IAIC DGBIC CREDA

DIRITTO MERCATO TECNOLOGIA

FONDATA E DIRETTA DA
Alberto M. Gambino

COMITATO DI DIREZIONE
Valeria Falce, Giusella Finocchiaro, Oreste Pollicino,
Giorgio Resta, Salvatore Sica

8 febbraio 2024

Use of Biometric Data in research activity. The solution adopted by the Arcadian Project

Giovanni Maria Riccio, Fabiola Iraci Gambazza, Paolo Gentili; Adriana Peduto, Ginevra Munafò

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

USE OF BIOMETRIC DATA IN RESEARCH ACTIVITY. THE SOLUTIONS ADOPTED BY THE ARCADIAN PROJECT

Giovanni Maria Riccio, Fabiola Iraci Gambazza, Paolo Gentili, Adriana Peduto, Ginevra Munafò

1. Introduction

In the complex and fragmented spectrum of personal data protection, biometric data represent one of the most challenging issues. On one hand, because, as will be discussed below, they represent data that allow for precise and unique identification of individuals. On the other hand, because they offer vast opportunities in many sectors, including in relation to the recognition of minors (and their protection) for accessing internet services.

There is another aspect that raises concerns, namely the use of biometric data for the purpose of citizens' recognition by public authorities. Dystopian scenarios that link the needs of public security with the legitimate expectations of individuals not to be constantly monitored in their movements in public spaces.

This paper aims at investigating the regulations regarding biometrics in the General Data Protection Regulation (EU Regulation No. 2016/679 - GDPR), and then analysing the rules of the AI Act (in the currently available version, the text of which is not yet finalised). These rules have been applied in the compliance activities within the Arcadian project, funded under the Horizon2020 measure of the European Commission: the legal activity

carried out has allowed, in particular, to examine the rules on biometrics and personal data applied to the research project pilots and the guidelines provided in this context.

2. General framework of biometric data in the GDPR

Biometrics is generally qualified as the automated recognition of individuals by means of unique physical characteristics, such as fingerprints, facial recognition, iris patterns, and voiceprints, typically for the purposes of security[1]. The most advanced technologies in biometrics have made possible the implementation of increasingly precise and efficient systems, but at the same time have raised significant issues regarding privacy and personal data protection. Therefore, the processing of biometric data requires special attention to ensure compliance with rigorous security standards and enable adequate user control and consent regarding the collection and use of their biometric data[2].

The advent of advanced technologies, particularly artificial intelligence (AI), has revolutionized biometric data processing. AI algorithms greatly enhance the accuracy and reliability of biometric systems, enabling intricate pattern recognition and analysis. On the other hand, the integration of AI raises significant concerns regarding security, potential biases in data processing, and, specially, privacy.

However, biometrics has not always been included within European data protection legislation. In fact, the last piece of European Union legislation on personal data protection - before GDPR - had been published in 1995, with the Directive 95/46/CE, and it did not include any provision regarding biometrics. Since then, technological evolution has undergone an extraordinary development, also bringing about new needs for intervention

[1] See S. Romesh, K. Breckenridge, S. Gruskin, J. Klaaren, *Rights and Ethics in Biometric Population Registration: Mapping the Limits of Digital Recognition and the Drivers of Exclusion* (October 9, 2023). Available at SSRN: https://ssrn.com/abstract=4647719

[2] Many of these aspect are specifically investigated in the report of T. Christakis, K. Bannelier, C. Castelluccia, D. Le Métayer, *Mapping the Use of Facial Recognition in Public Spaces in Europe, Part 3: Facial Recognition for Authorisation Purposes*, Report of the AI- Regulation Chair (AI-Regulation.Com), MIAI, 2022.

by the authorities. In particular, new systems for detecting particular genetic characteristics of individuals, also through the use of artificial intelligence, have attracted the attention of the European legislator, who has included, for the first time, specific provisions about the processing of biometric data within the General Data Protection Regulation (GDPR)[3].

Within the GDPR, specific provisions address the processing of biometric data, recognizing its sensitive nature and potential privacy implications. The Regulation, at article 4 n. 14), provided a definition of biometric data as *"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data*". The definition adopted by the GDPR is therefore very broad, encompassing possible technological developments, and is characterized by the fact that the data allows for the unique identification of the subject through its biological and/ or behavioural characteristics[4]. In other words, biometric data is data that identifies only and exclusively a specific subject, and in this sense, it is more sensitive data compared to "traditional" sensitive data, such as health data, which could be common to multiple individuals[5].

