IAIC MiBACT DGBIC CREDA

Diritto Mercato Tecnologia

26 marzo 2020

Critical Infrastructures, Use of Drones and Data Protection Impacts

Giovanni Maria Riccio e Fabiola Iraci Gambazza

Nuova Editrice Universitaria

La rivista è stata fondata nel 2009 da Alberto M. Gambino ed è oggi pubblicata dall'Accademia Italiana del Codice di Internet (IAIC) sotto gli auspici del Ministero dei beni e delle attività culturali e del turismo - Direzione generale biblioteche e istituti culturali (DGBIC) e dell'Università Europea di Roma con il Centro di Ricerca di Eccellenza del Diritto d'Autore (CREDA).

Norme di autodisciplina

1. La pubblicazione dei contributi sulla rivista "Diritto Mercato Tecnologia" è subordinata alla presentazione da parte di almeno un membro del Comitato di Direzione o del Comitato Scientifico e al giudizio positivo di almeno un membro del Comitato per la Valutazione Scientifica, scelto per rotazione all'interno del medesimo, tenuto conto dell'area tematica del contributo. I contributi in lingua diversa dall'italiano potranno essere affidati per il referaggio ai componenti del Comitato Scientifico Internazionale. In caso di pareri contrastanti il Comitato di Direzione assume la responsabilità circa la pubblicazione.
2. Il singolo contributo è inviato al valutatore senza notizia dell'identità dell'autore.
3. L'identità del valutatore è coperta da anonimato.
4. Nel caso che il valutatore esprima un giudizio positivo condizionato a revisione o modifica del contributo, il Comitato di Direzione autorizza la pubblicazione solo a seguito dell'adeguamento del saggio.

La Rivista adotta un Codice etico e di buone prassi della pubblicazione scientifica conforme agli standard elaborati dal Committee on Publication Ethics (COPE): Best Practice Guidelines for Journal Editors.

Sede della Redazione

Accademia Italiana del Codice di Internet, Via dei Tre Orologi 14/a, 00197 Roma, tel. 06.8088855, fax 06.8070483, www.iaic.it, info@iaic.it

Critical Infrastructures, Use of Drones and Data Protection Impacts*

Giovanni Maria Riccio
Università di Salerno

Fabiola Iraci Gambazza
Dottoressa in Giurisprudenza

1. Introduction. Drones: Uses and Categories

Nowadays, when a reference is made to "drones", it is a common thought to imagine an aircraft that does not need a human pilot on board. The reality is much more complex and the typologies of drones are wider.

Preliminarily, it is important to make a difference between two different drones: the Remotely Piloted Aircraftes System, also called RPAS, which are the ones that need a control by an human being with a pilot station and the ones that are "*autonomous".* There is also another acronym which includes the two categories: UAVs, that states for "*unmanned aerial vehicles"*[1].

* The present research has financially supported by the EU Horizon 2020 Innovation Programme "Defender" under grant agreement No 740898. Although the present paper has been jointly conceived, the authorship of paragraphs 1-4 must be attributed to Fabiola Iraci Gambazza, while paragraphs 5-7 to Giovanni Maria Riccio.

[1] European Parliament Directorate general for internal policies, Policy department c: citizens' right and constitutional affair, *Privacy and Data Protection Implications of the Civil Use of Drones,* 2015, Bruxelles;

The history of the creation of drones goes back to war eras: the first drone was created before the first manned airplane and it was employed to surveillance and to combat for the first two World Wars (especially during the Second World War, when the drone technology was more intensively used). The Wright Brothers must be considered probably the inventors of unmanned flights, but Nikola Tesla too, and his studies about radio-controlled boat invention have strongly influenced the actual scenario.

During the Sixties, drones started to be used for stealth surveillance and new versions of drones appeared in Israeli, the country recognized to be "*an aggressive UAV developer*"[2]. Despite the initial and large military use – recently, especially for USA's use of killer drones in Afghanistan War -, during the Nineties UAVs started to be object of interest for civil uses, thanks to the technological development and the consequent affordability and accessibility of drones.

By way of illustration: infrastructure protection, monitoring and safety and security inspections; geo-spatial mapping; environment monitoring; law enforcement, surveillance and monitoring of individuals and of people and of electronic communications (particularly, to protect people for threats and illegal actions or to investigate in public events intercepting communication or controlling someone); civil protection[3].

Drones have been also used for ludic intentions, but the civil use reveals to be indispensable in many situations: for instance, in environmental emergency. An interesting case occurred in Australia, in which two surfers struggling with waves were saved by a drone which dropped them a inflatable pod. Similarly, in Rwanda, drones help to supply blood deliveries and to be necessary in a dramatic health crisis, such as in Tanzania too, where drones are used to ship medical sample[4].

