operations while guaranteeing at the same time the required high levels of privacy must be established at the European level, because such harmonised rules are seen as a necessary precondition for public (societal) acceptance of this disruptive technology.

Acknowledging public acceptance as key to the growth of drone services was also the standpoint of the European aviation community (which the European Parliament later agreed with and fully supported as one of the essential principles for future drone technology development),[84] which pointed out in the 2015 Riga declaration that in order to achieve this public acceptance the respect of citizens' fundamental rights, such as the right to privacy and the protection of personal data, must be guaranteed. The aviation community confirmed the importance of joint European action and stressed the necessity for European regulators to ensure that all conditions are met for the safe and sustainable emergence of innovative drone services, but at the same time highlighted that regulations must help the industry to thrive and adequately deal with citizens' concerns. This point of view reflects the importance of striking a fair balance between different competing values.

Following the adoption of the Basic Regulation, which provided a mandate to the European Commission to adopt legislation in relation to the operation of unmanned aircraft, as well as requirements for their production and certification, the Commission delegated Regulation (EU) 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems and the Commission implementing Regulation (EU) 2019/947 on the rules and procedures for the operation of unmanned aircraft were adopted and came into force, with the latter applied since 2021. In general, the Basic Regulation together with the aforementioned two regulations of the European Commission, brought in important changes regarding drone operations, especially in relation to the right to privacy. For example, the obligation was introduced to register drones and their users and to

[82] See European Commission, 'A new era for aviation – opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner', COM(2014) 207 final.

[83] Until then all activities with aircraft lighter than 150 kg were under the regulatory competence of the EU Member States.

[84] See European Parliament resolution of 29 October 2015 on the safe use of RPAS, commonly known as UAVs, in the field of civil aviation (2014/2243(INI)), OJ J C 355.

install direct remote identification systems in unmanned aircraft, it also established that courses and exams for remote pilots should include subjects on the right to privacy and data protection, with examination certificates valid only for a limited period of time (currently five years), which means that remote pilots will have to periodically renew their knowledge on this matter.

As pointed out in recital 28 of the Basic Regulation,

> The rules regarding unmanned aircraft should contribute to achieving compliance with relevant rights guaranteed under Union law, and in particular the right to respect for private and family life, set out in Article 7 of the Charter of Fundamental Rights of the European Union, and with the right to the protection of personal data, set out in Article 8 of that Charter and in Article 16 of the TFEU [Treaty on Functioning of European Union], and regulated by Regulation (EU) 2016/679 of the European Parliament and of the Council [General Data Protection Regulation (GDPR)].

Therefore, it is enshrined in Annex IX to the Regulation (EU) 2018/1139, that unmanned aircraft and operations with unmanned aircraft must comply with relevant rights guaranteed under Union law. But at the same time, it follows that 'unmanned aircraft […] operations should be subject to rules that are proportionate to the risk of the particular operation or type of operation'.[85] The European legislator therefore seems to be sharing the view of the aviation community, by taking the risk-based approach towards drone regulation in the search for a fair balance between conflicting legal values. However, at first sight it does not seem to be completely successful, to the detriment of the right to privacy and data protection, although the EU promotes high standards when it comes to the protection of these fundamental rights.

The analysis of the EU drone regulations concerned shows that there are a lot of exceptions from such important mechanisms as the registration of drones and their users or the direct remote identification of unmanned aircraft, which hardly seems to be well founded and makes it quite difficult to ensure the effectiveness of these measures while protecting the right to privacy and ensuring personal data protection. For example, the Basic Regulation states that operators of unmanned aircraft shall be registered in accordance with the acts adopted by the Commission when they operate unmanned aircraft, the operation of which presents risks to privacy or protection of personal data, and such unmanned aircraft shall be individually marked and identified.[86] Therefore, it seems that the obligations related to registration should apply whenever a drone with any sensor that allows the capture of private or personal data is used or is going to be used. Yet Regulation (EU) 2019/947 adds some ambiguity regarding registration, because according to it such registration is

[85] See recital 26 of the Regulation (EU) 2018/1139.
[86] See Annex IX 4.2–4.3.