Before the entry into force of the GDPR, some references to the notion of biometric data can be found in other European provisions and notably those connected with border controls, such as the Regulation 2252/2004, which establishes standards for security features and biometrics in passports and travel documents issued by Member States, and the Regulation 2017/2226, which establishes an entry/exit system of the access to a member State. Regulation 2017/2226 also includes several references to biometric data, which are qualified "fingerprint data and facial image" (Article 3(18)), and

[3] The General Data Protection Regulation entered into force on May 24, 2016, and applies from May 25, 2018. It is a comprehensive data protection law enacted by the European Union (EU) to safeguard the privacy and personal data of individuals within the EU and the European Economic Area (EEA).

[4] A. Jain, L. Hong, S. Pankanti, *Biometric identification*, 43 Communications of the ACM, 2000, 91.

[5] C. Bourcha, M.-L. Deftou, A. Koskina: *Data Mining of Biometric Data: Revisiting the Concept of Private Life?*, 3 *Ius et Scientia*, 2017, 46.

"fingerprint data" as "the data relating to the four fingerprints of the index, middle finger, ring finger and little finger from the right hand where present, and otherwise from the left hand" (Article 3(16). Finally "facial image" is defined as "digital images of the face" (Article 3(17)[6].

However, biometric data, such as fingerprints, facial features, or iris scans, are considered special categories of personal data under the GDPR. Consequently, their processing is subject to stricter regulations aimed at ensuring transparency, accountability, and respect for individuals' rights, so that they fall within those special categories of personal data (commonly referred to as sensitive data) outlined in Article 9 of the GDPR, from which may emerge:

- racial or ethnic origin;
- political opinions, religious or philosophical beliefs;
- trade union membership;
- genetic data and biometric data intended to uniquely identify an individual;
- data concerning health or a person's sex life or sexual orientation.

As a practical example of application of biometric data, the European legislator has primarily considered facial recognition systems, in which, through optical (such as the face-scan feature of a mobile phone) or physical measurement procedures, data related to the external appearance characteristics of a person are collected[7]. In many Member States' legislation, furthermore, the use of biometrics has been applied to electronic ID cards and in the healthcare sector, also sparking numerous criticisms and protests[8].

[6] See L.A. Bygrave, L. Tosoni, Biometric data, in C. Kuner, A. Lee Bygrave, C. Docksey, (Eds.), *The EU General Data Protection Regulation (GDPR)*, Oxford Univ. Press, 2020, 210.

[7] L.A. Bygrave, L. Tosoni, Biometric data, in C. Kuner, A. Lee Bygrave, C. Docksey, (Eds.), *The EU General Data Protection Regulation (GDPR)*, Oxford Univ. Press, 2020, 207.

[8] See for instance, B. Custers, A.M. Sears, F. Dechesne, I. Georgieva, T. Tani, S. van der Hof*, EU Personal Data Protection in Policy and Practice*, Springer, 2019, 159. This aspect is also discussed by the European Court of Justice in the decision of 17th October 2013, CJEU, C 291/12, *Schwarz v Bochum*, ECLI:EU:C:2013:670.

The main argument is related to the automation recognition of individuals, as highlighted also by the WP29, in relation to the biometric identification and authentication schemes, which may "*change irrevocably the relation between body and identity, because they make the characteristics of the human body "machine- readable" and subject to further use*"[9].

In this regard, another EU institution, the European Data Protection Board (EDPB) has issued guidelines on the use of facial recognition technology in the realm of law enforcement to ensure compliance with data protection laws and uphold individuals' rights to privacy and personal data protection[10]. These guidelines provide guidance on the lawful and ethical use of facial recognition technology, stressing the importance of necessity, proportionality, and accountability in its deployment. The EDPB emphasizes the need for clear legal bases, such as public interest or law enforcement tasks, for processing biometric data through facial recognition technology.

Other common examples of biometric processing are given by fingerprint analysis or on iris recognition. In particular, the biometric data provided by the fingerprint is characterized by the fact that it leaves a trace, thus distinguishing it from those biometric features that leave no trace, referred to as traceless.

As for the notion of processing, pursuant to the GDPR, it means "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*" (art. 4 n. 2 GDPR).