---

[2] https://www.pbs.org/wgbh/nova/spiesfly/uavs.html: for a further deepining about the historical development of drones.

[3] European Parliament Directorate general for internal policies, Policy department c: citizens' right and constitutional affair, *Privacy and Data Protection Implications of the Civil Use of Drones,* 2015, Bruxelles

[4] https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642230/EPRS_BRI(2019)642230_EN.pdf

The present paper analyzes how drones may be used for civil activities and, in particular, in order to prevent and limit the damages that may occur, due to attacks or non-human accidents, to critical infrastructures. In particular, elaborated within a project called Defender[5], will examine how drone may be used in emergency cases and how the managing of such emergencies, especially in activities research and preventive tests, should comply with personal data regulations.

2. The Legal Framework of Critical Infrastructures

A crucial use that in this case, Defender project propones to do is the monitoring of essential infrastructure, with a specific focus on critical energy infrastructures (CEI). For essential or critical infrastructure, it is meant all the systems that provides necessary services to people, such as water, electricity, transportation, gas, and so on. The emphasis on essential infrastructures is recent and dates from the Second World War and then, started to be regulated during the years of Cold War.

However, only recently, in the last twenty years, there has been a concrete intervention to regulate structurally and systematically, by both the European Union and the single member States. Indeed, the first document was the resolution *A Secure Europe in a Better World—European Security Strategy,* in 2003, unfortunately limitedly to identify the perimeter of essential infrastructures and their meaning. Furthermore, in 2004, the EU for the first time in the *European Programme for Critical Infrastructure Protection* holds the necessity to a achieve a regulation in order to prevent the possible attacks to the essential infrastructure and to prepare all the necessary measures to remedy after one. The approach of this document was indispensable to identify the necessity of designation of European essential infrastructure and a common approach to evaluate the necessity to ameliorate the protection, due to the presence of any criticality. But the most important point of the European

[5] https://defender-project.eu

program for critical infrastructure protection was the attempt to create a standardization of security management process[6].

A definition of critical infrastructure and European critical infrastructure is provided by the Article 2 of the Directive 2008/114 about the identification and designation of European critical infrastructures (ECIs). Indeed, a critical infrastructure is "*an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*".[7] And especially, the Directive identifies when there is a risk for the infrastructure, establishing that *"a risk analysis means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure".*

Each Member State shall inform the other Member States which may be significantly affected by a potential ECI about its identity and the reasons for designating it as a potential ECI: indeed, the application of the directive is limited to the ECIs, so to a Member State, in case the damage would be affect two Member States. In that case, a drone can be indispensable and useful to prevent a possible damage in front of a menace or in order to monitor an emergency situation: in fact, the vulnerability of these infrastructures were proved by tragic events, such as the Deepwater disaster and the nuclear incident Fukushima Dai-ichi[8].

---

[6] For further information on this topic: Lewis, T. G. *Critical infrastructure protection in homeland security: defending a networked nation.* John Wiley & Sons (2019*)*; Luiijf, E., Nieuwenhuijs, A., Klaver, M., van Eeten, M., & Cruz, E., *Empirical findings on critical infrastructure dependencies in Europe,* in *International Workshop on Critical Information Infrastructures Security*, Springer, 302 (2008); Alcaraz, C., Zeadally, S., C*ritical infrastructure protection: Requirements and challenges for the 21st century,* 8 *International Journal of Critical Infrastructure Protection*, 53 (2015).

[7] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

[8] The Deepwater disaster is remembered as the industrial disaster that began in 2010 in the Gulf of Mexico, caused by a petroleum spill; the Fukushima Dai-chi was the nuclear accident occured in Okuma Fukushima in 2011.

Though drones have different features too and to simplify, it seems to be necessary to separate categories, based on: weight, type, price and diffusion, and finally regulation. These characteristics are useful to make a comparison between the drones used for military purposes and those used for civil uses[9]. For instance, a small UAV can be used to inspect, to video and to surveil and to accomplish other civil uses, due to its price and its structure; there considerations are valid for light UAV as well, even if the use can be extended to geospatial and broader surveillance. Differently, the use of large drones is predominant in military missions, thanks to their capabilities.

3. Main Issues and Revised Legal Framework

Since the large number of users, the continuous technological development, EU Parliament and Commission have been working since 2015 in adopting a regulation about the use of civil drones. In 2018, the European Parliament decided to create EASA, the European Aviation Safety Agency, which may is aimed at analyzing all the relevant aspects and questions connected to cybersecurity and aviation. In 2019, the European Parliament and EASA published the Commission Delegated Regulation (EU) 2019/945 and Commission Implementing Regulation (EU) 2019/947, that will be enter in force in 2020.