mandatory only when operating a drone equipped with a sensor able to capture exclusively *personal* data, which covers only information related to an identified or identifiable natural person (data subject),[87] leaving aside the data, which strictly does not fall within the scope of the definition of personal data, despite the fact that collection of such data could infringe the right to privacy. Moreover, the obligation to register is not applied when using drones that are considered to be toys within the meaning of Directive 2009/48/EC, although the latter also can be fitted with cameras, microphones, and various other sensors capable of capturing and storing both private and personal data. Therefore, as the remote pilot of an unmanned aerial vehicle (UAV) and the pilot of a manned aircraft ultimately have the same responsibility for following the legal regulations when operating their aircraft,[88] the obligation to register is highly important when dealing with their anonymity issue, as it can ease traceability in the case of their possible liability for failing to comply with those rules. This was also the standpoint of the European Parliament, noting that all drones in line with a risk-based approach should be equipped with an ID chip and registered to ensure traceability, accountability, and the proper implementation of civil liability rules.[89]

The same goes for a direct remote identification system,[90] which, despite the European Parliament's expressed view that the question of identifying drones, of whatever size, is crucial,[91] does not apply to drones categorised as C0 class (i.e.,

[87] Article 4 of the GDPR.

[88] See ICAO, *Unmanned Aircraft Systems* (2011), Cir 328, AN/190, p. 5.

[89] See European Parliament resolution of 29 October 2015 on safe use of RPAS, commonly known as UAVs, in the field of civil aviation (2014/2243(INI)), OJ J C 355.

[90] As stated in Delegated regulation (EU) 2019/945, 'direct remote identification' means a system that ensures the local broadcast of information about a UA in operation, including the marking of the UA, so that this information can be obtained without physical access to the UA. Remote identification system must:

(a) allow the upload of the UAS operator registration number in accordance with Article 14 of Implementing Regulation (EU) 2019/947 and exclusively follow the process provided by the registration system;

(b) ensure, in real time during the whole duration of the flight, the direct periodic broadcast from the UA using an open and documented transmission protocol, of the following data, in a way that they can be received directly by existing mobile devices within broadcasting range: (i) the UAS operator registration number; (ii) the unique physical serial number of the UA compliant with standard ANSI/CTA-2063; (iii) the geographical position of the UA and its height above the surface or take-off point; (iv) the route course measured clockwise from true north and ground speed of the UA; and (v) the geographical position of the remote pilot or, if not available, the take-off point; and

(c) ensure that the user cannot modify the data mentioned under paragraph (b) points ii, iii, iv and v.

A similar technical solution was introduced by the US Federal aviation administration in December 2020 (see Department of Transportation, Federal Aviation Administration, 'Remote identification of unmanned aircraft' (2020), www.faa.gov/sites/faa.gov/files/2021-08/RemoteID_Final_Rule.pdf).

[91] See European Parliament resolution of 29 October 2015 on safe use of RPAS, commonly known as UAVs, in the field of civil aviation (2014/2243(INI)), OJ J C 355.

drones with an operating mass less than 250 g) or C4 class (i.e., drones already made available on the market) within the meaning of delegated Regulation (EU) 2019/945,[92] although this system is essential for effectively dealing with the issue of drone users' anonymity and ensuring their traceability; that is, remote ID is crucial for individuals to be able to take measures to protect their privacy from aerial surveillance by such drones. It is hard to understand the grounds for this exception because it does not seem that such an obligation could be regarded as unsuitable, unnecessary, or disproportionate, even when talking about the drones already made available on the market, as direct remote identification according to the same Regulation (EU) 2019/945 can be provided as a separate add-on, which can be retrofitted on drones by their users themselves.[93] This is especially the case when in 2017 one of the world's leading drone manufacturers had released a white paper outlining a concept in which each drone could transmit its location as well as a registration number or similar identification code using inexpensive radio equipment that is already on board many drones today and that could be adopted by all manufacturers.[94]

Furthermore, the delegated Regulation (EU) 2019/945 sets out the requirements for a geo-awareness system, which should alert remote pilots when a potential breach of airspace limitations is detected so that they can take effective immediate action to prevent that breach; for example, in areas where drone use is restricted owing to privacy concerns. But this system is not mandatory, not to talk about a geo-fencing system, which is completely omitted from the EU drone regulations, although it could automatically prevent drones from entering or launching in restricted (no-fly) zones and help to ensure privacy in these areas.[95] However, some drone manufacturers tend

[92] See Annex of Delegated regulation (EU) 2019/945.

[93] Part 6 of the Annex of Delegated regulation (EU) 2019/945, which sets out the requirements for a direct remote identification as a separate add-on, and requires for it to be placed on the market with the clear instructions on how to install the module on the unmanned aircraft.