---

[9]Article 29 Data Protection Working Party (WP29), *Opinion 3/2012 on developments in biometric technologies*, April 27, 2012, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf; See also CJEU, C 291/12, Opinion of the Advocate General, *Schwarz v Bochum*.

[10] EDPB, *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*, May 17, 2023, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf.

The lawfulness of processing biometric data under the GDPR, as outlined in Article 6, hinges on several principles.

Firstly, processing must have a legal basis, such as obtaining the explicit consent of the data subject or fulfilling contractual obligations. Additionally, processing may be lawful if necessary for compliance with legal obligations, protection of vital interests, performance of tasks carried out in the public interest or exercise of official authority, or legitimate interests pursued by the data controller or a third party. However, special attention must be paid to biometric data, as their processing is subject to stricter requirements under Article 9 of the GDPR, necessitating explicit consent or reliance on specific legal grounds such as substantial public interest or legal claims.[11]

Thus, ensuring compliance with both Article 6 and Article 9 is essential to lawfully process biometric data while upholding data subjects' rights and privacy. In order to do that, the controller must conduct a Data Protection Impact Assessment (DPIA), which is a procedure ruled by Article 35 of the GDPR[12].

This process is designed to systematically analyze and assess the potential risks and impacts of a specific data processing activity on individuals' privacy and data protection rights. The primary purpose of a DPIA is to identify and mitigate risks associated with processing personal data, particularly when the processing is likely to result in high risks to

[11] Other examples of lawful processing of sensitive data are given by Article 9, par. 2 (GDPR), when: a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes; b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law; c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

[12] Under Article 4, n. 7) of the GDPR, the controller is the "*natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"*.

individuals' rights and freedoms. The Working Party set up under Article 29 of Directive 95/46/EC, which is an independent European advisory body on data protection and privacy, published the "Guidelines on Data Protection Impact Assessment (DPIA)", where it states that "*a DPIA is a process for building and demonstrating compliance"*[13].

In the context of the DPIA, in addition to the assessment of the adequacy of technological measures adopted, the proportionality of the data collected taken must also be considered. The European Court of Human Rights (ECtHR) addressed this aspect in the *S and Marper* decision, where it found that English legislation was disproportionate and in violation of Article 8 of the European Convention on Human Rights (ECHR) when it retained certain biometric data (fingerprints, cellular samples, and DNA) of individuals suspected but not convicted of criminal offenses[14].

3. Data Protection Authorities' provisions on biometrics

National Data Protection Authorities (DPAs) play a pivotal role in upholding and enforcing the General Data Protection Regulation (GDPR) within their respective jurisdictions. Their responsibilities encompass a wide range of activities, including providing guidance and advice on GDPR compliance, investigating complaints and data breaches, conducting audits and inspections, and imposing sanctions for non-compliance[15].

A recent case, which occurred in 2022, concerns a sanction imposed by several National Authorities on Clearview AI, a US-based company, for employing biometric surveillance methods on individuals. In Italy, the national Data Protection Authority (Garante per la protezione dei dati

[13] https://ec.europa.eu/newsroom/article29/items/611236/en, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679;*
[14] *S and Marper v. United Kingdom* [2008] ECHR 1581.
[15] A. Giurgiu, T.A. Larsen, *Roles and Powers of National Data Protection Authorities. Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?*, 2 *European Data Protection L.Rev.*, 2016, 342.

personali) imposed a fine of EUR 20 million on Clearview AI[16], who reportedly possesses a database containing over 10 billion facial images sourced from various public online platforms such as media outlets, social media, and online videos, utilizing web scraping techniques. The company offers an advanced earch service enabled by AI systems, allowing the creation of profiles based on extracted biometric data from these images. These profiles can be enriched with additional information such as image tags, geolocation, and source web pages. Following complaints and alerts, investigations by the Italian Data Protection Authority revealed that Clearview AI unlawfully tracked Italian nationals and individuals within Italy. The company processed personal data, including biometric and geolocation information, without a legitimate legal basis, infringing several fundamental principles of the GDPR such as transparency, purpose limitation, and storage limitation.

Based on the infringements found, the Italian SA (Supervisory Authority) fined Clearview AI EUR 20 million and ordered the company to erase the data relating to individuals in Italy; it banned any further collection and processing of the data through the company's facial recognition system[17].

The investigations were also carried out by other European Data Protection Authorities, such as those of Sweden[18] and Germany[19], followed by decisions from the Belgian SA[20].