These new rules have the purpose to allow any citizen to buy and operate a drone ensuring safety, security, privacy and environmental protection. In fact, even if it is sure to recognize the high potential of using drones to achieve the mentioned purposes, there are some risks that must be taken into account, that can be sum up in three aspects: safety and operation; insurance and liability; privacy and data protection.

Over these coming years, the European Commission decides to adopt the highest safety standards, thanks to an assessment of the risk of the operation and a balance between the obligations of the drone's operator and the safe

[9] https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642230/EPRS_BRI(2019)642230_ EN.pdf

operation to accomplish. In 2007, in relation to the safety topic, the European Commission launched an analysis to regulate drones, dealing with this critical issue, in a discussion with organizations and scientific members. In 2013, there was an official publication, called the Roadmap, composed by three report, which each one deals with the use of RDPA: "the regulatory approach; the strategic research plan; the societal impact"[10].

In 2015, in Riga, there was the publication of a regulatory framework, a guidance for a future EU regulation, which contains some principles, starting from two points: drones must be considered a new typology of aircraft and must be regulated with a specific regulation and their social and public impact. After Riga, EASA and the EU Commission jointly began to collect and report information about drones and safety operations, with the collaboration of Member States, as well. The idea was to create a unique framework for all the Member states that contained all the most important principles, including the rules of civil drones.

In 2019, technical requirements were adopted by the European Commission, regulating the safety standards in order to respect the EU aviation strategy. With the Regulation 2019/947, the EU Commission imposed to the pilot to register in a public register in his/her State Member and to be authorized before the flight when a drone weighing more than 25 kg- if some conditions are met. Once the authorization is obtained, the pilot can flight his/her drone abroad in the European space[11].

Having a unique regulation manages to be clear in order of what pilots – professional or not- have to respect during and in preparation of a flight, considering that the drone must be identifiable to flight in security and the cases in which the authorization is necessary to use the drone[12].

There are two types of operations: the VLOS operations and the BVLOS operation. The first operation is made with the necessity of visual sight;

[10] https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642230/EPRS_BRI(2019)642230_EN.pdf
[11] https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/642230/EPRS_BRI(2019)642230_EN.pdf
[12] https://www.easa.europa.eu/newsroom-and-events/press-releases/eu-wide-rules-drones- published

instead the BVLOS ones, are made without the eye contact on the drone. The new regulation identifies three categories of operations: open category; specific category; certified category.

All the operations in open category do not need a pilot license or a previous authorization, but all these operations must be VLOS and have to respect the technical requirements of the regulation or the drone has to be the result of private creation. To certificate the compliance to the requirements, the drone must show an identification class label, involving limitation in order to the distance that must be respected between the drone and people, and the UAVs must flight below 120 meters. The second category denominated specific category, in which the operator uses usually a drone that weights more than 25 kg, and in a BLOVS operation. In this case, due to the medium risk of the operation, the pilot must evaluate the risk before the flight, thanks to a standard risk assessment, and evaluate all the conditions of the flight to obtain an authorization by the national aviation authority, that will contain all the specific requirements to the specificity of the operation. [13]

The last category is the certified one: this kind of operations have as protagonist large drones in controlled airspace and the pilot must have a license and his/her drone. In this area, there is no distinction between unmanned and manned aircraft, and the rules are the same[14].

4. Use of Drones and Data Protection Before the GDPR

Probably the most controversial topic related to the use of drone is the risk to infringe personal data regulations.

The use of drones might be a danger for the fully compliance of the right to privacy of individuals, in order to the specific features, especially the capability to capture personal information. Indeed, the Article 29 Working Party in the Opinion 1/2015 analysed the data protection issues relating to the

[13] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0947&from=EN

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0947&from=EN

utilization of drones[15]. A drone may be composed only by essential elements and in that case, it does not represent a threat to privacy, but "*still cause annoyance and social disturbance to others".* Instead, a drone usually – beyond its basic structure - shows other equipment that might interfere with private life of individuals.

For instance, in case of visual recording equipment, the drone has the capability to capture and to send images, with the possibility to recognize people, things or events or to read license plates or vehicles, even if environmental conditions might not allow the full visibility. Another supply is represented by specific sensor that are up to identify traces of nuclear, biological, chemical and explosive stuff. A detection equipment in a drone manages to follow vehicles and find the right location thanks to the optical-electronic sensors, even if there are walls or other obstacles. Instead, a radio-frequency equipment, for example antennas, are able to find the location of Wi-fi access point or cellular stations.