[94] See A DJI Technology Whitepaper, '"What's in a name?" A call for a balanced remote identification approach', 22 March 2017, www.dropbox.com/s/v4lkyr2kdp8ukvx/DJI%20Remote%20Identification%20Whitepaper%203-22-17.pdf?dl=0). In order to help solve this issue and increase pilot accountability some drone manufacturers also include a specific permissions clause in their software licence agreement permitting access to pilot location data and some identifying information about them (e.g., see Dedrone, www.aerialarmor.com/blog/how-to-track-a-drone-operator-trace-drone-pilots-with-aerial-armor).

[95] There is a counterview among scholars that aerial surveillance by drone is not solely a privacy issue and should be regulated through property law, more specifically, landowners' airspace rights. Rule emphasises in his article 'Airspace in an age of drones' that 'the growing affordability of drones is jeopardizing the ability for low-altitude airspace to serve in its long-held role as a privacy buffer', because 'camera-equipped drone flights can enable drone operators to cheaply gaze onto private land areas that would otherwise be visible only from airplanes or helicopters at much higher altitudes'. Accordingly, he argues in favour of increasing the scope of landowners' airspace rights and states that in order 'to preserve a level of privacy […] comparable to what landowners enjoyed prior to the drone era, laws clarifying landowner airspace rights should define these rights as extending all the way up to the navigable airspace line of 500 feet above-ground in most locations': T. A. Rule, 'Airspace in an age of drones' (2015) 95 *Boston University Law Review* 1, 155–208. Following this idea, Blank, Kirrane, and Spiekermann proposed the software framework, which could enable drone operators to determine whether a selected drone flight path intersects with a restricted area, by considering privacy

to install geo-fencing systems in their drones voluntarily, which shows that business awareness extends far beyond that of the legislators.[96] What is more, alarming drone cybersecurity issues are not covered by the EU regulations either.[97]

Of course, the EU legislator acknowledges the need to further develop requirements regarding the registration of drones and their pilots, as well as geo-awareness and remote identification systems, as these are seen as the foundations of the U-space system, which is being developed to safely integrate drones into the airspace.[98] However, this step-by-step approach, based on the current state of drone technology development, considering the fast pace of technological progress in comparison to the evolution of legal regulation, risks lagging far behind the technology and does not correspond to the standpoint of the European Parliament expressed in a 2015 resolution on the safe use of remotely piloted aircraft systems (RPAS) in the field of civil aviation that the global regulatory framework for drones should be part of a long-term perspective, taking into account possible future developments.[99]

From the global perspective, it is quite clear that a similar approach to drone regulation is being taken by legislators worldwide; for example, in the US,[100] Canada,[101] and Australia,[102] where specific requirements for drone registration, pilot licensing, built-in remote identification systems, operations above gatherings of people, minimum distance from airports, other people and property, geo-fencing and/or geo-awareness systems, among others, are being established. Some of these are

preferences that can be configured by citizens themselves: P. Blank, S. Kirrane, and S. Spiekermann, 'Privacy-aware restricted areas for unmanned aerial systems' (2018) 16 *IEEE Security and Privacy* 2, 70–9. Unfortunately, the latter proposal, because of the plausible segregation of airspace, would jeopardise aviation safety, as it would become more difficult to plan and execute safe flight routes, especially bearing in mind the constantly increasing number of drone operations. And as already mentioned, advanced optical and digital zoom capabilities of modern cameras used in drones enable the capture of high resolution images from a large distance. Therefore, acknowledging landowner airspace rights up to the specific line above the ground would also be of little use when ensuring the protection of the right to privacy, although it could serve as a safeguard (though very limited) for drones with low-definition cameras.

[96] E.g., see DJI, 'DJI GO app now includes a GEO geofencing system' (2016), www.dji.com/newsroom/news/dji-go-app-now-includes-geo-geofencing-system.

[97] Although it may be concluded from Article 2.1.7 of Annex IX to Regulation (EU) 2018/1139 that the EU legislator seeks to solve this issue by imposing an obligation for organisations involved in the design of unmanned aircraft to take precautions so as to minimise the hazards arising from conditions, both internal and external, to the unmanned aircraft and their systems, that experience has shown to have a safety impact, which includes protection against interference by electronic means.

[98] See, e.g., recital 26 of Implementing regulation (EU) 2019/947.