The investigative activity conducted by the various Authorities revealed that Clearview had collected and stored biometric data without the

[16] Garante Privacy, Provision n. 50 del 10 febbraio 2022, available at the following link*: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9751362.*

[17] See also G. Pathak, *Manifestly Made Public: Clearview and GDPR*, 8 *European Data Protection L. Rev.*, 2022, 419.

[18] Original text of the measure is available at URL: *https://www.imy.se/globalassets/dokument/beslut/beslut-tillsyn-polismyndigheten-cvai.pdf. A* summary is also available at European Data Protection Board website*: "Swedish DPA: Police unlawfully used facial recognition app",* 12 february 2021.

[19] German Supervisory Authority of the Land of Hamburg, Decision No. 545/2020.

[20] The Belgian Data Protection Authority, during an inspection, found that the services of the company collecting the data were also being utilized by the Belgian Federal Police.

knowledge of the individuals concerned, leading to several condemnations against the company.

Specifically, in the Swedish case, the company had provided the data to local police for investigative and crime prevention purposes. It is interesting to note how the incident highlighted the primacy of citizens' rights over their biometric data, even in cases of public crime prevention efforts.

The issue of processing biometric data has also concerned the EU Court of Justice, which has ruled on the storage without any time limit of biometric data of prisoners by Bulgarian police (Case C-118/22). In particular, in Bulgaria, an entry was made in the police records concerning a person in the course of a criminal investigation for failing to tell the truth as a witness. That person was ultimately found guilty of that offence and given a one year suspended sentence. After serving that sentence, that person was legally rehabilitated. He subsequently applied to be removed from the police records. Under Bulgarian law, the data relating to him are retained in those records and may be processed by the authorities, who have access to them without any time limit other than his death. His application was rejected on the ground that a final criminal conviction, even after legal rehabilitation, is not one of the grounds for removal of the entry from the police records. On appeal, the Bulgarian Supreme Administrative Court referred questions to the Court of Justice.

In its judgement, the Court of Justice holds that the general and indiscriminate storage of biometric and genetic data of persons convicted of an intentional offence, until their death, is contrary to EU law. Ultimately, the Court notes, Under EU law, national legislation must lay down an obligation for the data controller to review periodically whether that storage is still necessary and to grant the data subject the right to have those data erased if that is no longer the case[21].

[21] *Right to erasure: the general and indiscriminate storage of biometric and genetic data of persons convicted of criminal offences, until their death, is contrary to EU law,* CJEU Press release n. 20/24, January 30, 2024 at URL:
https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-01/cp240020en.pdf;
for the full text of the judgement, Case C-118/22, CJEU:
https://curia.europa.eu/juris/document/document.jsf;jsessionid=06CFEA72B9DA5D8CB

In conclusion, the importance of processing biometric data lawfully has been pointed out both by the European Court of Justice and by national privacy authorities across the European Union. These bodies emphasize the fundamental rights to privacy and data protection enshrined in European law and advocate for the responsible and transparent use of biometric data.

4. Biometric data within the Artificial Intelligence Act

In April 2021, as part of the EU Digital Strategy, the European Commission published a proposal for a regulation to harmonize the rules regarding the use of Artificial Intelligence by both public and private entities, aiming to promote the integration of Artificial Intelligence systems (EU Regulation 2021/0106), and at the same time trying to balance two potentially contradictory interests such as law and innovation.

Most recently, the European Union, following the Trilogue negotiations, reached a political agreement on the AI Act on December 8, 2023. Pending the approval of the official text - which must be voted on by the Committees on the Internal Market and Civil Liberties of the Parliament and then formally adopted by the Parliament and the Council to become EU law - it is possible to analyze the regulation concerning the processing of biometric data.

The Artificial Intelligence Act addresses the processing of biometric data within the realm of artificial intelligence (AI) technologies. With the proliferation of AI-driven systems utilizing biometric data for various applications, the Act aims to establish a comprehensive regulatory framework to ensure the responsible and ethical use of such data, and inevitably triggers the application of the GDPR. Specifically, the Act sets out requirements for transparency, accountability, and fairness in the processing of biometric data by AI systems.