On the one hand, this equipment, however, don't represent a menace to privacy in an habitual use, but when personal data are stored and processed without the consent or the awareness of the individual, by the data processing equipment on-board. So, there are several risks for data protection caused by using drones, and this could be happening just by seeing a drone and by the fear to be supervised. On the other hand, drones can without difficulty enter private premises and collect a large amount of data, and if there is the presence of a particular technology on board, it's possible collect data without any direct sight (through roofs, for example) or during a long period of time and supervising a large area. The high risk is represented by the collection of data is occult and damages deeply the private and family life.

So, in the light of the above mentioned circumstances, the question arises: how could be possible a balance between the use of drones and its equipment and the data protection issues?

Before the GDPR (Regulation EU 2016/679), all the Member States adopted the implementation of the Directive 95/46. In fact, the processing of

[15]https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2015/wp231_en.pdf

personal data carried out by the equipment on-board of drones can be judged as lawful, only in the case where there is a legal bases, so for example, when the individual has given his/her consent (Article 7 of the Directive), or when the processing is necessary for the performance of a contract to which the data party is a subject (Article 7 b); or even when the processing is necessary for compliance with legal obligation or necessary for the performance of a task carried out in public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed (Article 7 c and e); or when the processing is necessary in order to protect the vital interests of data subject (Article 7d) or finally when the processing is necessary for the purposes of a legitimate interest (Article 7f). However, a legal basis is required and all the data must be collected when there are a specified, explicit and legitimate purposes and not further processed for others aims- unexpressed to the data subject, in accordance with the proportionality, necessity and minimization principles. According to the EU directive, the data must be collected in order to fulfill the purposes, without any further information, this could be possible adopting privacy by default measures or in case of collecting images, using graphical effects that prevent the traceability of the subject[16].

Another important step in the drones regulatory framework are the recommendations given by the WP 231, which were especially addressed to the operators of a drone, before the flight in which – just quoting the most significant rules - the operator had: to control if there was he necessity of a previous authorization before the flight; to do a impact assessment of the operation on privacy, such as the dimension of the drone, the possible information captured, the security measures in case of not consensual data catches and the importance to the sudden communication to the Authority Guarantor; to inform people who could be "*impacted*" by the drone and the operation, realizing a clear and direct information; to take all the security

[16] Pauner, C.; Kamara, I.; Viguri, J., *Drones. Current challenges and standardisation solutions in the field of privacy and data protection*, ITU Kaleidoscope: Trust in the Information Society (K-2015), December 2015, 5; Ketan M.*, Drones and Their Legality in the Context of Privacy,* Leiden Law School; National Law University Jodhpur (NLUJ), November 25, 2015, 12.

measures to prevent any privacy possible violations; to delete or anonymize any unnecessary personal data soon after the collection or as soon as possible[17].

5. The Intersection between Data Protection and Drones EU Regulatory Frameworks

The General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council, hereinafter: GDPR) has been issued on 27th April 2016 and is in force in all EU members from 25th May 2018.

It is a complex text which aims, on one side, at updating the European legislation on data protection with a legislative act which is more adequate to the modified technological and sociological scenario and, on the other hand, to adopt a text which will be enforceable, without differences, guaranteeing a full legal harmonization, in all the member States. The GDPR has, among its purposes, that of *"ensuring a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data in the Union".* This purpose of harmonization has not been achieved by the previous EU directives and notably by the Directive 46/97/EC, although it is regarded as a central issue by the same European Institutions. The option of adopting a Regulation instead of a Directive aims at ensuring a common framework, limiting the regulatory interventions by member States and national data protection authorities.

GDPR affected the drones regulation, from mainly four aspects:

A) the broader meaning of personal data; the concept of accountability;
B) the application of data protection by design or by default measures;
C) all the rights granted to individuals, such as the right to be forgotten, the right to access to data, etc.);
D) the adoption of DPIA (data protection impact assessment) before using the technologies within the machines.

[17]https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf (specifically, pages 19 and next); for the other recommendation consult the WP231.

At a first sight, the drones Regulation seems to be already compliant with the notion of personal data of the GDPR[18]. In fact, the Regulation 947/2019 referred to personal data and protection in the whereas and in next articles, specifying, for example, that in the UAS geographical zone, that is the portion of space in which all the operations of flight are allowed by the Authority, excluding all the zones where there was a possible risk for personal data.

Secondly, as said, the GDPR, in the light of the accountability principle, has legislatively introduced the concepts of privacy by design and privacy by default.

These concepts were not included in the EU Data Protection Directive (Directive n. 96/45/CE), as the Directive only held the obligation for data processors to implement technical and organizational measures in order to fully protect personal data against unlawful conducts. Similarly, member States' regulations did not hold any specific rules on these issues, even if some Data Protection Authorities (e.g. UK's ICO) has already issued specific guidelines for implementing such measures by default or by design.