[99] European Parliament resolution of 29 October 2015 on the safe use of RPAS, commonly known as UAVs, in the field of civil aviation (2014/2243(INI), OJ C 355.

[100] For more information see US Department of Transportation, Federal Aviation Administration, 'Drones', www.faa.gov/uas/.

[101] For more information see Government of Canada, 'Drone safety', https://tc.canada.ca/en/aviation/drone-safety.

[102] For more information see Australian Government, Civil Aviation Safety Authority, 'Drone rules', www.casa.gov.au/knowyourdrone/drone-rules.

already being implemented; others are still in progress (in a transitional period).[103] Meanwhile, in other European (non-EU) countries, such as the UK,[104] Norway,[105] and Iceland,[106] drone regulation is based on common EU drone rules or the latter are de facto applied. The aforementioned countries also share a risk-based approach – like the EU, other countries tend to differentiate drone regulations based on the type of operation (i.e., different flight purposes: recreational, commercial), drone size and weight, other drone characteristics (e.g., with or without camera), level of pilot competence, and so on. This regulatory approach in a sense materialises the vision of the European Parliament that a 'harmonised and proportionate European and global regulatory framework needs to be developed on a risk-assessed basis, which avoids disproportionate regulations for businesses that would deter investment and innovation in the [drone] industry, whilst adequately protecting citizens'.[107]

Although such an approach at first glance may seem beneficial for industry, it is not the case in the context of drone technologies. When the legislator avoids taking more decisive steps in order to develop a clear and well-defined provision, this creates a sort of 'chicken and egg' problem, whereby regulators are reluctant to develop standards until the industry comes forward with technologies for authorisation; however, the industry is reluctant to invest in developing the necessary technologies without certainty surrounding how they will be regulated. Such a deadlock is dangerous from the human rights perspective and suggests a failure on the part of the legislator to balance conflicting values, and nor does it help the industry to thrive. As the ECtHR has ruled on several occasions, it is essential to have clear and detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated, and there must be adequate and effective safeguards against abuses.[108] Such rules must form part of a legislative framework affording sufficient legal certainty, so that all parties can foresee the consequences for themselves.[109]

[103] E.g., in the US all drone pilots required to register their UAV will have to operate their aircraft in accordance with the rule on remote identification (ID); that is, equipped with a remote ID system, which provides ID and location information that can be received by other parties during flight, beginning 16 September 2023. Accordingly, drone manufacturers have until 16 September 2022 to produce drones with built-in standard remote ID, and the FAA encourages the early production of remote ID broadcast modules for retrofitting (see US Department of Transportation, Federal Aviation Administration, 'Remote identification of drones', www.faa.gov/uas/getting_started/remote_id/, and US Department of Transportation, Federal Aviation Administration, 'Remote ID for industry and standards bodies', www.faa.gov/uas/getting_started/remote_id/industry/).

[104] For more information see UK Civil Aviation Authority, 'Drones: information about all aspects of remotely piloted aviation and drones', www.caa.co.uk/consumers/remotely-piloted-aircraft/.

[105] For more information see CAA Norway, 'Drones', https://luftfartstilsynet.no/en/drones/.

[106] For more information see Icelandic Transport Authority website: www.icetra.is/aviation/drones/.

[107] See European Parliament resolution of 29 October 2015 on the safe use of RPAS, commonly known as UAVs, in the field of civil aviation (2014/2243(INI)), OJ J C 355.

[108] See, for instance, *Kruslin v. France*, Application no. 11801/85, Judgment of 24 April 1990, paras. 33–5.

[109] See, for instance, *Valenzuela Contreras v. Spain*, Application no. 27671/95, Judgment of 30 July 1998, paras. 59–61.

This brings to mind the control dilemma elaborated by Collingridge, following which, influencing technological developments is easy when their implications are not yet manifest, but once we know these implications, they are difficult to change. In other words, when a technology is still at an early stage of development, it is possible to influence the direction of its development, but we do not yet know how it will affect society. On the other hand, when the technology has become societally embedded, we can recognise the implications, but by then it is very difficult to influence its development. Nevertheless, legislators should not put human rights at risk, but should refrain from a step-by-step approach based on the current state of technological progress, as such an approach tends to lag behind the development of technologies. Shifting from a reactive to proactive legislation and establishing a sufficiently clear and balanced legal framework could help foster further technological development, while at the same time ensuring adequate protection of human rights. As the deployment of drones may inevitably raise tensions between the right to privacy and other human rights, a holistic approach must be taken when regulating the use of drones, focusing not merely on the protection of the right to privacy, but paying more attention to other fundamental freedoms and human rights, and seeking a well-balanced legal framework.[110]