Firstly, at recital n. 8, the Proposal provides a "functional" definition of biometric identification systems, as *"an AI system intended for the*

E4B21A4ACB17407?text=&docid=282264&pageIndex=0&doclang=it&mode=req&dir=&occ=first&part=1&cid=4727537

identification of natural persons without their active involvement, typically at a distance, through the comparison of a person's biometric data with the biometric data contained in a reference database, irrespectively of the particular technology, processes or types of biometric data used. Such remote biometric identification systems are typically used to perceive multiple persons or their behaviour simultaneously in order to facilitate significantly the identification of natural persons without their active involvement"[22].

Recital n. 8, then, offers a distinction between "real-time systems" and "post" systems. "Real-time" remote biometric identification system means systems whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay.

This comprises not only instant identification, but also limited short delays in order to avoid circumvention; in the case of "post" systems, in contrast, the biometric data have already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned.

Given this distinction, the Regulation considers "real-time remote biometric identification systems" an "high risk AI system". In fact, the Artificial Intelligence Act adopts a risk-based approach to regulate the deployment and use of artificial intelligence technologies within the European Union. This approach aims to assess the potential risks associated with AI systems based on their intended use and impact on individuals and society. By categorizing AI applications into low, high, and unacceptable risk levels, the Act aims to provide a fair protection to every possible outcome.

Specifically, Article 5, lett. d) of the Regulation prohibits the use of the aforesaid "real-time" remote biometric identification systems in publicly

[22] For the full text of the Proposal: *https://media.licdn.com/dms/document/media/D4D1FAQH5Z58kTYtrOQ/feedshare-document-pdf-analyzed/0/1708295883717?e=1709769600&v=beta&t=iytPFvVgcP1C9ahlQs_Ty2ev18usbfYQ_06U9L9mmpA*

accessible spaces for the purpose of law enforcement, unless and in as far as such use is strictly necessary for one of the following objectives:

1. the targeted search for specific victims of abduction, trafficking in human beings and sexual exploitation of human beings as well as search for missing persons;
2. the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;
3. the localisation or identification of a person suspected of having committed a criminal offence, for the purposes of conducting a criminal investigation[23].

It should be specified, however, that biometrics qualifies as a high-risk system only when included in a massive surveillance context[24].

5. Biometric data within the Arcadian-IoT Project

5.1. The Arcadian-IoT Project and its legal framework

The ARCADIAN-IoT project aims to promote innovative, decentralised solutions for trust and identity management in IoT systems, by considering all the entities interacting with such systems, including persons, IoT devices (objects) and respective applications/services.

The design of such technologies, the interaction of the same and, above all, their use in the first prototype P1 raises questions which are specifically governed by several European regulations (and member state legislations) including, *inter alia*, the management of personal data[25].

---

[23] *https://media.licdn.com/dms/document/media/D4D1FAQH5Z58kTYtrOQ/feedshare-document-pdf-analyzed/0/1708295883717?e=1709769600&v=beta&t=iytPFvVgcP1C9ahlQs_Ty2ev18usbfYQ_06U9L9mmpA*

[24] 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).

[25] On this approach see L. Jasmontaite - I. Kamara, G. Zanfir-Fortuna, S. Leucci, *Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR, European Data Protection L. Rev*., 168 (2018).

The purpose of this section is to identify, specifically for Domain A, the main relevant legal concerns and, against this background, outline the applicable regulatory framework.

In fact, with reference to Domain A, some technologies used by the partners (*i.e.* AI, biometric technologies, IoT devices and drones) might raise issues on data protection.

it is considered useful to briefly summarise the main critical issues underlying each technology used in the Project:

- *IoT*: the major risks are the information asymmetry and, consequently, the quality of users' consent. The above mentioned risks are even more critical when the IoT process special categories of personal data pursuant to Article 9, GDPR;
- *facial recognition mechanism:* AI also entails risks, including threats to fundamental rights, such as risk that a bias (unconsciously set by the programmers) negatively influences machine learning and then affects the AI results (*e.g.*, the AI could "make decisions" influenced by ethnicity, gender, age, *etc.*) and the sharing of data, given that the AI feeds on data which is indispensable for the training of the machine. The above-mentioned risks are even more critical when using AI systems in the biometric recognition of individuals, who must be adequately informed of the technology and of the developments it may have. Moreover, the comprehensibility of what is being communicated must be guaranteed;
- *drones:* from a perspective focussing strictly on data protection, it must be noted that drones are combined with applications such as cameras or video-cameras and might also record the images, through software to process the video images, which might have further applications (including facial recognition). This implies the collection, recording, organisation, storing, use and combination of data allowing the identification of persons. The drone operations must be carried out with the minor interference with the privacy and personal data of individuals on the ground, and any personal data collected must be handled in compliance with the principles, requirements and individual rights laid down in the GDPR.