According to Whereas n. 78 of the GDPR "*In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account*

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0947&from=EN: there is a direct reference to GDPR and the concept of personal data, in the note number 4 of the Regulation. Quoting: "*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1*)."

the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations".

Privacy by default was not included in the European or national regulations and, as mentioned, it can be considered as a corollary of the accountability principle.

Pursuant to article 25, paragraph 2 of the GDPR "*The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility*".

It is a crucial aspect in case of drones, as the application of these measures requires that the architecture of the technologies with which the drones are equipped must be designed respecting the data protection rules since their development. In other words, companies which produce drones are expected to anticipate their obligations, in the sense that the privacy compliance should be ensured since the starting development of the technologies[19].

A sign of the compliance of Regulation 947/2019 with these principles of GDPR, may be found in the the Whereas 16 that holds that an operator should register his/her drone, when the UAV "*is equipped with a sensor able to capture personal data",* and it might represent a risk for the protection of personal data[20].

This aspect is confirmed by Article 18 letter m) of the Regulation: in fact the competent authority shall "*establishing and maintaining registration systems for UAS whose design is subject to certification and for UAS operators whose operation may present a risk to safety, security, privacy, and protection of personal data or the environment".* Another evidence is in the

[19] On this aspect see Jasmontaite, L., Kamara, I., Zanfir-Fortuna, G., & Leucci, S., *Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR*, Eur. Data Prot. L. Rev., 4, 168 (2018).

[20] Altawy, R., & Youssef, A. M., *Security, privacy, and safety aspects of civilian drones: A survey.* ACM Transactions on Cyber-Physical Systems, 1(2), 1-25 (2016*).*

Whereas 21, as well: "*Some areas, such as hospitals, gatherings of people, installations and facilities like penal institutions or industrial plants, top-level and higher-level government authorities, nature conservation areas or certain items of transport infrastructure, can be particularly sensitive to some or all types of UAS operations. This should be without prejudice to the possibility for Member States to lay down national rules to make subject to certain conditions the operations of unmanned aircraft for reasons falling outside the scope of this Regulation, including environmental protection, public security or protection of privacy and personal data in accordance with the Union law*".

In conclusion, it is fundamental to remind the most relevant innovations of these new regulations that can be summed up in a few whereas, concerning the intersection with the data protection regulations:

- Whereas n.4 Regulation 2019/947: Technologies for unmanned aircraft allow a wide range of possible operations. Requirements related to the airworthiness, the organisations, the persons involved in the operation of UAS and unmanned aircraft operations should be set out in order to ensure safety for people on the ground and other airspace users during the operations of unmanned aircraft;
- Whereas n.14 Regulation 2019/947: Operators of unmanned aircraft should be registered where they operate an unmanned aircraft which, in case of impact, can transfer, to a human, a kinetic energy above 80 Joules or the operation of which presents risks to privacy, protection of personal data, security or the environment,
- Whereas n. 19 Regulation 2019/947: National registration systems should comply with the applicable Union and national law on privacy and processing of personal data and the information stored in those registrations systems should be easily accessible;
- Whereas n. 20 Regulation 2019/947: UAS operators and remote pilots should ensure that they are adequately informed about applicable Union and national rules relating to the intended operations, in particular with regard to safety, privacy, data protection, liability, insurance, security and environmental protection.

As mentioned, another point that must be took into account is that of the necessity of drafting a DPIA before the use or entering into the market of

drones. Article 35 has introduced this new obligation to carry out an assessment each time "*a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons*". The data controller has to assess whether the processing of data collected and managed through the drones meets the definition of the above-mentioned article, even considering not only the actual level of risks, but also foreseeing the potential impact on the rights of individuals[21]. For instance, drones' technologies are able to collect, even if occasionally and involuntarily, sensitive data, such as people in the line for some sensitive medical checks (e.g. drug addiction services) or, in general, the monitoring of spaces where religious or political meetings take place.

These examples should suggest that a DPIA, even if not expressly requested by the European and national regulations, is a good practice for those companies which produce drones and, most of all, for the users of these drones for non-personal activities. Thus, even if the use of drones is not explicitly included in the list of the cases for which a DPIA is mandatory (lists which have been issued by the national supervisory authorities), it is considered to be a good practice in the light of the accountability principle on which is based the GDPR.

Furthermore, the use of drones may meet the case of the so-called invisible processing, i.e. the case of technologies collecting personal data from a source that cannot allow the providing of a privacy notice to the individuals. At the same time, the uncertain reference to the use of new technologies made by Article 35 may also include some specific drones, especially in cases in which the processing is aimed not only at controlling for security reasons (such as the case of critical infrastructures' premises), but also for other purposes.