In this regard, Article 52 § 1 of the Charter establishes that any limitation on the exercise of the rights and freedoms recognised by this Charter are subject to the principle of proportionality. This principle is also considered the most important tool for interpreting the ECHR and is widely applied by the ECtHR.[111] Therefore, in continental (Romano-Germanic) legal systems, the proportionality principle prevails as a balancing method. Despite the very concept of balancing being perceived slightly differently in non-continental legal systems,[112] the substantial objective remains the same – to strike a fair balance between conflicting legal values. Legislators worldwide should rely more on the principle of proportionality (or other legal balancing methods) when regulating the usage of drone technology in order to reconcile conflicting human rights. As technological development in this field is inevitable and drone usage in modern society seems to keep growing rapidly, further discussion of these issues is of great importance.

[110] The European Parliament in resolution 2014/2243(INI) has also stressed that the use of drones must respect not only the fundamental right to privacy and data protection, but also the freedom of movement and freedom of expression, and that the potential risks connected to these rights, regarding both surveillance of individuals and groups and the monitoring of public spaces (including borders), need to be addressed.

[111] See E. Leonaitė, 'Proporcingumo principas Europos Žmogaus Teisių Teismo Jurisprudencijoje', PhD thesis, Vilnius University (2013), 45.

[112] E.g., in the US, when the balancing test is applied, often the burden of a restriction of a right is weighed against the importance of the general interest. Meantime, in the UK, such criteria as legality, *ultra vires* doctrine, or Wednesbury's unreasonableness (or irrationality) test are usually applied. Furthermore, various other methods for balancing different values are distinguished in legal literature (e.g., see D. A. De Vries, 'Balancing fundamental rights with economic freedoms according to the European Court of Justice' (2013) 9 *Utrecht Law Review* 1, 169–92, at 171–2).

14.4 CONCLUSIONS

This study has revealed that the use of drone technology can interfere with the right to privacy in diverse ways. Although many of the discussed dangers that the use of drones pose to the right to privacy are not new relatively speaking, the frequency and severity of privacy violations may increase significantly owing to the capabilities of drones. In this regard drones pose a dual threat: (a) as a technology that inexpensively 'gives wings' to other technologies (e.g., cameras, sound recorders, GPS, infrared and other sensors, etc.), thus allowing their use in a completely new environment (i.e., in the air) and opening up new surveillance possibilities, and (b) as a platform (base) that integrates various technologies into one whole, including the incorporation of AI technology, thus creating qualitatively new surveillance instruments.

However, various restrictions imposed on the use of drones in favour of privacy protection could undermine other human rights that are equally important; for example, the right to engage in work and the freedom to conduct a business, the right to property, freedom of expression, and the right to information, or even the right to life. This requires a holistic approach from legislators in order to strike a fair balance between these conflicting values. It is important, when regulating the usage of drone technology, to rely more on the proportionality principle (or other legal balancing methods) in order to reconcile conflicting human rights.

The legal response to the threats posed by the use of drones tends to lag behind the development of these technologies, and various poorly grounded and extensive exceptions are being established. Illustrated by the example of the EU, the study reveals that further joint action must be taken to develop legal requirements regarding the registration of drones and their users, as well as geo-awareness and remote identification systems, while also establishing common rules related to drone cybersecurity, geo-fencing, and others. More attention should be paid to by-design and by-default measures (e.g., minimisation of the data gathered by drones, automatic anonymisation or removal of unnecessary data, etc.), possible obligations for online service providers (e.g., remote signal blocking, restrictions for data sharing, etc.) and AI related issues in drone systems.

The legislators should foster the development of standards using a long-term perspective. In order to be effective, the legislation has to shift from reactive to proactive, and establish a more future-orientated legal framework taking into account possible future developments, rather than a step-by-step approach based on the current state of technological progress. The industry, regulators, and the public must come together to seek a harmonised global regulatory framework and to guarantee legal certainty while balancing competing values. As drone usage in modern society keeps growing, it is of great importance to tackle these challenges in a timely manner and ensure that all the conditions are met for the safe and sustainable emergence of innovative drone services, enabling the industry to thrive and at the same time adequately deal with human rights concerns.