Given this premises, the relevant legal framework for this project is the Regulation (UE) 2016/679 on the protection of natural persons with regard to the processing of personal data and on free movement of such data ("Regulation" or the "GDPR"), as well as the other provisions adopted by the competent authorities European authorities and bodies, namely:

- the Opinion 8/2014 on the "*Recent Developments of the Internet of Thing*" of the Article 29 Data Protection Working Party (now, the European Data Protection Board, "WP29" or "EDPB");
- "*White Paper on Artificial Intelligence*" of the European Commission;
- "*Ethics Guidelines for Trustworthy Artificial Intelligence*" adopted by the High Level Expert Group on Artificial Intelligence set up by the Commission;
- EU Regulations 2019/947 and 2019/945, setting out the framework for the safe operation of civil drones in the European skies through a risk-based approach.

5.2. Using AI technologies for individual facial recognition purposes

As said, Artificial Intelligence is a set of technologies that combines data, algorithms and computing power. As pointed out by the EU Commission in its "*White Paper on Artificial Intelligence*", the latter is rapidly developing and is going to transform the pattern of society and the way people act in it, improving, for example, health care and increasing the safety of citizens.

In this regard, the European Parliament has pointed out that the increasing use of AI systems also entails risks, including threats to fundamental rights, including:

1. risk that a bias (unconsciously set by the programmers) negatively influences machine learning and then affects the AI results (*e.g.*, the AI could "make decisions" influenced by ethnicity, gender, age, *etc.*);
2. opacity of the algorithms: the steps through which the data are interpreted are not always explainable (transparent);
3. privacy and sharing of data, given that the AI feeds on data which is indispensable for the training of the machine;

4. consent and autonomy: the data subject must be adequately informed of the technology and of the developments it may have. Moreover, the comprehensibility of what is being communicated must be guaranteed.

Back in 2018, the European Commission set out its vision of ethical, safe and state-of-the-art AI "made in Europe". To support the implementation of this vision, the Commission has set up a High Level Expert Group on Artificial Intelligence, which has developed the "*Ethics Guidelines for Trustworthy Artificial Intelligence*", with the aim of promoting trustworthy AI. Starting from a fundamental rights-based approach, the Group identifies ethical principles and values that must be respected in the development, deployment and use of AI systems.

In particular, the Group provides key indications (such as paying special attention to situations involving vulnerable subjects, taking appropriate measures to mitigate risks, *etc.*), as well as indications on how to achieve reliable AI by listing seven requirements that AI systems should meet, namely:

1. human intervention and surveillance;
2. technical robustness and security;
3. confidentiality and data governance;
4. transparency;
5. non-discrimination and fairness
6. social and environmental well-being;
7. accountability.

Within the ARCADIAN-IoT framework, AI components are used for facial recognition purposes and therefore imply the processing special categories of personal data pursuant to Article 9.

It has been said that biometric data fall within the special categories of personal data regulated by the Article 9, GDPR which states that "*processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited*" unless

one of the conditions laid down in Article 9, par. 2 is met and, in particular, if the data subject has given explicit consent or if the processing.

While processing this type of data, it is important to keep in mind that the risk-based approach of the GDPR requires data controllers to use greater care because collecting and using it is more likely to interfere with these fundamental rights or open someone up to discrimination. In the context of the Pilot, AI systems are not used to make decisions about individuals.

Moreover, for the purposes of the development of the Pilot, the Partners of the Project use only personal data of volunteers, who, before taking part in the Pilot, have received an information notice in accordance with the Regulation, containing all the information related to the Project and, on the basis of this information, have given their consent to participate and to the processing of their personal data. Therefore, the risk of lack of information and invalid consent is prevented[26].

With specific reference to the facial recognition system, the AI system, in its use, is monitored and supervised with human intervention, as well as protected by robust cybersecurity systems, as detailed above. The personal data processed are therefore protected from any loss of confidentiality.

Finally, it should be noted that the data used for training the algorithms for the Pilot are not disclosed outside the Project. Therefore, all concerns highlighted above are addressed.