---

[21] Cortina S., Valoggia P., Barafort B., Renault A. (2019) *Designing a Data Protection Process Assessment Model Based on the GDPR*, in Walker A., O'Connor R., Messnarz R. (eds), *Systems, Software and Services Process Improvement*. EuroSPI, Springer, 2019; Bieker F., Friedewald M., Hansen M., Obersteller H., Rost M. (2016) *A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation*, in Schiffner S., Serna J., Ikonomou D., Rannenberg K. (eds), *Privacy Technologies and Policy*. APF, Springer, 2016.

Finally, even if exclusively used in order to prevent attacks to the infrastructures, it is undoubted that the use of drones implies "*a systematic monitoring of a publicly accessible area*", even if not always "*on a large scale*".

In this context, considering the above-mentioned considerations, our opinion is that the data controller, also for research activities or security purposes, should carry out a data protection impact assessment, with the advice of the data protection officer, where designated.

Another issue which should be considered in analyzing the connections between data protection and drones regulations concern the applicability of the rights granted to the data subjects by articles 16-22 of the GDPR. As already pointed out, it is impossible to provide data subjects with a prior privacy policy. However, the data collected through the drones must be stored for a minimum period (also in order to comply with the minimization principle): in this case, national regulations are slightly differences and, in general, the rules on video surveillance system – and, in particular, on the period of storage allowed by such rules – can be also applied to drones[22]. Another possibility is that of blurring the face of the persons which are depicted through the machines: however, the results of the Defender research, shows that this kind of technology is not always technically applicable, also because for the high costs which are connected to that.

As long as this article is devoted to the use of drone by private entities, it cannot be applied the exemption held by Article 2, paragraph 2, lett. d) of the GDPR which excludes from its material scope the processing of personal data made by "*competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*".

[22] See M. N. Asghar, N. Kanwal, B. Lee, M. Fleury, M. Herbst and Y. Qiao, *Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective*, in IEEE Access, vol. 7, 111709 (2019).

6. Member States' Regulations on the Use of Drones

The Regulation 2019/945 and the Regulation 2019/947 will entirely replace the existing national rules in EU member States, including all the rules which contain the technical and operational measures requirements for drones, defining the conditions of flights and the minimum remote pilot training requirements.

6.1. The Royal Decree in Spain

In 2017, drones are regulated by the Royal Decree n. 1036 which states the registration and circulation of unmanned aircrafts. According to the new rules, operators shall ensure that drones are visible and identifiable as possible. The Royal Decree introduced new scenarios regarding drones' use: for aircrafts weighting more than 2 kilograms and dedicated to professional use, flights over cities, night flights or flights with less visual control are now authorized, but also having license and a liability insurance is mandatory.

Recreational flights, however, shall not exceed 120 meters of height from the ground and for night flights only aircrafts weighting less than 2 kilograms are authorized. They may flight maximum over 50 meters height from the ground.

The Spanish Data Protection Authority clarifies that, accordingly with articles 8, 9 and 10 of the Royal Decree, the drones shall have characteristics associated with the data controller and the operator shall be visible and identifiable as the controller of the drone.

In the data protection prospective, the Spanish Authority issued a guide aiming at clarifying data protection aspects when using a drone. In cases when is inevitable to the operator record personal data during the flight, the Authority advises to minimize as much as possible the presence and/or collection of personal data in the operating zone. To comply with such recommendations, operators should perform flights at times where there are not large concentrations of people or when access to the flight zone is restricted, consider the possibility of not capturing the full flight but only necessary moments as well to promote and apply privacy features from design

such as, for example, adjust the resolution of the image to the minimum necessary, reduce the granularity of geolocation or apply techniques for the anonymization of images.

6.2. The role of ENAC in Italy

In Italy the European regulation on drones did not came fully into force. At the time being, the use of drones is regulated by the "*Air Pilot Regulation with Remote Pilotage*" of ENAC - National Civil Aviation Authority.

The first version of the Remote Pilotage Aircraft Regulation was issued on December 16, 2013 and has been amended to adapt it to the international and European legislation.

The ENAC, pending the adoption of a regulation implementing the European legislation, with a provision dated 25 September 2019, has decided to partially suspend the application of the Remote Piloting Aircraft Regulation.

It can certainly be anticipated that the registration on the D-Flight website www.d-flight.it and the application of an electronic identification device will become mandatory. For critical operations, future Specific operations, the pilot and the vehicle must have the relevant authorizations, certifications and be registered on the D-Flight site.