5.3. The use of drones in the Arcadian-IoT Project

From a perspective focussing strictly on data protection, drone operations can be classified into two main categories: purpose of the operation involving personal data processing, on one hand, and, on the other hand, operations whose purpose does not include the processing of personal data.

With specific reference to the first type of operations, it must be noted that drones are combined with applications such as cameras or video-cameras and might also record the images, through software to process the video images, which might have further applications (including high power

[26] In the pilots' activities the research has followed also the suggestions provided by OpenAIRE, Personal data and the Open Research Data Pilot, www.openaire.eu

zoom, facial recognition, behaviour profiling, movement detection, night vision, GPS systems processing the location of the persons filmed, *etc*). This implies the collection, recording, organisation, storing, use and combination of data allowing the identification of persons.

It must be noticed that regulations for the use of airspace apply in parallel with personal data protection regulation such as the EU Regulations 2019/947[27] and 2019/945[28].

In particular, this balance should take into account national security strategies and the necessity of not to step back in the protection of privacy and security of the individuals. This is a crucial issue as new technologies (and, among them, drones) may impact in several individual aspects[29].

---

[27] Full text at URL: https://eur-lex.europa.eu/eli/reg_impl/2019/947/oj. 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. 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. There are two types of operations: the VLOS operations and the BVLOS operation. The first operation is made with the necessity of visual sight; 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. 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.

[28] Full text at URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0945

[29] C. Pauner, I. Kamara, J. Viguri, *Drones. Current challenges and standardisation solutions in the field of privacy and data protection*, ITU Kaleidoscope: Trust in the Infor-

This precondition and the potential clash between fundamental rights of the individuals and the necessity of the European Union and of the member States to monitor the emerging threats to security has guided the approach of ARCADIAN-IoT and its legal and ethical outcomes.

According to EU Regulations 2019/947 and 2019/945, there is no distinction between leisure or civil, commercial drone activities. What is relevant for the EU regulations is the weight and the specifications of the civil drone as well as the operation it is intended to conduct.

Regulation (EU) 2019/947, which is applicable since 31 December 2020 in all EU Member States, including Norway and Liechtenstein, caters for most types of civil drone operations and their levels of risk. It defines three categories of civil drone operations. The Regulation also emphasises that all drone operators and remote pilots must comply with European and national rules regarding privacy and data protection[30]. The drone operations must be carried out with the minor interference with the privacy and personal data of individuals on the ground, and any personal data collected must be handled in compliance with the principles, requirements and individual rights laid down in the GDPR.

In the Pilot, the use of drones implies the processing of personal data which, however, as explained above, only takes place with reference to volunteers data, who, before taking part in the Pilot, have received an information notice in accordance with the Regulation, containing all the information related to the Project and, on the basis of this information, have given their consent to participate and to the processing of their personal data.

Furthermore, in the Pilot, the drones are only used in a space that is not accessible to the general public, but only to researchers who have reason to access it, as well as to volunteers who have given their consent to participate in the Project. Therefore, the use of drones for the Pilot does not raise legal concerns.

---

mation Society (K-2015), December 2015, 5; M. Ketan, *Drones and Their Legality in the Context of Privacy*, Leiden Law School; National Law University Jodhpur (NLUJ), November 25, 2015, 12.

[30] The relation among these regulations are fully inspected in G.M. Riccio, F. Iraci Gambazza, *Critical Infrastructures, Use of Drones and Data Protection Impacts*, in *Diritto Mercato Tecnologia*, 2020, 1.

6. Conclusions

The use of such technological components (*i.e.*, AI, biometric technologies and IoT medical devices and drones) might raise issues on the applicable law. However, in the context of Pilot all possible concerns are addressed for the reasons above mentioned.

Given that personal data legislation is the main legal framework, it should be also noted that many partners do not use personal data in the development of their own technologies: this is due to the fact that, on the one hand, these are sometimes security systems (e.g. cyber threat intelligence component, encryption algorithms, eSim, *etc.*) that by their very nature do not involve the processing of data and, on the other hand, because in some cases data are processed anonymously. Furthermore, from this perspective, many concerns are already addressed by the nature of the Project itself, which, as is known, aims precisely at enable decentralised management of trust, identity, privacy and security in IoT systems.

Finally, with regard to the interaction of the components within P1, as already pointed out, all possible concerns are addressed, especially in light of the fact that the Pilot is performed exclusively with volunteer data, who have been informed about the Project, in spaces specifically reserved for Pilots (and thus not accessible to the public).

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