As regards the protection of personal data, the Italian regulation, in accordance with European legislation, states as follows: Remotely Piloted Aircraft System with aircraft with operating take-off mass of less than 25 kg (Article 8 General provisions for operating RPAS: "*The RPAS shall be identified by a plate installed on the RPA showing the identification of the system and the operator. An identical plate is also on the remote ground pilot station. 2. As of the 1st of July 2016, in addition to plates required by the Art 8.1, any RPAS shall be equipped with an Electronic Identification Device, which allows the transmission of real time data, its owner/operator and basic flight parameters, as well as the recording of these data. Electronic Identification Device performances and characteristics are defined by ENAC*".); Remotely Piloted Aircraft System with aircraft operating with take-off mass of more than or equal to 25 kg (*Art. 14 Registration and*

identification: 1. RPA with operating take-off mass more than or equal to 25 kg, flying inside the Italian airspace, shall be registered by ENAC in the RPAS register, by assigning dedicated registration marks; identical registration marks to be shown on the remote ground pilot stations. The identification plates shall be installed on the RPA and the remote ground pilot station. 2. The application for registration shall be made by the RPAS owner in a form and manner established by ENAC); and finally Article 34 Data protection and privacy ("*When operations carried out by a RPAS could lead to the processing of personal data. 2. As amended (Italian Data Protection Code), with regard to the use of forms of identification of a person only, pursuant to Article 3 of the related Code, as well as in accordance with the regulations in charge of protection of personal data*").

6.3. The 2017 Act in Germany

In Germany, the Federal Aviation Office is the responsible office for the issuance of permits and authorizations for unmanned aircrafts operations. The German law was modified in 2017 and added a certain number of restrictions in comparison with the former regulation.

The 2017 Act to regulate drones' use stablished that for drones weighting more than 250 grams an identification label – water, fire and crash resistant - with the operator's name and address is required. Drones up to 5 kilograms may be operated without a permit as long as it complies with other safety rules, still a license is required. One of the peculiarities of the German Act is the prohibition of drones' flights over nature reserves due to the German Laws for nature conservation.

The new drone regulation eliminated mostly of the previous separation between leisure and commercial pilots and having a liability insurance is a mandatory requirement for all types of operators.

Regarding data protection aspects, the German Act states that aircrafts weighting more than 250 grams or capable to collect, store or transmit optical data, acoustic data or radio signals are prohibited to fly over residential properties. For flights with the usual camera drones, the consent of the person whose rights might be affected must be obtained.

6.4. The French Regulation

The regulation of the drones has been recently modified by the Decree n° 2019-348 of 19th April 2019 on the notification of the information concerning the use of aircrafts traveling without anyone on board.

In general, the use of drones is regulated by articles from L6214-1 to L6214-3 of the Transportation Code, which are dedicated to the rules on the circulation of drones.

As for the data protection aspects, the Direction Générale de l'Aviation Civile has issued, in 2016, the guidelines which have been agreed with the CNIL, the French data protection authority. These rules mix security and data protection interests, and notably hold that the pilot must never lose sight of his drone, nor fly it at night or higher than 150 meters; that the drone must not fly over the urban area or where crowded people may be located; and also that the drone does not have to approach aerodromes and sensitive sites.

In case of drone equipped with cameras, microphones and other sensors must respect the general privacy rules. Especially, it is forbidden to record images allowing to directly or indirectly recognize or identify people (such as through faces, number plates, etc.) without their prior consent.

7. The Results of the Defender Project

How can be possible to use drones to prevent essential infrastructure disaster and, at the same time, to protect data?

As anticipated in the first paragraph, the Defender project propones the monitoring of essential infrastructure with the indispensable use of drones. In this case, how can be possible the balance between the use of drone and data protection? What are the most relevant implications on data protection? May the single member States' regulation jeopardize a research project which involves partners from many different countries?

The most significative aspect concerns the concept, earlier discussed, of privacy by default and privacy by design. As long as the legislation may not guarantee the protection of personal data, it is fundamental that all the

organizations collaborates to put in place all the technical and organizational measures. Defender has the intention to adopt all the safeguards that are needed to realize a full protection of personal data, especially applying drivacy by design principles during the implementation phase of the project.

In the guides lines 4/2019 on Article 25 about data protection by design and by default, adopted by the EDPB[23], the term "*measures"* is defined as "*any method or means"* that a controller can apply during the operation. All the measures must be *appropriate*, intending that they must correspond to the purpose to achieve and the "*effectiveness"* means that they must be capable to reduce the danger or the menace of the risk to the personal data. Besides, it's said that "*A technical or organizational measure can be anything from the use of advanced technical solutions to the basic training of personnel, for example on how to handle customer data. There is no requirement to the sophistication of a measure as long as it is appropriate for implementing the data protection principles effectively".* Besides, there are some examples of safeguards that a controller could choose: involving data subjects during the data processing or giving constantly updates about the storage of personal data to the data subject, or installing an alert of data in the storage, or pseudonymizing of personal data, thanks to the principle of minimization.

Defender has mobilized to respect the principle of privacy by design, applying these following measures: face recognition component; people detection component; HILT component. The face recognition component is a system that allows to process the biometrical data of an individual in real time. This is a data that needs to be carefully processed: in fact, there is not an automatic decision made during the train model of facial recognition and the legal basis to capture data is the public interest, without the necessity of data subject's consent.

Thus, all the collection of face recognition is totally complaint to GDPR, in order to the fact that the purposes of processing are specific, legitimate and explicit.

[23] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

However, it's important to define the category of data subject that will be involved in the operations and to establish the duration of the data storage, according to the Article 5 of GDPR. About the category of data subject, for example, if the flight will be in a working area, it is recommended to inform previously the employees with a specific privacy policy, and to obtain a written and explicit consent from them. In fact, in the phase of the pilot, the Consortium of the Defender Project has limited the test, during the pilots, to the premises of the single companies of the partners involved in the project, in order to collect in advance their express consent to be depicted in the video took by the drones.

Secondly, the people detection component is not subjected to the GDPR. Indeed, it is an operation that classify humans differentiating them from other objects or non-objects, without any conservation of personal data or any identification of individuals and his/her characteristics. So, in this case, it is impossible to lead back an information to a person. This is a crucial issue, as long as the pilots made have demonstrated the possibility of developing security activities, aiming at avoiding human attacks to the strategic infrastructures, minimizing the collection of personal data.

Finally, the HILT component states for "*Human in the loop",* which consists in geolocating people, without capturing any further information, previously asking for their consent. This is another aspect which goes beyond the specific area of the critical infrastructure: a recent example is the use of data tracking during the Covid-19 emergency, used for example in Germany, with the purpose of monitoring people's movements through data which are anonymized and aggregated.

The same approach has been used in this project. All the data are encrypted, even if some problems arise with the use of blockchain technologies which make the encryption: in fact, even if blockchain and GDPR have the same purposes, namely for instance to collect data in a full transparency protecting the data subject, blockchain is immutable and so, for individuals, it would be

impossible to exercise the right to erase, the right to be forgotten or the right to modify their data[24].

In addition, another important issue is that blockchain is organized in decentralized system with undefined number of data processor or data controller, differently from GDPR, that privileges a centralized system. Furthermore, even if a collection of personal data is not made, it is recommended to increase the security measures to prevent data breach and to inform the data subjects about the data processing, implementing these procedures, as well as to define in advance the duration of data storage and made a communication of it to interested people.

In conclusion, in relation to the HILT component, there are some concerns about the total compliance to GDPR, especially, in consideration of the usage of blockchain: the storage of personal data in a blockchain can be dangerous because of the usage of public keys that is always connected to personal data (even if, this data are encrypted, are still attributable to the data subject) and that allows the storage of the data longer than the period which is strictly necessary for the purposes for which the personal data are processed.

Another topic concerning Defender and its compliance to GDPR is the storage of personal data during the implementation phases. If there is a usage of drone during a programmed operation, the consent by the individuals involved should be obtained before starting the processing. In any case, the following conservation of this data is covered by the Article 89, in so far as it establishes "*Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes".*

[24] See Compert C., Luinetti M., Portier B., IBM, *Blockchain and GDPR How blockchain could address five areas associated with GDPR compliance,* White Paper, 2018.

Diritto Mercato Tecnologia

Numeri Speciali

2016 Lo Statuto Etico Giuridico dei Campioni Biologici Umani
a cura di Dario Farace

2017 Il Mercato Unico Digitale
a cura di Gianluca Contaldi

2018 La Ricerca su Materiali Biologici di Origine Umana:
Giuristi e Scienziati a confronto
a cura di Alberto M. Gambino, Carlo Petrini e Giorgio Resta

2019 La Tassazione dell'Economia Digitale tra Sviluppi Recenti
e Prospettive Future
a cura di Alessio Persiani

La rivista "Diritto Mercato Tecnologia" intende fornire un costante supporto di aggiornamento agli studiosi e agli operatori professionali nel nuovo scenario socio-economico originato dall'interrelazione tra diritto, mercato e tecnologia, in prospettiva interdisciplinare e comparatistica. A tal fine approfondisce, attraverso studi nei settori privatistici e comparatistici, tematiche afferenti in particolare alla proprietà intellettuale, al diritto antitrust e della concorrenza, alle pratiche commerciali e alla tutela dei consumatori, al biodiritto e alle biotecnologie, al diritto delle comunicazioni elettroniche, ai diritti della persona e alle responsabilità in rete.

ISSN (Online Edition): 2239 -7442